Nationwide Financial Services, Inc.

Public Sector Retirement Plan Administration

Report on Management's Description of its System and the Suitability of the Design and Operating Effectiveness of its Controls

For the Period January 1, 2023 to December 31, 2023

Nationwide Financial Services, Inc.

Public Sector Retirement Plan Administration

Report on Management's Description of its System and the Suitability of the Design and Operating Effectiveness of its Controls

Table of Contents

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
Suite 500
191 West Nationwide Blvd.
Columbus, OH 43215-2568

Independent Service Auditors’ Report

Board of Directors of Nationwide Mutual Insurance Company and its Nationwide Financial Services, Inc.:

Scope

We have examined management of Nationwide Financial Services, Inc.’s accompanying description of its Public Sector Retirement Plan Administration System (the System) for processing user entities’ transactions throughout the period January 1, 2023 to December 31, 2023 titled “Management of Nationwide Financial Services, Inc.’s Description of its Public Sector Retirement Plan Administration System” (the 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 “Management of Nationwide Financial Services, Inc. Assertion” (the Assertion). The controls and control objectives included in the Description are those that management of Nationwide Financial Services, Inc. believes are likely to be relevant to user entities’ internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

The information included in Section V, “Other Information Provided by Management of Nationwide Financial Services, Inc.”, is presented by management of Nationwide Financial Services, Inc. to provide additional information and is not a part of the Description. Information about Nationwide Financial Services, Inc.’s SEC Custody Rule has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description and, accordingly, we express no opinion on it.

Nationwide Financial Services, Inc. uses the subservice organizations identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities’ internal control over financial reporting. The Description includes only the control objectives and related controls of Nationwide Financial Services, Inc. and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Nationwide Financial Services, Inc. can be achieved only if complementary subservice organization controls assumed in the design of Nationwide Financial Services, Inc.’s controls are suitably designed and operating effectively, along with the related controls at Nationwide Financial Services, Inc. Our examination did not extend to controls of the subservice organizations, 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 Nationwide Financial Services, Inc.’s controls are suitably designed and operating effectively, along with related controls at Nationwide Financial Services, Inc.. 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.

Service Organization’s Responsibilities

In Section II, management of Nationwide Financial Services, Inc. has provided the 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. Nationwide Financial Services, Inc. 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 Auditors' 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 the Assertion, the Description is fairly presented and the controls were suitably designed and operated effectively to achieve the related control objectives stated in the Description throughout the period January 1, 2023 to December 31, 2023. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the Description, 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 the Assertion:

- the Description fairly presents the System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023
- 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 January 1, 2023 to December 31, 2023, and subservice organizations and user entities applied the complementary controls assumed in the design of Nationwide Financial Services, Inc.'s controls throughout the period January 1, 2023 to December 31, 2023
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period January 1, 2023 to December 31, 2023 if complementary subservice organization controls and complementary user entity controls, assumed in the design of Nationwide Financial Services, Inc.'s controls, operated effectively throughout the period January 1, 2023 to December 31, 2023.

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 management of Nationwide Financial Services, Inc., user entities of Nationwide Financial Services, Inc.'s System during some or all of the period January 1, 2023 to December 31, 2023, 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 these specified parties.

KPMG LLP

Columbus, Ohio
March 21, 2024

Section II.

Management of Nationwide Financial Services, Inc.'s Assertion

Nationwide®
is on your side

Management of Nationwide Financial Services, Inc.'s Assertion

We have prepared the accompanying description of the Public Sector Retirement Plan Administration system (the System) for processing user entities' transactions throughout the period January 1, 2023 to December 31, 2023 titled "Management of Nationwide Financial Services, Inc.'s Description of Its Public Sector Retirement Plan Administration System" (the Description) for user entities of the System during some or all of the period January 1, 2023 to December 31, 2023, 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 subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of user entities' financial statements.

Nationwide Financial Services, Inc. uses, the subservice organizations, identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The Description includes only the control objectives and related controls of Nationwide Financial Services, Inc. and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at Nationwide Financial Services, Inc. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Nationwide Financial Services, Inc.'s controls are suitably designed and operating effectively, along with related controls at Nationwide Financial Services, Inc. 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 System made available to user entities of the System during some or all of the period January 1, 2023 to December 31, 2023 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description

   i. presents how the System made available to user entities of the System was designed and implemented to process relevant 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 communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to Nationwide Financial Services, Inc.'s System during the period covered by the Description.

iii. does not omit or distort information relevant to Nationwide Financial Services, Inc.'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 auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period January 1, 2023 to December 31, 2023 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Nationwide Financial Services, Inc.'s controls throughout the period January 1, 2023 to December 31, 2023. 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 Nationwide Financial Services, Inc;

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; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Roger Green

Associate Vice President – Financial Analysis Nationwide Financial

DocuSigned by:
Roger Green
22CAC18C07FA4E8...

March 21, 2024

Michael Carrel

SVP and Chief Technology Officer Nationwide Financial

DocuSigned by:
Michael Carrel
2923B5B0AA39435...

March 21, 2024

Section III.

Management of Nationwide Financial Services, Inc.'s Description of its Public Sector Retirement Plan Administration System

Overview of Operations

Nationwide Financial Services, Inc. (Nationwide), an affiliate of Nationwide Mutual Insurance Company (NMIC), provides a broad array of financial services including Retirement Plans, Annuities, Life Insurance, Mutual Funds and Banking. Certain retirement plan operations of Nationwide are provided through Nationwide Retirement Solutions, Inc. (NRS), with its custodial affiliates Nationwide Life Insurance Company (NLIC) and Nationwide Trust Company, FSB (NTC). NRS, NLIC, and NTC are wholly owned subsidiaries of Nationwide.

NRS markets and administers defined contribution plans for governmental employees. The majority of plan participants contribute to employer-sponsored plans (including Internal Revenue Code Section 401, 403, and 457 plans), which allow the accumulation of retirement assets through pretax employee contributions. Contracts with plans are separated into two different levels of service based upon whether NRS handles the participant accounting. These levels of service are Full Service (plan and participant level records are maintained) and Unallocated Service (only plan level records are maintained). Professional money management is available to Full-Service contract plan participants through Nationwide ProAccount, a managed account service offered by Nationwide Investment Advisors, LLC, (NIA), and a subsidiary of Nationwide. NIA utilizes the services of RIA Services, Inc., a subsidiary of Nationwide, to interface with the operations of NRS. This report has been prepared to provide information on Nationwide, RIA Services, and ProAccounts controls, which may be relevant to internal control of both types of User Entities as well as both levels of service entered into by the plans.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication and Monitoring

Control Environment

As this description is intended to focus on features that are likely to be relevant to internal control over financial reporting of Nationwide's User Entities, it does not encompass all aspects of the services provided or procedures followed by Nationwide for User Entity accounts.

Organization

Nationwide's activities are overseen by Nationwide Mutual Insurance Company (NMIC) Board of Directors and the Audit Committee of the Board of Directors of NMIC. The Board of Directors is comprised of 16 members, including 15 external board members. The Audit Committee monitors internal and external examinations of Nationwide's activities and helps ensure that suitable internal control is maintained.

Nationwide, which has the responsibility for the processing of certain plan transactions, is organized along geographical regions of the User Entities it serves, with a senior executive responsible for oversight of the business unit's activities. The senior executive reports to the President of NMIC.

Nationwide's activities are conducted in accordance with established policy and procedural guides, which are periodically updated. The responsibilities of Nationwide are allocated among personnel to segregate the following functions: input of transactions, processing of transactions, recording of transactions, custody of assets and reconcilement activities.

Personnel Policies and Procedures

NMIC has formal hiring procedures that are designed to help ensure that new employees are qualified for their job responsibilities. New employees must be jointly approved by the Human Resources department and the manager of the department requiring the position. Hiring policies include meeting minimum education and experience requirements, and completion of reference, background, and credit investigation checks. NMIC is an affirmative action/equal employment opportunity employer.

Training of personnel is accomplished through supervised on-the-job training, external seminars, and in-house courses. Certain positions require completion of specific training. It is the immediate supervisor's responsibility to help ensure that employees have completed such training. Department managers are also responsible for encouraging training and development to continue to qualify personnel for their functional responsibilities.

Formal performance reviews are conducted on a semi-annual basis. On a monthly basis, immediate supervisors meet with their employees to review performance goals and provide feedback. Employees are evaluated on objective criteria based on performance.

Risk Assessment

Nationwide activities are subject to review by the Office of Internal Audits (Internal Audits). Internal Audits has been established as an independent, objective appraiser of Nationwide's Group of Companies activities, acting in the interest of Nationwide and its policyholders. Internal Audits reports administratively to the NMIC CEO and the Nationwide Mutual Audit Committee. Internal Audits' scope, responsibilities, and reporting relationships are outlined in a charter that is reviewed annually by the Nationwide Mutual Audit Committee.

During the performance of audit engagements, Internal Audits reviews the reliability and integrity of operational and financial controls; ascertains the extent of compliance with established policies, plans, procedures, laws, and regulations to which Nationwide is subject; verifies the accuracy and propriety of transactions processed; and ascertains the reliability of management information developed within the organization. The audits also cover automated system application controls, and review to help ensure that internal control is adequate to account for and safeguard assets, deter fraud, detect errors, and promote the efficient and effective use of Nationwide resources.

Internal Audits prepares an annual audit plan, which is reviewed and approved by executive management and the Nationwide Mutual Audit Committee. The plan is developed using a formal risk management methodology and provides for an audit approach covering business issues deemed significant by Internal Audits. Activities for the year typically include operational and financial audits, special projects, and system development reviews. Formal reports of audit findings are provided to management after each audit and significant audit findings are summarized and reported to the Nationwide Mutual Audit Committee. Finally, audit findings are tracked to help ensure that action is taken on reported audit findings, and there is an escalation process for issues that are not resolved timely.

Information and Communication

Nationwide's control activities are documented in various procedures, which are updated on an "as-needed" basis.

A Conflict of Interest policy exists, and a Conflict of Interest statement is required to be completed by managers and other key employees, except those whose duties are clerical in nature.

Nationwide is subject to regulation by the state regulators in the states in which it operates. As such, Nationwide may be required to file periodic reports with and is subject to periodic examination by regulatory authorities.

Monitoring

A formal management information and reporting system exists to provide monitoring of key control and performance measurements by management.

Adherence to controls is monitored through periodic management reporting of exceptions and production and transaction volume. Results of Nationwide’s operations are communicated to various levels of management and culminate in a monthly report. Management also conducts an annual review of the carved-out subservice organizations SOC 1 or SOC 2 reports, where they review the applicable third-party service provider’s SOC reports to review:

1. The service provider’s general IT controls to make sure they are addressed within the report and to review them for any potential deficiencies.

2. For any subservice organizations to determine if additional SOC reports are needed for review.

3. The service provider’s recommended user controls to make sure Nationwide has the necessary processes and controls in place.

Computerized Information Systems

Nationwide uses computerized information systems to process client and partner transactions. The supporting systems are comprised of internally developed solutions and vendor products for specific capabilities. These systems include the following:

- DCdirect (RPLink) – is a Java-based application allowing both online real-time and batch processing. DCdirect (RPLink) uses a batch flow to apply the majority of financial transactions. Nonfinancial and financial transactions, for which the price of the investment options is known, are processed real-time. Investment options include fixed and variable options provided by various financial institutions. Daily interfaces provide pricing information for the variable products while fixed pricing is calculated daily based on certain predetermined rate factors. DCdirect (RPLink) uses a combination of different online inquiry transactions to aid in customer's inquiries. Online update transactions are also available for plan level activity. DCdirect (RPLink) houses many accounts and processes large volumes of transactions while still meeting daily service level agreements. DCdirect (RPLink) interfaces with different systems to facilitate User Entity record keeping and provides daily reports, which support transaction activity.

- Interactive Voice Response (IVR) – IVR provides participants, via their touch-tone phone, the ability to review their account balance and current investment allocation information. It also gives them the ability to change their future investment allocation and process exchanges.

- Retail Service Center (RSC) – RSC provides participants and plan sponsors with a variety of plan and individual participant level information, including balances and current investment allocations. The RSC allows input of participant enrollments, participant demographic changes and participant exchange and investment allocation change transactions.

- RIA Managed Accounts Transaction Management System (Public) –TMS (Public) is an Oracle Reports and PL/SQL based application that provides omnibus level modeling and trade capability of portfolios of mutual funds, a fee calculating engine, and reporting. The application allows both online real-time and batch processing. TMS (Public) is used by Nationwide Investment Advisor ProAccount for managing 457 plans participant investments.

- NRS Imaging & Workflow (NRS Imaging) - Document Intake and Distribution Solutions receives, scans, and indexes multiple types of media (paper, email, and faxes) into NRS Imaging & Workflow for Nationwide Financial. Each business unit sets their own prioritization of documents based on batch types. At the point of indexing, requests are assigned more specific transaction types which allows transactions to flow to the appropriate Public Sector processing team.

- NWFIN Enterprise GL (General Ledger) - NWFIN Enterprise GL is the Enterprise financial book of record. Enterprise source systems send financial data to the General Ledger, and on-line financial transactions are recorded. The General Ledger is used for reconciliation of cash transactions applicable to the recording of investments.

- PMTS – The Payments System is used for the processing of disbursements. These can be checks, Digital, ACHs, or Wires. PMTS is responsible for creating, tracking, and reporting on all payments issued by the Nationwide Financial administration areas listed: Financial Operations, Commissions, Individual Investment Products, Nationwide Advisory Solutions, Nationwide Life, Nationwide Financial Network, Claims, Payouts, Pensions, and Public Sector Retirement Plans.

- RPS 6 – Income Products annuity policies, including Individual Annuities, Deferred Comp, annuitized 401K, Defined Benefit and Defined Contribution, Group, NW Agents, Annuity Trust, and Single Premium, are supported by RPS 6. The system provides real-time update of Deferred policy information and input of nonfinancial and financial transactions, which are processed in batch.

- Taxport – Accumulates withholding amounts to prepare tax Forms 1042S, Puerto Rican 480.6 and 1099.

- Taxcalc (Client/Server) - Taxcalc (C/S) is a Unix tax calculator that calculates Federal, and State Income Tax based on the withholding rules established by the IRS and state governments. Taxcalc (C/S) runs a daemon process that waits for requests and returns FIT and/or SIT amounts to the calling system.
- UV Cloud (UVC) – A variable product asset management and unit value pricing functionality platform. UVC calculates unit values and provides prices to Nationwide administration systems each business day. Additionally, UVC is an intermediary between Nationwide and National Securities Clearing House and is used to execute trade orders interfaced from the respective Nationwide administration systems. Also, UVC is utilized to reconcile shareholder account activity between fund houses, the G/L, and administration systems. Last, UVC calculates fund performance to report downstream to the various lines of business and provides fund of fund administration capability.
- Frontier - A third-party vendor tool hosted on Nationwide Amazon Web Services (AWS) environment. Frontier is an automated reconciliation and reporting system. The purpose of Frontier system is to make it as easy as possible to match monetary items, resolve outstanding items, generate reports, and reconcile accounts. By using this system to interface with our internal source and general ledger systems, it reduces the time spent matching items to determine outstanding reconciling items. The tool is also used for fraud prevention. By sending current check status information to the bank on which checks are available for cashing.
- AWD-10 NF - Automated Workflow Distribution, an imaging and workflow application for the independent channel used by Retirement Solutions. AWD 10-NF (AWD) – is a vendor application owned by SS&C, licensed to Nationwide Financial, and being configured for use by Retirement Solutions for managing the workflow related to processing financial and non-financial transactions. AWD interfaces with DCdirect (RPLink), NF's record-keeping application for Retirement Solutions, and FileNet, via APIs. It produces and consumes Kafka events for messaging and alerting. Participant-facing applications, such as RSC (Task Center and Status Tracker), access AWD workflow information through APIs, as well.

The following describes the general controls surrounding the in-scope applications.

Program and System Software Change Control

Software changes are prepared by the development team using the several version control tools:

- Changeman for RPS6 and Mainframe change (JCL) for PMTS
- GitHub and UrbanCode Deploy (UCD) for AWD-10 NF, DCdirect (RPLink), and PMTS
- GitHub and Harness for Retail Service Center, NRS Imaging and TaxCalc (C/S)

- Phire for NWFIN Enterprise GL
- *DCdirect (RPLink), Interactive Voice Response (IVR), and TMS (Public)*

Nationwide has documented change and emergency change management standards that describe the process for requesting and executing changes to the production environments.

For operational changes, a request is initiated by the Business Analyst (BA), an application member, or a business customer by entering information into the ServiceNow Request Tool. A Delivery Leader is assigned, and the work is prioritized and scheduled by collaboration of the Delivery Leader, Software Engineering Product Manager (SEPM), Break-Fix (BF)/Walk-Up (WU) Lead, BA, and Customer Manager.

For TMS (Public), a request is initiated by the business consultant on behalf of an end user, operations team member, or a business customer by submitting a Work request form by email which is received by the AVP, Nationwide ProAccount, and Operations Director. The work is accepted, prioritized, and scheduled through collaboration with the AVP, Nationwide ProAccount, Operations Director, and Software

Engineering Product Manager (SEPM) during the monthly project prioritization meeting or ad hoc meetings as needed.

Once work is approved, a ServiceNow Change Request (CHG) is completed by the developer or Release Manager. The CHG is submitted as soon as work begins on the change and an implementation date is finalized. The CHG captures information regarding the change: summary of change, description of change; contact information; implementation window; impacts to customers during implementation, after install, and postponement of change; installation strategy; back-out strategy; verification strategy; and classification of the change (e.g., minor, significant, major) as well as lines of business impacted. Each CHG is then assigned a developer. For TMS (Public), once work is approved, the work begins on the change and an implementation date is tentatively targeted.

The software design is prepared by the development team through iteration story cards. Coding and unit testing are performed once the design document has been approved. For TMS (Public), the functional/technical requirements are prepared by the development team through iteration story cards. Coding and unit testing are performed once the requirements have been approved. Version control packages are used to facilitate the development, testing, and implementation process. If developers are making changes to production code, they must create one or more branches in the version control software. Production code is checked out into these branches and the developers make their changes to the code. Once created, the branches are promoted into the testing environment by the developers for unit, system, and acceptance testing. Version control packages installed into Production must be installed in the testing environment first. Branches must also be approved by the developer before installation into Production. The BA is responsible for conducting and recording acceptance testing. If there are no discrepancies between the expected test results and the actual test results, the developer sends an e-mail to the BA group, describing the changes made and asking for their approval to implement. The BA replies to indicate approval. For TMS (Public), changes are validated by both the Quality Engineer as well as acceptance testing, which is completed and recorded by the Business application owner (BAO) or another person from the business. If there are no discrepancies between the expected test results and the actual test results, the developer provides an implementation plan, and the overall deployment process begins.

In the event that a change needs to be inserted into the monthly project release, after the release scope or code freeze has passed, a CHG needs to be completed online by the developer interested in making the change. The developer completes the form with information regarding the application area, environment, change type, application name, approver, description of the change, effective date and time, server name, CHG number, and comments/instructions. When selecting the approver, the system automatically provides the developer’s manager and that manager’s manager as choices. The developer also has the option of selecting another approver.

Once the request is completed and submitted, the selected approver is notified of the request via e-mail. The approver is responsible for reviewing the request and approving or rejecting the request. The developer is notified of the status of the request (i.e., approval, assignment, completion, etc.) via e-mail during the entire process. For TMS (Public), Business approval is also received via the BAO.

Once the request is approved, the developer making the change completes an Implementation Specification form. This document outlines the modules that have changed as well as procedures to install and verify any version control package changes. The following people must review and approve/sign the form before the change is migrated into the production environment:

- Document Author – for all changes
- Document Reviewer – for all changes
- Business Manager – for changes that affect business users only
- BF/WU Lead – for operational changes only
- Delivery Leader – for project changes only
- SEPM – for all changes

The changes are migrated to production by a designated individual or team which does not have development responsibilities. The specific teams are application or platform specific. Once the changes are installed, the CHG status is updated to closed. For operational changes, the CHG is also closed.

For TMS (Public), when the request is approved, the developer making the change or Tech Lead completes an Implementation Specification form. This document outlines the modules that have changed as well as procedures to install and verify any version control package changes. The following people must review the implementation plan document before the change is migrated into the production environment:

- Document Author – for changes
- Document Reviewer – for changes

This documentation is used as input to the Release Management team as they will open up a change request through Service Now, establish a change window, and receive appropriate approval from the Change Activity Board (CAB). Once deployment is scheduled, post implementation validation ticket is created in ServiceNow and assigned to the team. Once the changes are installed, post-implementation validation is performed and then the CHG status is updated to closed.

PMTS

All changes fall into one of the following categories: operational changes or project changes. For operational changes, a request is initiated by the Business Analyst (BA), an application member, or a business customer by entering information into ServiceNow Request Tool. The change is prioritized, and work is scheduled by collaboration of the Business Application Owner (BAO) or application steering team, Agile Leader, Software Engineering Product Manager (SEPM) and team leads.

For projects, changes are initiated by the Line of Business or the Business Support Services (BSS) Account Team. A Project Manager (PM) is assigned, and the work is prioritized and scheduled by collaboration of the BAO, PM, Agile Leader, and SEPM.

If the developers are making client/server changes to production code, they must create one or more GitHub (change management software) branches. Production code is checked out into these branches, and the developers make their changes to the code. Once created, the branches are promoted into the IT testing environment using the UrbanCode Deploy (UCD) tool by the developers for unit testing. Branches are promoted into the ST (staging) environment by the developer for System Testing. Developers can always demote branches from ST to IT if changes need to be made. GitHub branches with the changes are installed into all testing environments. There are three environments: IT (development), ST (staging), and PT (pre-production). Once the tester successfully tests the change, the tester schedules a sign-off meeting with the Business sponsor who provides an approval for installation into Production. Business sponsor will also provide appropriate approval in the CHG itself.

In addition, as part of the client/server deployment process, a task for IDOC within the CHG needs to be created online by a developer making the change. The developer creates the task with information regarding the installation of the change, effective date and time, server name, CHG number, and comments/Instructions (such as the URL of the UCD deployment). IDOC then approves the UCD deployment.

If developers are making mainframe changes to production code, they must create one or more ChangeMan (change management software) packages. Production code is checked out into these packages, and the developers make their changes to the code. Once created, the packages are promoted into the testing environment using the ChangeMan tool by the developers for testing. Once the tester successfully tests the change, the tester schedules a sign-off meeting with the Business sponsor who provides an approval for installation into Production. Business sponsor will also provide appropriate approval in the CHG itself.

Once the Business sign off is received, the developer making the change completes an Implementation Specification form. This document outlines modules that have changed as well as procedures to install and verify any changes for the effort. The following people must review and approve/sign the form before the change is migrated into the production environment:

- Document Author – for all changes
- BAO or delegate – for changes that affect business users only
- System Tech Lead – for all changes
- PM – for project changes only
- SEPM – for all changes

Once work is approved, a ServiceNow Change Request (CHG) is completed by the developer for operational changes. The CHG captures information regarding the change: summary of change, description of change, contact information, implementation window, impacts to customers during implementation, after install, and postponement of change, installation strategy, back-out strategy, verification strategy, and classification of the change (e.g., minor, significant, major), as well as lines of business impacted.

In addition to the approval of the implementation plan, the SEPM, BAO, Team Test Lead and Peer reviewer must complete tasks within the CHG.

Once the changes are installed, the CHG status is updated. For operational changes, the ServiceNow request is also closed when applicable.

Taxcalc (C/S)

Nationwide has documented change and emergency change management standards that describe the process for requesting and executing changes to the production environments.

For operational changes, a request is initiated by the Tax Unit within NF Financial Operations by entering information into the ServiceNow Request Tool. The Tax Unit assesses the changes (including possible consultation with legal and the business units) to determine the impact of the changes. It is then determined if the changes are to be made by Financial Operations and / or Financial Systems.

The software design is prepared by the development team through iteration story cards and if changes are made by FinOps team they conduct their own process to complete the change. Coding and unit testing are performed once the design document has been approved. Version control packages are used to facilitate the development, testing, and implementation process. If developers or FinOps are making changes to production code, they must create one or more branches in the version control software. Production code is checked out into these branches and the developers / FinOps make their changes to the code. Once created, the branches are promoted into the testing environment by the developers for unit, system, and acceptance testing. Version control packages installed into Production must be installed in the testing environment first. Branches must also be approved before installation into Production via CHG.

The Business Product Owners and IT(Systems) Resources teams are responsible for conducting and recording acceptance testing. If there are no discrepancies between the expected test results and the actual test results, the FinOps Business Lead will conduct a review meeting describing the changes made and asking for their approval to implement. The Business Product Owners and IT(Systems) Resources teams replies to indicate approval. The following people must review and approve/sign the form before the change is migrated into the production environment:

- Document Author - for all changes
- Document Reviewer - for all changes
- Business Product Owners - for all changes
- SEPM - for all changes

Once work is ready for implementation a ServiceNow Change Request (CHG) is created by the developer for changes. The CHG captures information regarding the change: summary of change, description of change, contact information, implementation window, impacts to customers during implementation, after install, and postponement of change, installation strategy, back-out strategy, verification strategy, and classification of the change (e.g., minor, significant, major), as well as lines of business impacted.

In addition to the approval of the implementation plan, the SEPM, BPO (Business Product Owners) and Team Test Lead must complete tasks within the CHG.

The changes are migrated to production through Harness. Once the changes are installed, the CHG status is updated to closed. For operational changes, the CHG is also closed.

NRS Imaging

NRS Imaging & Workflow is custom Java Swing and PL/SQL code stored in a GitHub repository. This code is built into a Java application and deployed to the desktop using Java WebStart. Web Services are deployed using Harness pipeline. Production deployments are controlled by the standard ServiceNow Change Request (CHG).

NWFIN Enterprise GL

For NWFIN Enterprise GL, Code versioning, change management and deployment is handled by a Peoplesoft-specific change management software package named Phire. The code deployment process is handled through a series of steps requiring approvals. Each user is assigned a role within Phire that limits his/her rights to certain steps. Only associates with the appropriate role can execute a specific step. Developers can migrate through test environments except for PT (pre-production) with approval from the testing team. Only administrative users can move code into production during a specific release window.

Retail Service Center (RSC)

Nationwide has documented change and emergency change management standards that describe the process for requesting and executing changes to the production environments.

For operational changes, a request is initiated by the Business Analyst (BA), an application member, or a business customer by entering information into ServiceNow Request Tool. A Project Manager (PM) is assigned, and the work is prioritized and scheduled by collaboration of the PM, Application Owner Break-Fix (BF)/Walk-Up (WU) Lead, BA, and Customer Manager.

Once work is approved, a ServiceNow Change Request (CHG) is completed by the developer or Release Manager. The CHG is submitted as soon as an implementation date is finalized. The CHG captures information regarding the change: summary of change, description of change; contact information; implementation window; impacts to customers during implementation, after install, and postponement of change; installation strategy; back-out strategy; verification strategy; and classification of the change (e.g., minor, significant, major) as well as lines of business impacted.

The software design is prepared by the development team through iteration story cards. Version control software is used to facilitate the development, testing, and implementation process. If developers are making changes to production code, they must create one or more branches in the version control software and the developers make their changes to the code in the branches. Before branches can be merged back into the main branch automated code quality checks must pass. Once completed, the branches are merged into the master from which artifacts are created and pushed into the testing environment by the developers for unit, system, and acceptance testing. Successful verification in the testing environment is required before changes can be installed into Production. Harness pipelines are used to automate code deployment.

The RSC application is being transformed from monolithic application to micro frontend which allows multiple lines to work on the app with less coordination in releases.

RPS 6

RPS 6 software changes are prepared by the development teams using the ChangeMan version control tool to create a change package. The Tech Lead reviews and approves at the first level in ChangeMan, all changes that are to be promoted to Beta for testing. The changes are promoted to Beta, by submitting a service request using the ServiceNow Request Tool.

When changes are ready to migrate to production, a ServiceNow Change Request (CHG) is prepared, which is used to coordinate changes across the enterprise. In addition, to engage the 7x24 Production Services team, a service request is prepared using ServiceNow. The request identifies the package to be moved to Production and is used to obtain and log IT and Business approvals for the change. The CHG provides a list of preselected approvers. When the form is completed and the user clicks on the submit button, the selected approving personnel are notified of the request via Microsoft Outlook. Once approved the approval status, date, and time are recorded and maintained as part of the ServiceNow request, and the request is sent to the 7x24 Production Services team.

The 7x24 Production Services team ensures that the CHG have been approved and are complete before approving ChangeMan at the highest level. This approval allows the promotion of the changes to Production on the install date and time coded within the package. After code has been migrated, validation of the CHG is performed by the development teams.

AWD 10-NF

For operational changes, a request is initiated by the Business Lead or a business customer by entering information into the ServiceNow Request Tool. A Project Manager (PM) is assigned, and the work is prioritized and scheduled through collaboration of the PM, Application Owner, Agile Leader, and Project Team.

Once work is approved, a ServiceNow Change Request (CHG) is completed by the Agile Leader. The CHG is submitted as work is being completed on the change and an implementation date is finalized. The CHG captures information regarding the change: summary of change, description of change; contact information; implementation window; impacts to customers during implementation, after install, and postponement of change; installation strategy; back-out strategy; verification strategy; and classification of the change (e.g., minor, significant, major) as well as lines of business impacted. Each CHG is then assigned a team.

If the developers are making changes to production code, they must create one or more GitHub (change management software) branches. Production code is checked out into these branches, and the developers make their changes to the code. Once completed, the branches are merged into the master from which artifacts are created and are promoted into the testing environment using the UrbanCode Deploy (UCD) tool by the developers for unit, system, and acceptance testing. The Business Lead is responsible for conducting and recording acceptance testing. If there are no discrepancies between the expected test results and the actual test results, the development team sends an e-mail to the Business Team, describing the changes made and asking for their approval to implement. The Business Lead replies to indicate approval. Successful verification in the testing environment is required before changes can be installed into Production. Final release management approval is required within UCD before changes can be installed into Production.

Once the request is completed and submitted, the approver is notified of the request via e-mail. The approver is responsible for reviewing the request and approving or rejecting the request. The team is notified of the status of the request (i.e., approval, assignment, completion, etc.) via e-mail during the entire process.

Logical Access

Passwords

Password requirements are governed by a corporate-wide management-approved policy at the network and application levels. Before accessing any application, access to the network must be obtained. Passwords have minimum length, complexity, and uniqueness restrictions. Additionally, default passwords created are required to be changed upon first log on.

The Password policy standards are clearly communicated to employees as they are updated over time to maintain the integrity of data. All user-level and system-level passwords must conform to the standards established at the time for password strength.

Access Administration

Addition and Modification of Access

DCdirect (RPLink), TMS Public, AWD 10-NF

Nationwide has a documented and formalized policy in which Access Control is assigned based on predefined roles with access granted with enough permissions to perform job responsibilities.

Nationwide Associates are only provisioned the access necessary to do their jobs. A centralized, automated tool SailPoint IIQ (IIQ) is leveraged to manage the life cycle of an ID, and to enforce least-privileged access. The IIQ tool integrates with our HR and Directory systems. These tools work in conjunction to enforce identity, authentication, authorization, auditing & accountability.

Access to provision IDs is handled through a centralized ID administration team which is separated in roles and functional access from those who can provision access. For TMS(Public) User Access Request Form is submitted for any RIA role access.

Newly provisioned access must be reviewed and approved within the tool by the People Leader prior to permissions being granted and IDs being created. For TMS(Public), the user access request form must be approved by users' people leader).

If an Associate transfers departments, their access is required to be reviewed within the IIQ tool by the new hiring manager prior to the Associate beginning the new role.

People Leaders are required to complete access reviews of their direct reports on a quarterly basis.

Privileged access to record-keeping applications is tightly monitored using a Privileged Identity Management Tool (PIDM).

The IIQ tool is integrated with our HR and central directory systems to immediately revoke access upon termination.

Regarding physical security, the employee's badge access to enter the building is also revoked.

Frontier

To gain access to the Frontier application, a user must first have a valid Nationwide Active Directory (NWIE) ID. Users authenticate to the Frontier system utilizing Nationwide Single Sign On and access their accounts with their NWIE IDs. In addition to a valid NWIE ID, users must have a Frontier application ID and role. Frontier access requests are initiated via SailPoint IIQ. Approvals are required by the manager of the requestor for access and the Reconciliation Technology & Governance business group and the Identity Lifecycle Management and Governance (ILMG) group grants access.

For employees who no longer require application access, and management wants the access removed before the review process, management can submit a SailPoint IIQ request and access will be removed by the ILMG group.

NWFIN Enterprise GL

NWFIN Enterprise GL access requests are initiated via SailPoint IIQ. Approvals are required by the manager of the requestor for access as well as a secondary business SME approval. Once both approvals are received, an automated process assigns the role to the user. The Identity Lifecycle Management and Governance (ILMG) group also have the ability to grant the access manually should the process fail.

Access levels, Update, or Inquiry authority is determined by the roles assigned to a user ID and those roles contain permissions that allow specific authority within the General Ledger.

NRS Imaging and Workflow

NRS Access requests are initiated via SailPoint. Approvals are required by the manager of the requestor for access as well as a secondary business SME approval. The user is added to the authorized roles by the automated process within SailPoint IIQ in response to this request. The team supervisors, then uses the user configuration tools to add the user to the appropriate workflow queues and job specific roles.

PMTS

To gain access to the PMTS application, a user must first have a valid Nationwide Active Directory (NWIE) ID within Nationwide. Once a NWIE ID is created, that user must have a valid Oracle ID, specifically for the application's database. The access request must be submitted via IIQ and approved by Business Manager prior to provisioning. There are several security roles within PMTS, and each user is assigned one or more security roles.

A user logs in with his/her NWIE password, and the password follows the rules for Single Sign-on passwords. Users are automatically logged-off the database after a predetermined length of inactivity. In addition, users can have no more than two concurrent sessions of the PMTS application open.

It is the responsibility of the user's manager to have access revoked for employees who are leaving or transferring using SailPoint IIQ.

RPS 6

To gain access to the RPS 6 application~~s~~, a user must first have a valid Nationwide Active Directory (NWIE) ID. The system administrator creates and assigns user IDs. Users access their accounts with their NWIE ID. This sign-on password must adhere to Nationwide rules for Single Sign On password for RACF IDs. Once a NWIE ID is created, a RACF ID must also be created. The password for the RACF ID is synchronized with the NWIE ID. File permissions for RPS 6 as it relates to the user role are granted to the RACF ID through a CICS Group Connect request. Both creation of the RACF ID and file permission assignment are handled by the RACF team.

Once a RACF ID is created, that user must have a valid RPS 6 ID, specifically for the application. The IT Manager or Business Manager must submit a ServiceNow Request that is sent to ILMG group. This request includes the user and security role for the system; there are several security roles within RPS 6 defining which screens a user may access and/or update. The ILMG group is responsible for setting up the RPS 6 user ID for the access requested. The ILMG group will notify the user as well as the approver once the user's access has been set up.

It is the responsibility of the IT Manager (for IT employees) or Business Manager (for business employees) to submit requests to remove access when their employees leave, transfer or no longer need access to RPS 6, or to request any needed changes in access.

RSC and IVR access by plan providers and participants

Plan participants and Sponsors can manage their accounts in the RSC system. They use their access IDs and passwords, which are verified against an enterprise repository. The participant can create a username and a password, and the process is supported by system prompts and system help messages. A password must be alphanumeric, and the account is suspended after five invalid logon attempts. Plan participants can access their information via IVR using their Account Number and unique PIN. If a PIN is not already established, participants can create a PIN within the IVR, when prompted, by entering a valid date of birth. A participant and a plan sponsor can also call in to the support team and have a team member provide services for them.

For enrollment and online account creation, the phone numbers are validated using an ANI match process utilizing Neustar. This service checks whether the phone number and address match that of the account holder information.

Taxport

Access requests are submitted via the IIQ tool. Approvals are required by the manager of the requestor for access as well as a secondary business SME approval. If a user has Basic access, they can only view and print a tax form. An advanced user can view, print, modify, and create a tax form. Advanced users also require a 2nd level of approval granted only by the Financial Operations Tax Unit.

It is the responsibility of business unit management to notify the application security administrators of employees leaving or transferring positions. Additionally, when an employee is marked as terminated in the Human Resource application, their internal NWIE ID is automatically disabled, revoking network access.

Nationwide Associates are only provisioned the access necessary to do their jobs. IIQ is leveraged to manage the life cycle of an ID, and to enforce least-privileged access. IIQ integrates with our HR and Directory systems. These tools work in conjunction to enforce identity, authentication, authorization, auditing & accountability.

UVC

To gain access to the UVC application, a user must first have a valid Nationwide Active Directory (NWIE) ID within Nationwide. Users authenticate to the UVC system utilizing Nationwide Single Sign On and users access their accounts with their NWIE ID. In addition to a valid NWIE ID, users must have a UVC application ID and role. The ILMG group creates user IDs and assigns roles within the UVC application.

New user requests are currently submitted via the IIQ Tool. Approvals are performed in an automated fashion within IIQ. Once the necessary approvals are obtained a member of the ILMG group sets up the new user account in the UVC application.

- For business employees who need a change in user access, an IIQ Request is submitted. Approvals are performed in an automated fashion within IIQ. Once the necessary approvals are obtained a member of the ILMG group updates the user account in the UVC application.
- For employees who no longer require application access, an IIQ Request is submitted, and approvals are performed in an automated fashion within IIQ. The ILMG group will process the request and lock the user ID.

Removal of Access

Upon termination of employment, an employee’s badge access to enter the building is revoked and HR notifies IS to remove associated system access. Network access is removed upon notification. Then the ILMG group uses a termination checklist that identifies a series of steps to confirm logical access is sufficiently removed. The annual revalidation process verifies the accuracy of access.

Review of Access

PMTS, NWFIN Enterprise GL, DCdirect (RPLink), Taxport, IVR, RSC, NRS Imaging & Workflow, RPS 6, UVC, AWD-10 NF, Frontier, and TMS (Public)

The above applications use the SailPoint IIQ application to facilitate and monitor regular management reviews of user access rights. Two types of reviews are processed within the IIQ application.

On a quarterly basis IIQ initiates a manager review of direct reports.

In addition, IIQ also initiates an individual review of access when an employee transfers to a new manager.

During the review process, managers can identify inappropriate or unneeded access and a request is generated and sent to the ILMG group to have the access changes, locked or removed.

For PMTS and Taxport, during the review process, managers can identify inappropriate or unneeded access and a request is generated in IIQ to have the access removed automatically.

In addition, NWFIN Enterprise GL and RPS 6 have implemented secondary review processes.

- For NWFIN Enterprise GL, PeopleSoft access controls are in place and reviewed monthly to determine valid access for NWFIN Enterprise GL.

For RPS 6, on an annual basis, Nationwide Financial Individual Product Solutions Operations does an annual user and role review.

Physical Access

Data Center North (DCN)

Production and Development systems are housed at the Data Center North (DCN), which is a Tier IV facility located in Lewis Center, Ohio. The low-profile building was constructed to withstand 250 mile-per-hour winds. No signs explicitly identify the building as a Nationwide data center. A security fence surrounds the entire building. Security cameras surveying the grounds are monitored by the security officer on duty.

Nationwide’s Corporate Security is responsible for the card key system and an officer is onsite 24x7x365. The glass wall of the security office located in front of the building is bullet proof. The officer monitors physical access, gates, video cameras and alarms. The card key system is configured to log each use. A hardcopy of the log is printed out at the security desk and is reviewed by one of the third shift security officers every day to ensure all access is removed from ID Badges. External doors are equipped with alarms that are monitored and access to the building is restricted by card key.

For permanent badge access to DCN, an email request approval by the On-site Support Manager or Team Lead is needed. Access levels are programmed into the card key system according to the job functions performed. There are 18 access levels which can provide access per room/space. Temporary badges are issued by the security officer and must be returned upon leaving. The security officer keeps a record of all temporary badges issued.

A monthly permanent badge access report is generated and reviewed to determine if any change is needed. Badge access is immediately disabled from terminated personnel. Along with Security staff, IT Onsite Support analysts and CRE building engineers are onsite 24x7x365.

Visitors who are not DCN employees are required to sign in and out at the security desk and must have a valid ServiceNow Request Item (RITM), Incident (INC) or CHG (with a RITM attached). All IT personnel/vendors must sign into iVisitor for all work beyond the office area. All CRE vendors performing work on the raised floor must also sign into iVisitor. Cleaning crews are contractors and must have a valid RITM to enter each day to perform their work. Access will be added by Security when they arrive and removed when they leave.

Computer Operations

Job Scheduling and Job Monitoring

Job scheduling procedures are documented and include procedures for job scheduling, job monitoring, and error handling.

Nationwide uses an automated job scheduler for applications residing on their servers. The ability to modify schedules is restricted to appropriate users. Incidents in the ServiceNow tool are used to communicate and track timely resolution of incidents, problems, and errors.

The automated job scheduler tool allows for the scheduling and execution of jobs across all platforms at Nationwide (Linux/Unix, Windows, and Mainframe). Jobs run at varying times and days based on calendar functionality and can execute based on dependency structures, not just time, such as file monitors, predecessors, and resources.

The tool provides a set of alerting mechanisms that can track jobs that are failing to execute, running too long, not executing, etc. This is used in tandem with BigPanda to create incidents in ServiceNow when failure/alert states occur, which are then routed to the appropriate teams for support. This ensures that the teams responsible for addressing issues are engaged and that there is historical tracking of when incidents occurred and how they were handled.

Retail Service Center (RSC)

The flow of data through the RSC begins with a customer accessing the corresponding Nationwide website. At the Nationwide site, the user selects the participant account option and is taken to the customer login screen. New participants can call to request this type of web access to their accounts or complete the setup access request on the website. They must provide their Social Security number or tax ID number, date of birth, and account number. Once this information is authenticated, the user is prompted to select a username and password. The password is case sensitive. The username must be unique. The account will be suspended after five invalid password attempts. The user must wait 20 minutes after the last unsuccessful attempt or call the Customer Service Center to get his/her password reset. A Customer Service Center Representative will perform the required user authentication procedures prior to resetting the user password.

Users must follow security standards to access Nationwide Retirement Plans information on the website. One of the security standards is encryption. RSC uses 256-bit encryption for transactions between the user and the website and between the website and the firewall. The session is terminated due to inactivity with any browser.

Once the username and password have been authenticated, the user can review account summaries and statements for past quarters, review fund performance, change user ID and/or password, and perform various types of exchanges and future allocation changes. User access is limited to the participant's own account(s). The Social Security number or tax ID number is an additional unique identifier, thus preventing unauthorized users from viewing any accounts other than their own. If a user has multiple accounts, he/she is prompted to select the account he/she wishes to access from the list of identified accounts.

Users can request loans and withdrawals through the Internet. If elected, users receive a confirmation via U.S. Mail for changes made to their account. If an address change is made, the confirmation is sent to the old address.

System Backups

The application owners and business management determine the backup schedule for each application commensurate with the risk of data loss based on the users' needs and criticality of the system. Operations personnel are responsible for ensuring that the backup schedule that is established is executed. Backup procedures have been documented which include processes for adding new backups, scheduling backups, and monitoring of backup jobs. If a scheduled backup job abends, the monitoring system automatically generates a problem ticket. The operations personnel then take necessary action to resolve the issue.

Approximately 95 percent of backup jobs are stored on a de-duplicated disk storage system. Offsite copies are automatically replicated to the reciprocal data center to provide an offsite copy. The remaining 5 percent of backup jobs are written to local SAN disk and then duplicated to two copies of tape. The primary copy is stored in a robotic tape silo in the primary data center. The second copy is transmitted to the remote reciprocal data center over secure links and written into a duplicate robotic tape silo. Backup tapes maintained on-site are stored within physically secure data centers.

PMTS

The Oracle databases for PMTS use the Nationwide standard database backups process Oracle's RMAN utility is used to write data from the database to Cohesity.

Production is also available in Disaster Recovery using Data Guard. This provides High Availability capabilities by shipping archive logs (change logs) from the production database in the DCN to a disaster recovery database in a secondary data center. This process will ship a log every 12-15 minutes or if the log is filled.

NWFIN Enterprise GL

Data for NWFIN Enterprise GL is replicated using Oracle DataGuard.

RPS 6

The RPS 6 nightly flows use mid-flow and post-flow jobs to back up the VSAM files. Also, the key feeds to and from RPS 6 are saved into generation data group (GDG) backup sets with multiple generations available. Backups created by the ADRDSSU utility are kept for 30 days. Some RPS 6 files also have monthly, quarterly, and year-end versions available. Year-end backups have a retention of 400 days.

NRS Imaging and Workflow

Standard nightly Oracle backups are performed for the NRS database. In addition, the database is in an Exadata environment for data redundancy and is replicated to a secondary data center.

Data Center

The computer room contains the following:

- Network and distributed computing hardware
- Console and peripherals
- Communications equipment
- Electronic media
- Power distribution units
- PBX
- Air conditioning units

PMTS, NWFIN Enterprise GL, IVR, NRS Imaging and RPS 6 production systems all reside at the DCN.

The DCdirect (RPLink) production systems primarily reside at the DCN. A small subset of RPWS (web service) code now resides in the AWS cloud.

The Taxcalc (C/S) production systems all reside on the Cloud Native Platform (CNP).

The RSC production systems and Frontier all reside at the NW-AWS.

The RIA TMS (Public) production systems all reside within the Nationwide Virtual Private Cloud (VPC) hosted via AWS.

The Storage Services department at Nationwide determines the backup schedule based upon on the users' needs.

Backup standards, procedures, and guidelines are documented and available online. Critical tables, reports, statements, files, and transactions are backed up daily and available online for immediate recovery and/or regeneration. Critical information is also backed up to disk on a daily, weekly, and monthly basis. Full system backups are performed weekly. Backups are stored at an alternate data center. Database activity is logged to allow for roll forward and roll back procedures. Database logs are copied from online files to disk when the online files are full.

Transaction Processing

New Plan Setup

New plan documents are received by a New Business Analyst, who then completes a pre-production checklist to verify that the correct documents have been signed and are in good order. The New Business Analyst then sets up the plan on the recordkeeping system according to the documentation received.

After the new plan has been set-up, in pending status, the Pre-production Checklist and associated plan documents are passed to a second New Business Analyst for Quality Control (QC) verification and sign-off. If the second New Business Analyst finds an error, it is noted on the QC Checklist and the plan setup documents are passed back for correction. Once the error is corrected, the Pre-Production Checklist, and plan setup documents are passed back through QC to the second New Business Analyst for verification that the correction has been made.

Upon QC completion, the pending plan is activated on the recordkeeping system. The New Business Analyst then completes the contract issuance process. Once the entire New Plan Setup process is complete, the New Business Analyst forwards the completed Checklist and plan set-up documents to management for review and validation that all process steps were completed. Management reviews the documents and electronically signs the Pre-production Checklist. The management reviewed Checklists and documents are then uploaded to the contracts repository and imaging system.

Fund Release

Fund Releases are pre-scheduled and consist of multiple types of fund related transactions. Relationship Consultants (RC) or Business Leads follow the intake process which includes completing an Intake Form on the Fund Release SharePoint Site. The RC or Business Lead will attach the supporting documents to the Intake Form. The Financial Services Team transcribe the required information from the Intake Form into the Scope Document for any of the following: fund additions, fund restrictions and/or closures, price conversions, and future date fund mapping. The Financial Services Team will send an email for Scope Verification to the Plan RC or Business Lead. The RC or Business Lead will verify that the information from the Intake Form has been transposed into the Scope Document correctly and reply to the email, verifying that the information in the Scope is correct. Financial Services will date the Scope Summary tab of the Scope with the date the RC or Business Lead replied. The Scope Document is an excel tool used to communicate the fund release activity to the various impacted teams in a concise manner with necessary approvals from each team involved in the release.

To ensure fund entry into DCdirect (RPLink) is complete and accurate, a secondary Plan Analyst performs a Quality Control (QC) review of the Intake Form, supporting documents, Scope Document, and fund data entry on DCdirect (RPLink). Both the Plan Analyst completing the DCdirect (RPLink) fund data entry and the secondary QC Plan Analyst authorize the fund addition sheet via annotating the good order on the Scope Document.

NRS plans impacted by a mass fund release appear on a corresponding system report the day after the release takes place. The report systematically displays all monetary exchanges in/out of DCdirect (RPLink) funds included on the fund release and provides the Financial Services Team with an additional validation step ensuring all monetary amounts (whether debits or credits) were completely and accurately migrated from one fund to another as listed on the DCdirect (RPLink) Fund Release Scope Document.

Participant Enrollments

Participants typically enroll using a Participation Agreement (PA) which can be remitted via employer, plan representative, or mail, fax, email to Imaging Services or to the plan administration home office for manual account setup.

New business applications are received by Imaging Services, where they are date and time stamped and imaged. They are then forwarded to the New Business Team for processing. The New Business Processor reviews the new business application to ensure it is in good order (name, address, date of birth, etc.). If the new business application is not in good order, the New Business Processor will key an Incomplete Enrollment in the RPLink website (DCdirect - system) and then forwards the business application to the appropriate department, Not In Good Order (NIGO) Team, who will try to collect the missing information. The NIGO Team Processor will reach out by phone call, email, and letter. If the (NIGO) Team Processor is not able to obtain the necessary information, the transaction will be closed.

Once the new business application is determined to be in good order, the New Business Processor enters the relevant information in RPLink (DCdirect). At the completion of entry, the system is configured to list error and warning messages, which can then be addressed by the New Business Processor before submission. The enrollment is immediately processed, and the account is established on the system. Samples of the applications are forwarded to the Quality Assurance (QA) Processor, who reviews the New Business Processor's work and verifies that data entries are correct. Nightly, the RP Link (DCdirect) system applies any purchases received prior to the input of the form and generates the application confirmation letters, if elected, to the participant and plan sponsor. Each day, the issue resolution team is required to review the RPLink (DCdirect) Daily 1061 Error Report for errors.

Contributions/Receipts

Each business day, money associated with retirement plan contributions is received by NRS in one of three forms:

- Checks
- Wires
- Automated Clearing House (ACH)

Checks are remitted either via the Direct Deposit Account (lockbox) with the bank or via U.S. Mail/Overnight Mail.

Receipt of Checks via Lockbox

Certain plans remit retirement plan contributions and payroll documents to a designated lockbox. The bank deposits the checks into the bank account. The bank then remits one copy of the checks, check detail (Advice of Credit and Batch Detail Listing) and the payroll documents via courier to the Payroll Team. A processor reviews the payroll documents sent by the bank with each deposit and verifies that deposits listed on the Advice of Credit and Batch Detail Listing are received and accurate.

The processor then creates a Manual Receipt on RP Link (DCdirect (RPLink) system) via the Create Receipt screen.

Receipt of Checks via the U.S. Mail/Overnight Mail

Certain plans remit retirement plan contributions to NRS via U.S. Mail or Overnight Express Mail. Imaging Services receives and opens mail and places a "For Deposit Only" stamp on the back of each check. A log of checks received is prepared by Mail Services. The log and checks are then remitted by Mail Services to a Check Processor in the Retail Service Center. After receiving the checks, the Check Processor restrictively endorses, and photocopies checks for that day's deposits. The Check Processor then prepares a deposit ticket and forwards the deposit ticket, checks and log to a QC Processor for review. After approval from the QC Processor, the deposit tickets and checks are returned to the Check Processor who is responsible for remitting them to Treasury Services via courier twice daily.

Receipt via Wire/ACH

Treasury Workstation will pull the Incoming Wire Report three times a day (10:00 a.m., 2:00 p.m., and 4:00 p.m.) from the bank's website, and automatically creates receipts for the wires on DCdirect (RP Link). The Payroll Processor will identify the wires/ACH's daily to ensure that the correct plan information is used with the RP Link receipt. The processors will search the unresolved screen to match the wire/ACH with any corresponding detail files that have come through electronic or manual submission.

All Contribution Receipts

Each business day, the detail supporting retirement plan contributions is remitted to NRS in hardcopy format via a lockbox, U.S. Mail, or Overnight Mail. Imaging Services receives and opens all mail. Hardcopy detail is remitted from the bank or Mail Services, or Imaging Services depending on who initially received the detail, to the Retail Service Center Payroll Team for processing. Alternatively, the plans can fax retirement plan contribution information to the Document Solutions team.

Once the deposit receipt information and corresponding retirement plan contribution detail is received by the Retail Service Center Payroll Team, a Payroll Processor reconciles the receipt information with the retirement plan contribution detail. If the retirement plan contribution detail entered into DCdirect (RP Link) does not balance to the receipt information, DCdirect (RP Link) will place the information in an unbalanced status until the discrepancy is resolved. Information that is "in balance" according to DCdirect (RP Link) is assigned an effective date. DCdirect (RP Link) updates the participant accounts using the information from the nightly batch processing. A Financial Transaction Register (FTR) report is generated by RP Link after the nightly flow. The FTR report shows that the total dollars received on DCdirect (RP Link) were processed in the system. These balancing procedures are performed by the Financial Service Representatives in the reconciliation area to ensure that deferrals are processed or placed in a suspense account.

Financial Operations personnel perform cash reconciliation on both a daily and monthly basis. Monthly reconciliations are reviewed by management within 25 business days of month end and signed off as evidence of approval.

Daily, the Not in Good Order (NIGO) Team will review the 1174 Purchase Unresolved Report to identify unprocessed deferral contributions. This report is used to monitor the timeliness of processing contributions against internal time standards (same day for contributions). Any unprocessed batches are assigned to a Processor to review, investigate, and resolve the unprocessed payrolls. Calls made to the entity to resolve the unprocessed payrolls are documented by the designated Processor. The Team Manager or Team Lead later reviews the report to verify with the Processors that the unbalanced payroll batches are being researched by a Processor. Also, the Processor will note any calls to the plan sponsor to resolve problems on the batch header.

Payroll deferrals that do not have an exact match on the DCdirect (RP Link) system are sent to the "Suspense Account" for various reasons, such as the entered Social Security number/plan sponsor number combination does not exist on the system, the account is at a closed or restricted status, or the life insurance premium exceeds the total deferral amount. Suspense reconciliations are performed daily and are distributed to Team Managers.

Each of the Suspense Account items must be researched and identified, and the final resolution must be made by the sixth day. Individual suspense tickets are delivered to the processing teams by the Internal Control Unit each day, and the 1176 Purchase Suspense Aged Open Items Report shows unresolved suspense items for regions to date. This report is reviewed daily by the processing teams to identify and clear suspense items. Open items older than 30 calendar days are distributed to NRS management on a weekly basis via email to ensure timely clearing.

The Reconciliation Processor validates wires were entered on RP Link and uses the Financial Transaction Report (FTR), 1174 Purchase Unresolved, and 1176 Purchase Suspense Aged Open Items Report to identify any outstanding issues. The Reconciliation Processor then enters dollar amounts from the outstanding issues on the reconciliation as an open item.

A payroll analyst pulls a random sample of payroll participants processed in the previous week to quality check (QC) for good order.

Withdrawals/Disbursements

Withdrawals

Participants can withdrawal funds from their retirement account using one of the following options:

- Annuitization
  - Purchased Annuity
- Systematic Withdrawal
  - Fixed Payment Systematic
  - Fixed Period Systematic
  - Required Minimum Distribution
- Immediate Payout (partial or total)
  - Termination
  - Retirement
  - Required Minimum Distribution
  - In-Service
  - In-Service Rollover
  - Testing Refund
- Unforeseeable Emergency/Financial Hardship
- Outgoing Funds to Another Carrier
  - External Plan to Plan Transfer
  - External Plan to Plan Rollover
  - Purchase of Service Credit
  - Insurance Premium Payment
  - In-Service Rollover
- Beneficiary/Alternate Payee
  - Beneficiary due to death
  - Alternate payee due to QDRO
  - Required Minimum Distribution due to Beneficiary

How Distribution Requests Are Received, Processed, & Quality Checked

An account holder can request a distribution form by:

- Contacting the Solution Center who will either email, fax, or mail out a form
- Contact the local office (if applicable)
- Visiting the NRS or plan website

Once the account holder completes the hardcopy distribution form, it can be returned via mail, fax, or email. All returned forms are received in Document Intake and Distribution Solutions who then scan the distribution forms into AWD. Upon receipt of the distribution form, a NRS Distribution Processor completes an "In Good Order" (IGO) review. If the request is deemed IGO, the request is processed and sent via AWD to the QC or Balancing location and is either quality checked by a Balancing Processor or sent directly to file. If a discrepancy or error is noted, the Balancing Processor will forward the request in AWD, back to the original processor to correct the transaction who will correct & reprocess the request. If a discrepancy is not noted, the Balancing Processor will forward the request in AWD to close. Transactions sent directly to file are done so systematically based on a Processors QC Sampling rate. If the request is deemed "Not In Good Order" (NIGO), the request is sent via AWD to the NIGO location and a NIGO Processor works to resolve the issue.

An account holder can also request a distribution via phone:

- Over the Phone (OTP)

The account holder contacts the Participant Contact Center to initiate an OTP request (must meet plan & participant requirements including the request must be no more than $10,000 or 95% of balance maximum and have a previous hardcopy distribution form on file). After verification of security information, the PCC Representative will obtain the distribution information over the phone and complete an OTP worksheet completing all fields. Once complete, the worksheet is scanned into AWD. If the request is deemed IGO, the request is processed and sent via AWD to the QC or Balancing location and is either quality checked by a Balancing Processor or sent directly to file. If a discrepancy or error is noted, the Balancing Processor will forward the request in Imaging, back to the original processor to correct the transaction who will correct & reprocess the request. If a discrepancy is not noted, the Balancing Processor will forward the request in AWD to close. Transactions sent directly to file are done so systematically based on a Processors QC Sampling rate. If the request is "Not In Good Order" (NIGO), the request is sent via AWD back to the PCC representative to resolve/clarify the issue.

Annuitization

The Income Products Service Center (IPSC) is responsible for maintaining the account information and making future payments for participants electing a purchased annuity option for payout (annuitization). Purchased payments is a lump-sum distribution from the plan moving the assets to the IPSC, with the future distributions made from the Repetitive Payment System 6 (RPS 6). For purchased annuities, the Annuity Purchase Distribution Form is received in NRS Imaging. The NRS Distribution Team reviews the request for IGO requirements & emails a copy of the form to IPSC via email. The IPSC team builds a processing request in Views for the participant. The IPSC Processor establishes the customer account and then enters the annuitization information contained on the payout election form on RPS 6. The setup in RPS 6 and the rate calculation is reviewed by Quality Control for accuracy. This review is evidenced by the reviewer by annotating the request in Views. Once the account has been established in RPS 6, the IPSC Processor sends an email to the NRS Processor requesting the account to be surrendered from the system.

The NRS Distribution Processor completes an IGO review, and if deemed IGO the request is processed by the NRS Processor in DCD and sent via Imaging to the Balancing location and is quality checked by a Balancing Processor. If the request is deemed "Not In Good Order" (NIGO), the request is sent via Imaging to the NIGO location and a NIGO Processor works to resolve the issue.

The day following the processing of the request in DCD, a manual wire payment for the amount of the distribution is set up in PMTS by the NRS Distribution Processor. The wire is created in PMTS and the detail is scanned into Imaging and forwarded to the Manual Payment location to be quality checked and approved/denied by a lead/manager. After the payment is sent, the NRS Processor sends an email advising IPSC the distribution was processed, and wire sent. The email includes the participant's name, SSN, effective date, and total amount liquidated.

The IPSC team will add the premium to the RPS6 system and calculate the benefit payment. The first annuity payment will then cycle and be issued on PMTS.

After the initial annuity payment with IPSC, reoccurring payments will be processed automatically. Once approved, the checks will be printed and mailed by Document Services. Once the first benefit payment commences, the benefit election cannot be changed.

A RPS 6 report identifying the expected checks from RPS 6, along with a PMTS report that identifies the checks that were processed is produced daily. These reports are reviewed as part of the balancing process daily. Those payments will include monthly, quarterly, semi-annual, and annual payments depending on the payment frequency elected by the participant.

Unforeseeable Emergency/Financial Hardship

Participants may request a distribution due to an unforeseeable emergency or financial hardship.
Upon receipt of a UE/Hardship application, the NRS Distribution Processor reviews the request for IGO requirements, including verification that the UE or hardship reason meets the IRS & plan specific guidelines. Supporting documentation is reviewed to help make the determination.

If the request is IGO, the request is processed in DCD or RP Link and sent via AWD to the QC location and is quality checked by a Balancing Processor.

If the request is "Not In Good Order" (NIGO), the request is sent via AWD to the NIGO Processor to resolve the issue. If additional information/confirmation from the participant is received within 30 days, the request will be re-reviewed for IGO requirements.

If the request is denied, the request is sent via AWD to the NIGO Processor who advises the participant of the decision via phone call, mail, or fax.

Overview of the Distribution Process

Payout requests are initiated through a paper application and with evidence of termination of employment. Once the payout terms are established and the participant takes an initial withdrawal of at least $25 by form, the participant can call at any time and request additional amounts from their established payout terms assuming the amount is up to $10,000 but not more than 95% of the account value. The participant can also call to change periodic payment amounts and processing dates.

For over the phone requests the customer service representative verifies the participant's name, SSN, DOB, and address. Once they have verified the account for security, they will then verify the initial distribution request was done via paper, and that the plan is eligible for this payment request. If the participant is eligible the customer service representative completes the request form with all the necessary information and submits it through Imaging for review in the processing department.

For other payout requests, the processor determines that the participant's name, address, and Account Number/Social Security Number agrees to information included on the system. Unless a plan instructs otherwise, the processor also reviews the date of birth to help ensure the request meets minimum distribution requirements governed by the Internal Revenue Code. The processor checks the participants' tax elections. Finally, the processor checks to see if the waiver of notice box has been initialed on the request form. This means that the transaction will be entered on the system with a future effective date. The processor accesses the system and enters the payee and distribution information for immediate payments, outgoing funds to another carrier, in-service withdrawals, and financial hardships. Once the transaction is entered the Balancing Processor will QC the transaction and generates the system report. The Balancing Processor reconciles withdrawal requests as reported on the systems. The Balancing Processor's name is automatically entered onto each withdrawal request on PMTS after review. If a discrepancy or error is noted, the Balancing Processor will forward the request using Imaging, back to the original processor to correct the transaction. Once the correction is made, the request will be reviewed by the manager (in the case of a manual check) or the balancer again if the error was created on the system. Once the transactions have been balanced, the balanced report is passed to the Manager for approval. Requests are approved online and evidenced by the manager's name being automatically entered onto each withdrawal request after review on PMTS. Payout election forms are then remitted to "closed" in the AWD System. Items that are processed on the system, but not on PMTS appear on reconciliation reports. Items in error during the interface between the system and PMTS are identified on the 511D PMTS Report and referred to Distribution or Loan/UE Teams for resolution.

Disbursements

Withdrawal payments (disbursements) can be issued in one of four formats:

- Manual check
- Operations check
- ACH
- WIRE A wire is also used to transfer funds to the IPPSC account when an annuity is purchased

Payment via Manual Check

Manual checks are used in certain situations (e.g., payments to those with a foreign address, and instances where corrective processing must be performed). For manual checks, the withdrawal information is entered on PMTS. A manual check request is prepared and imaged by the Disbursement Team Processor. The manual check request, along with the withdrawal request detail from the system, is given to the manager for review and approval. The manual check request and detail is then forwarded to Treasury Services. The Treasury Services Processor accesses PMTS and validates the payee and amount is correct and that the account balance is sufficient to cover the request. The check is then prepared and logged according to the method of delivery that will be used (regular mail, overnight, or pick-up by a NRS Processor). The checks will be mailed directly from Treasury Services or the mailroom to the designated recipient. After a batch of manual checks has been printed, a Treasury Services Disbursement Accountant compares the PMTS system report, which lists the checks requested with the check log, which shows checks printed. Any discrepancies between the number of checks requested and the number of checks printed is followed up by the Treasury Services Disbursement Manager.

Payment via Operations Check

Operations checks are those checks electronically approved in PMTS and automatically sent through the system to be printed in the Document Services print shop for mailing unless special mailing instructions are involved. A file is transmitted from PMTS to the Document Services print queue.

Infrequently, a check is destroyed in the printing process and an email is sent to Treasury Services, who voids the check on PMTS. The void is then passed to the business line to reissue the check.

For both manual and operations checks, there is an electronic signature in the system. Once a check request has been approved in the system, the system allows the electronic signature to be printed on the checks.

Payment via ACH or Wire

For manual ACH or Wire requests, a Treasury Services Accountant reviews for proper authorization and approves the request electronically. PMTS will then create and send a transmission file to the bank.

All Disbursements

Cash reconciliations are performed on a daily and monthly basis both by the Reconciliation Team and Treasury Services personnel. Monthly reconciliations are reviewed by management within 25 business days after month end, and initialed as evidence of approval.

Exchanges/Investment Election Changes

From time to time, participants and plans may wish to exchange funds or change the way future contributions are allocated to investment options. Participants can exchange funds or change their allocation mixes via the methods listed below. Plan Sponsors can also elect to add or delete funds offered within the plan through the fund mapping process which is separate from the methods listed below. Each business day, NRS receives exchanges/investment election changes from User Entities in one of three formats:

- Telephone
- Retail Service Center (RSC)
- U.S. Mail or Facsimile

Via Telephone

The telephone exchange and investment election change request process enable participants to call NRS' Customer Service Center on a recorded line and transfer money from one investment fund to another (in the case of an exchange) or change the manner in which certain future participant contributions will be allocated (in the case of investment election changes).

Participants can prompt out of the Interactive Voice Response (IVR) to a Customer Service Representative to perform these transactions.
If utilizing the IVR system, the participant is prompted to enter his/her Account Number and personal identification number (PIN) before the participant can access any account information or perform any transactions.

Transactions are entered into the system and confirmed with the participant. A QC review is completed on all exchanges greater than or equal to $200,000 for trades that are facilitated by a licensed CSR. Trades completed by the IVR do not go through the review process. Additionally, if elected, participants receive a confirmation of the exchange and/or investment election change by mail.

Via RSC

The RSC allows access to DCdirect (RPLink) from the Internet. The RSC allows participants to access current fund balance information, make changes to future investment allocations, and allows the movement of participant funds between investment options. The RSC feeds the system daily. Participants, if elected, receive a confirmation of the exchange and/or investment election change made via the web through the mail.

The RSC transactions and data in the system are protected with a combination of routers, servers, a network firewall, and transaction encryption methods. Unique participant information is required to gain access to the RSC and to establish an Internet account and password to that account. Once the account is established, a personal password is required to gain access.

RSC transactions use 256-bit encryption for transactions between the participant, the website, and the firewall for web browsers that support 256-bit encryption. After a period of inactivity with any browser, the session is terminated.

Via U.S. Mail or Facsimile

Hardcopy requests via U.S. Mail or facsimile are received by Imaging Services and are imaged and forwarded onto the Retail Service Center. A financial analyst will then process the requested exchange via the system. If elected, the accountholder receives a confirmation of the exchange and/or investment election change by mail.

A QC review is completed on all hard copy exchanges. Identified errors are monitored and resolved within five business days. Items may be pended for longer than five days provided research has been completed and documentation provided for the pended item. Team Leads and Managers monitor all errors daily to determine the status of each pending inquiry/item. Any exchange items needing retroactive investment processing must have management approval.

Investment Transactions

NRS provides full-service contract level of service, where NRS maintains participant records. Therefore, investment transactions are kept at the participant and plan levels.

Investment transactions that are the direct result of contribution, withdrawal and exchange transactions are entered onto the system upon receipt of notification from the account holder for participant level (full-service) contracts.

Variable Investment Options

Each day, typically before 4:00 a.m., DCdirect (RPLink) sends daily trade information to UVC. The interface feed received from DCdirect (RPLink) by UVC is balanced to the administrative feed received by the general ledger system. By 4:00 a.m., UVC notifies each Financial Operations staff member of the status of the National Securities Clearing Corporation (NSCC) flow. The UVC system is programmed to identify trades that can be processed through NSCC. NSCC allows trades to be initiated and settled in a timelier and cost-efficient manner (on a net basis) than manual fax order forms sent directly to the fund houses. By 6:15 a.m., UVC creates and sends a batch file to the NSCC of the daily trades. UVC automatically sends an e-mail notification to Financial Operations indicating that each line of business' NSCC trades were sent successfully. This alerts the staff if manual fax order forms need to be initiated for missed NSCC processing by an individual line of business. By no later than 9:30 a.m., the Financial Operations staff faxes the manual order forms to the fund houses that do not use NSCC. Around 10:00 a.m., manual wires are posted to PMTS, and the Disbursement Wire Totals Report and Manual Payment Summary Approval Sheet, after being signed by an authorized Financial Operations approver, are sent to Treasury Services for final approval and initiation of wires. The NSCC notifies UVC of the trades rejected as soon as they occur. This allows NRS to research and resolve any rejected trades in a timely manner. Confirmed or accepted trade notifications are received throughout the day from the NSCC. The final NSCC settlement information is received around 12:00 p.m., and an e-mail notification is sent to Financial Operations. After 12:00 p.m., the NSCC settlement information is balanced to the Cash Requirement Report, and settlement notification spreadsheet is completed and emailed to the bank and Treasury Services.

On a periodic basis (no less frequently than monthly), investment transactions with mutual fund houses are reconciled to mutual fund account statements by a Senior Accountant in Portfolio Accounting that is independent of the accountant placing the trades.

Fixed Investment Options

Each evening DCdirect (RPLink) updates the general ledger system for the cash associated with the fixed investments purchased and sold that day. A Senior Accountant performs monthly ledger reconciliations of fixed investments to the financial transaction information on the system, which includes deposits and withdrawals. In addition, a quarterly reconciliation is performed to ensure that the interface between DCdirect (RPLink) and the general ledger system is working correctly. This reconciliation involves an Accounting Supervisor verifying the fixed investment balances per the general ledger system to reports of fixed investment balances per the record-keeping systems. A Senior Accountant ensures that the fixed investment balances per this report agree to what was entered onto the Company's general ledger system.

Quarterly, valuation summaries are uploaded by NRS Systems Department to a website and then downloaded by the Actuarial Department. Either an Actuarial Analyst or a Senior Actuarial Assistant reconciles DCdirect (RPLink) valuation summaries to data obtained from the original source table data files. On a quarterly basis, a Senior Actuary approves the cash associated with the fixed investment data to be uploaded to the general ledger system by the Finance Department.

Unit Valuation

Both variable and fixed investment options are valued based upon unit values multiplied by the number of units held (i.e., an underlying investment option's unit value multiplied by the number of units held by the participant equals the value of the investment option). The change in unit value is calculated for each underlying mutual fund in a variable annuity contract and for each fixed investment option. These calculations are performed daily by the UVC system for variable investment options and DCdirect (RPLink) for fixed investment options. For variable investment options, an Associate in the Unit Value Accounting Department, independent of the Associate who entered the information into UVC, reviews a system-generated report of the data entry information for accuracy and evidence review by initialing the system-generated report. For fixed investment options, an Actuarial Assistant reviews interest earned monthly for reasonableness compared to the contract rate.

Both variable and fixed investment option unit calculations are equal to the previous day's unit value multiplied by a Net Investment Factor (NIF).

Variable Investment Options

The NIF for the variable investment option is calculated using the following formula: NIF = [(NAVt + Div + Cap Gains)/NAVt-1] – (□dys * Daily Admin Charge)

where

NAVt = The mutual fund's net asset value (NAV) at the end of today. NAVt-1 = The mutual fund's NAV at the end of yesterday.

Div = Dividends. Accumulated income distributed by the mutual fund at the end of today.

Cap Gains = Capital Gains. Distribution of net capital gains by the mutual fund at the end of today.

dys = The number of days since the last unit value calculation.

Daily Admin Charge = The daily administrative charge assessed by the contract.

Each evening, the Unit Value Accounting Department electronically receives the current day's dividend rate, capital gain rate, NAV per share and change in NAV per share by one of three ways. They receive them via email, through the NSCC or by FTP file from the fund house or agent. There are also some prices that may have to be entered manually.

Once prices are received by the UVC system, the system performs a series of control checks for accuracy. If any price fails the control checks it will suspend, (does not process) until the accountant researches the issue and validates the price received or makes any necessary corrections. As each price (including NAVs/Divs/CG) are processed and any suspended items are cleared, the UVC system calculates the current unit value using the above formula. UVC then interfaces with and updates the recordkeeping system with current unit values.

For prices entered manually an Associate in the Unit Value Accounting Department, independent of the Associate who entered the information onto UVC, reviews a system generated report of the data entry information for accuracy; this is evidenced by the Associate initialing the generated report. Once the information is input onto UVC, UVC calculates the current unit value using the above formula. UVC then interfaces with and updates the recordkeeping system with current unit values.

Dividend and Capital Gain rate information is received by the Unit Value area and entered into the UVC system. This information is then posted to UVC along with the NAV information. UVC then calculates the number of shares to be reinvested into the account. This is then reconciled by comparing outstanding share balance post Dividend or Capital Gain share reinvestment between UVC and what the fund house reports as their shares outstanding. All sporadic Dividends and Capital Gain are reconciled to the penny and the shares to the thousandths decimal place. For daily interest funds, by the fifth workday of each month, the Portfolio Accounting Area (PA) requests a Monthly Detailed Daily Dividend (Per Fund House Range) report. This report illustrates the daily dividend amounts that the UVC system has calculated for the General Ledger period. The PA will retrieve the Dividend information from the fund houses via NSCC electronic data, calling, monthly account statements, or DST Vision access. These amounts are written on the Monthly Detailed Daily Dividend report.

Any variances over the acceptable amount, $500, are researched by the PA. The accountant will verify that the daily Dividend rates and Record/Reinvest dates that the UVC system supplied agree to the fund house information. The accountant is independent of the Associate that entered the information onto VALU/UVC and of the Associate that placed the trades with the fund house.
Once Dividend is reconciled, the PA will input the information into the UVC system for monthly processing. The reconciliation is placed in a file evidencing the review.

Fixed Investment Options

The NIF for fixed investment option is calculated using the following formula:

NIF = $(1+ \text{Interest})^{1/N}$ where

Interest = The annual interest rate credited on the guaranteed return insurance contract which includes the guaranteed interest rate earned less any contract charges assessed

N = Number of days in the year

On the first business day of each quarter, the interest rate calculation for fixed investment options is electronically downloaded by a Senior Actuarial Analyst who reconciles the system valuation summaries to the data obtained from the original source data files. The data runs through the nightly flow and the system uses the unit value process to update the system with the current unit values.

For fixed investment options that may have interest rates change throughout the quarter, the Company Actuary will create a memo which orders a change in interest rate for that particular fixed investment option. This memo (which lists the fund #, daily factor, and the new interest rate) is then delivered to the Internal Control Team Manager, who reviews the memo for reasonableness. The memo is then given to an Accounting Clerk, who manually enters the change into the system. The data then runs through the nightly flow where the system updates the interest rate credited information maintained on the system. The following business day, the Internal Control Team Manager will compare the system with the memo to ensure the change was made. Any discrepancies are investigated and followed up by the Internal Control Team Manager.

User Entity Reporting

Statements

Participant and plan statements are generated from the record-keeping systems beginning on the first day following the calendar quarters. Prior to generating statements, files of statement data are received from outside providers and reviewed by the Statement Unit Team for good order. These files are reconciled against the system files and reports are generated to balance the data and to report unbalanced accounts.

The Statement Unit Team performs an audit ensuring financial transactions fields on the statement and funds available to the entity are properly being reported. These fields include beginning and ending balances, deferrals and incoming transfers, withdrawals and surrenders, exchanges, charges, and gain/loss on investments. In addition, nonfinancial data is verified including phone numbers and address. Also, fund performance is verified. Both participant and plan statements are included in the audit. Once verified, statements are released to be printed and to insert into statement envelopes. Systematic and manual controls are in place to ensure insertion quality and counts. An additional audit is performed on the statements loaded to the web prior to the release of the on-line statements for participant and plan viewing.

The control activities consist of the following:

An audit is performed by the Statement Team prior to the releasing of statements to be printed or loading to the web. The audit consists of verifying fund balances by calculating the unit values and verifying that the beginning balance agrees with the previous period's ending balance. They also ensure that financial transactions are included in the audit. The address and phone numbers, etc., are checked. An audit checklist is prepared and initialed by the processor and by a Unit Manager to ensure completeness of the audit. An OCR and Filebase/MRDR code are printed on each statement page to ensure page counts are accurate and the statement matches the mailing address.

Once the statements are inserted into envelopes, the NSC Quality Control Team performs a "Mailroom Audit." This consists of pulling statements at random, opening them up to ensure that statements are properly included, the correct postage is metered, the correct envelope is used, and the address presentation meets postal requirements.

Investment/insurance product provider data not accounted for by NRS is remitted electronically to the system. The information is received via teleprocessing, from the outside provider. The teleprocess file is received directly by the IT area. Once the data is identified as in good order, the reconciliation program runs and produces balanced and unbalanced reports, based on a comparison of the systems records to the carrier's records.

Tax Reporting

Taxpayer information is entered onto the record-keeping systems by processors from the participant's tax form or, in the case where no tax form is received, the tax information is defaulted by the system based on the withdrawal request. Payment information is then electronically fed to PMTS. PMTS electronically feeds Taxport the tax reportable YTD transactions monthly for the Internal Revenue Service (IRS) Tax Forms 1042S, Puerto Rican 480.6, and 1099 to be prepared. The 1099 print files are forwarded to the Printing and Document Services area; forms are created, printed, and the participant copy is mailed by Printing and Document Services before the IRS deadline. SOVOS prints and mails 1042S, Puerto Rican 480.6, and 1099 forms before the IRS deadline.

Monthly, the Finance Tax Reporting Unit generates rejection reports from Taxport for unusual withdrawal information electronically fed to it by PMTS. These rejection reports are forwarded monthly to the Internal Control Area to determine the nature of each unusual item. True discrepancies are forwarded to tax maintainers to be corrected. The Tax Coordinator reviews corrections made on discrepancy items and checks to make sure they are resolved within time standards prior to the release of the tax information.

The Tax Reporting Analyst reviews the following month's rejection report to ensure discrepancies were properly cleared. After the Tax Reporting Analyst reviews the report, it is submitted to the NRS Disbursement Manager. Since the exception reports are cumulative (i.e., error conditions remain on the report until corrected and/or cleared), the NRS Disbursement Team can review the report at year-end to determine if the necessary changes have been made to release the year-end tax information.

Complementary User Entity Controls

The controls described in the previous section cover only a portion of the overall internal controls supporting Nationwide's transaction processing. It is not feasible that all objectives related to a user entity's environment are achieved completely by Nationwide acting alone. Nationwide achieves some objectives (as indicated in Section IV) and contributes to others. Achievement of control objectives is accomplished through additional controls placed in operation and operating effectively at user entities. Therefore, a user's internal controls must be evaluated in conjunction with the controls of Nationwide and testing summarized in Section IV, "Nationwide Financial Services, Inc.'s Control Objectives, and Related Controls and KPMG LLP's Tests of Controls and Results of Tests."

This section describes additional controls that Nationwide has assumed in the design of its system that will be in place at user entities and are necessary for the achievement of the control objectives in this report. The control considerations presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User auditors should consider whether user entities have placed these controls in operation when understanding and evaluating the internal controls at the respective user entity.

Specifically, user entities should have controls in place to address the following:

Ref. #	CUEC	Related CO
01	User entities should have controls in place for timely review of reports, including tax reports and transaction confirmations provided by Nationwide of account balances and related activity, and written notice should be provided to Nationwide of discrepancies as compared with the user entity's record.	CO7, CO10, CO13
02	User Entities (or their Authorized Plan Representatives) should have controls in place for ensuring that participant enrollments are properly authorized.	CO7
03	User Entities (or their Authorized Plan Representatives) should have controls in place for maintaining adequate physical and logical security controls over on-site terminals with the capability to interface with Nationwide's systems.	CO2, CO3
04	User entities that utilize RSC should have controls in place surrounding user IDs and passwords established for account use.	CO4, CO10
05	User entities should have controls in place for reconciling the contributions made with the employer's records (and related billings), notify Nationwide of any differences, and provide Nationwide with additional funds where necessary.	CO8

Subservice Organizations

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

This section describes additional controls that subservice organizations should have placed in operation and are operating effectively for the achievement of the control objectives in this report.

Specifically, Nationwide has assumed the following controls in the design of their systems at the subservice organizations and are necessary to meet the control objectives:

Subservice Organization	Function	Complementary Subservice Organization Controls
TierPoint Data Center	Hosts the TMS (Public) system.	• Subservicer should have controls to ensure that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the TMS (Public) system. [Control Objective 3]
SOVOS	Hosts the Taxport system, performs all program changes and performs job processing and backups.	• Subservicer should have controls to ensure that changes to the Taxport system are authorized, tested, approved, properly implemented, and documented. [Control Objective 1] • Subservicer should have controls to ensure that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the Taxport system. [Control Objective 3] • Subservicer should have controls to ensure that administrative and operational procedures are established within the systems operations group to provide for complete processing of jobs, and backup and retention of systems and data as it relates to the Taxport system. [Control Objective 4]

Subservice Organization	Function	Complementary Subservice Organization Controls
Zinnia (formerly Convergent Financial Technologies and SE2)	Hosts the UV Cloud (UVC) system, performs all program changes, job processing and performs backups.	• Subservicer should have controls to ensure that changes to the UVC system are authorized, tested, approved, properly implemented, and documented. [Control Objective 1] • Subservicer should have controls to ensure that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the UVC system. [Control Objective 3] • Subservicer should have controls to ensure that administrative and operational procedures are established within the systems operations group to provide for complete processing of jobs, backup and retention of systems and data as it relates to the UVC system. [Control Objective 4]
Amazon Web Services	Hosts the Frontier and RSC systems.	• Subservicer should have controls to ensure that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to Frontier systems. [Control Objective 3]

Control Objectives and Related Controls

Nationwide's control objectives and related controls are included in Section IV of this report, "Nationwide Financial Services, Inc.'s Control Objectives and Related Controls and KPMG LLP's Tests of Operating Effectiveness and Results of Testing," to eliminate the redundancy that would result from listing them in this section and repeating them in Section IV. Although the control objectives and related controls are presented in Section IV, they are, nevertheless, an integral part of Nationwide's description of the system.

Section IV.

Management of Nationwide Financial Services, Inc.'s Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Testing

Control Considerations

KPMG's examination of the operating effectiveness of certain controls of Nationwide was restricted to the control objectives and the related controls specified by Nationwide in the "Testing Matrix" within this section and was not extended to procedures in effect at client locations or other controls that may be included in management's description of its system but not listed in the aforementioned matrix.

KPMG's tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the specified period. KPMG's tests of the operating effectiveness of specific controls were designed to conclude on the operating effectiveness of controls throughout the specified period, for each of the controls listed in the matrices in Section IV. In selecting particular tests of the operating effectiveness of controls, the following were considered: (a) the nature of the items being tested; (b) the types and competence of available evidential matter; (c) the nature of the control objectives to be achieved; and (d) the expected efficiency and effectiveness of the test. In addition, when using information produced by Nationwide, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Test procedures performed in connection with determining the operating effectiveness of controls detailed in the matrices in Section IV are described below:

Test Procedure	Description
Inspection	Inspected documents, reports, or electronic files that contain evidence of the performance of the control. This includes, among other things, inspection of client-directed documents, reading of reconciliations and management reports that age and quantify reconciling items, to assess whether balances and reconciling items are properly monitored, controlled, and resolved on a timely basis.
Reperformance	Re-applied the relevant control. This includes, among other things, reviewing reconciliations for proper sources of balances, reasonableness of reconciling items and accuracy of mathematical calculations.
Observation	Viewed the application of specific controls by Nationwide personnel.
Inquiries	Interviewed appropriate Nationwide personnel about the relevant controls.

Program and System Software Change Control

Control Objective 1:

Controls provide reasonable assurance that new applications and changes to existing systems are authorized, tested, approved, properly implemented, and documented.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
1.1	Change and emergency change management standards are documented, available and reviewed by management annually.	Inspected the Nationwide Change Management Policy to determine that the change and emergency change management standards were documented.	No Exception Noted.
		Inspected the Nationwide intranet to determine that the standards were available to employees.	No Exception Noted.
		Inspected the Document Information and Revision History sections of the IT Service Management Policy and IT Changes Management Process Owner Guide to determine that the standards were reviewed by management annually.	No Exception Noted.
1.2	System changes are developed and tested in separate environments before being implemented in production.	Inspected system evidence to determine that separate testing and production environments existed for each in-scope system.	No Exception Noted.
1.3	User access is administered such that users with application development roles do not have administrative level privileges to the production environment, including access to application configuration changes.	Inspected system generated listings of users with application development roles and users with privileged level roles to determine that users with application development roles do not have administrative level privileges to the production environment for each in-scope system.	No Exception Noted.

Control Objective 1:

Controls provide reasonable assurance that new applications and changes to existing systems are authorized, tested, approved, properly implemented, and documented.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
1.4	The Harness change tool is configured to require independent approval of changes prior to code promotion to the production environment.	Inspected the Harness configuration to determine that independent approval is required prior to promotion to the production environment.	No Exception Noted.
		Inspected a system generated listing of users with the ability to modify Harness configurations to determine that user's access was appropriate and segregated from users with development and approval privileges.	No Exception Noted.
		Observed an unapproved change request in Harness to determine that the system prevented selection of the install and promote actions.	No Exception Noted.
		Observed an approved change request in Harness to determine that the system allowed selection of the install and promote actions.	No Exception Noted.
1.5	The UrbanCode Deploy change tool is configured to require independent approval of changes prior to code promotion to the production environment.	Inspected the UrbanCode Deploy configuration to determine that independent approval is required prior to promotion to the production environment.	No Exception Noted.
		Inspected a system generated listing of users with the ability to modify UrbanCode Deploy configurations to determine that user's access was appropriate and segregated from users with development and approval privileges.	No Exception Noted.
		Observed an unapproved change request in UrbanCode Deploy to determine that the system prevented selection of the promote action.	No Exception Noted.
		Observed an unapproved change request in UrbanCode Deploy to determine that the system prevented selection of the promote action.	No Exception Noted.

Control Objective 1:

Controls provide reasonable assurance that new applications and changes to existing systems are authorized, tested, approved, properly implemented, and documented.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
1.6	The ChangeMan change tool is configured to require independent approval of changes prior to code promotion to the production environment.	Inspected the ChangeMan configuration to determine that independent approval is required prior to promotion to the production environment.	No Exception Noted.
		Inspected a system generated listing of users with the ability to modify ChangeMan configurations to determine that user's access segregated from users with development and approval privileges.	No Exception Noted.
		Observed an unapproved change request in ChangeMan to determine that the system prevented selection of the promote action.	No Exception Noted.
		Observed an approved change request in ChangeMan to determine that the system allowed selection of the promote action.	No Exception Noted.
1.7a	The GitHub Code Repository tool is configured to require independent approval of changes prior to code merger to the production environment.	Inspected the GitHub configuration to determine that independent approval is required prior to code merger to the production environment.	No Exception Noted.
		Inspected the GitHub Repository Settings to determine that repository administrators are unable to modify Branch Protection rules to override the independent approval configuration.	No Exception Noted.
		Observed an unapproved change request in GitHub to determine that the system prevented selection of the merge action.	No Exception Noted.
		Observed an approved change request in GitHub to determine that the system allowed selection of the merge action.	No Exception Noted.

Control Objective 1:

Controls provide reasonable assurance that new applications and changes to existing systems are authorized, tested, approved, properly implemented, and documented.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
1.7b	From 1/1/2023-7/30/2023 GitHub configuration logs are reviewed by management to verify branch policy override actions were appropriate for changes committed to the main branch.	Inspected management's review of Github Configuration logs to determine configuration changes are documented and approved.	No Exception Noted.
1.7c	The GitHub tool is configured to require independent approval of changes prior to code merger to the production environment.	Inspected the GitHub configuration to determine that independent approval is required prior to code merger to the production environment.	No Exceptions Noted.
		Observed an unapproved change request in GitHub to determine that the system prevented selection of the merge action.	No Exceptions Noted.
		Observed an approved change request in GitHub to determine that the system allowed selection of the merge action.	No Exceptions Noted.
1.8	Changes to system programs and configurations are authorized, tested, and approved prior to implementation into the production environment.	Inspected a selection of in-scope system changes to determine that management authorized each change prior to development.	No Exception Noted.
		Inspected a selection of in-scope application changes to determine that each change was tested and approved by IT, and, if applicable, the end user prior to implementation into the production environment.	No Exception Noted.

Logical Access

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
2.1	Passwords for in scope systems are configured according to password policies defined in the Access Control Standard including: • Password history • Account lockout • Length requirement • Password expiration • Password complexity	Inspected the Nationwide Access Control Standard to determine that enterprise information security standards were documented.	No Exception Noted.
		Inspected Active Directory SSO configuration to determine the in-scope systems that are configured to authenticate through Active Directory.	No Exception Noted.
		Inspected the Active Directory Default Domain Policy password configuration to determine that passwords were configured to comply with company policy.	No Exception Noted.
		Inspected the password configurations for the in-scope systems not configured to authenticate through Active Directory SSO to determine that passwords were configured to comply with company policy.	No Exception Noted.

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
2.2	Administrative accounts are assigned to a limited number of individuals who require those rights to perform their job responsibilities.	Inspected system-generated listings of in-scope application, operating system, and database administrators to determine that users on the list were authorized and access was appropriate based on the individual's job titles in Workday.	Exception Noted. Frontier 3 out of the population of 14 administrative users had inappropriate access to the Frontier accounting application. Management inadvertently provisioned administrator access as they believed the functionality would be needed to perform job responsibilities. DC Direct 2 out of the population of 19 administrative users had inappropriate access to the DC Direct application. One user changed roles and access should have been removed sooner to prevent them from having administrator capabilities post role change. The other user received access temporarily to complete testing, but the access should have been revoked at the completion of testing and was not. Additional Procedure 1: A lookback analysis was performed by management for the five user accounts and per analysis of the user access logs administrative access

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
			was not used by the five accounts.
Frontier Management Response: Management identified three contractors from Cognizant that had administrative access rights to Frontier Accounting. Administrative access rights to Frontier Accounting is reserved for the Identity Lifecycle Management and Governance (ILMG) group and contractors working with the team. To remediate this finding, the administrative access was removed for all three contractors prior to the finding being created. The remediation of this finding has been tested, validated and the finding has been closed. Management performed a lookback of the administrative access for all three contractors. Management's review of three contractors access logs identified that these users never used the administrative access function. **DC Direct Management Response:** Management identified two business users as having administrative access rights to the DC Direct application. To remediate this finding, Management removed the administrative access for both users. The remediation of this finding has been tested, validated and the finding has been closed. Management's review of the two users access logs identified that these users never used the administrative access function.			
2.3	Privileged Identity Management System (PIDM) is configured to grant users access to IDs for shared administrative privileges for a period of time and will automatically reset the password after 10 hours.	Inspected system-generated listings of in-scope application, operating system, and database administrators to determine that users on the list were authorized and access was appropriate based on the individual's job titles in Workday.	No Exception Noted.
		Inspected the PIDM Account Permissions web page for one in-scope user to determine that a user is only able to view and check out a password for IDs assigned to their Active Directory account.	No Exceptions Noted.

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
2.4	Manager Certifications are performed quarterly within the SailPoint IIQ system to validate application user access is appropriate based on roles and responsibilities.	For a selection of quarters, inspected the Manager Decision Report within SailPoint IIQ containing the population of users with access to the in-scope applications to determine that the access was reviewed by management.	No Exceptions Noted.
		For the population of changes identified in the prior test, inspected system generated evidence to determine that changes to access permissions noted by management were implemented.	No Exceptions Noted.
2.5	Shared ID entitlement certifications are performed quarterly to validate access is appropriate within the SailPoint IIQ system.	For a selection of quarters, inspected the Manager Decision Report within SailPoint IIQ containing the population of the shared IDs with access to the in-scope applications to determine that the access was reviewed by management.	No Exceptions Noted.
		For the population of changes identified in the prior test, inspected system generated evidence to determine that changes to access permissions noted by management were implemented.	No Exceptions Noted.
2.6		For a selected semi-annual review, inspected the PIDM group review, containing the population of users with access to the PIDM groups associated with the in-scope applications to determine that the access was reviewed by management.	No Exception Noted.

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
	Privileged Identity Management System (PIDM) group reviews are performed semi-annually to validate access to the associated shared ID is appropriate based on roles and responsibilities within the SailPoint IIQ system.	For the population of changes identified in the prior test, inspected system generated evidence to determine that changes to access permissions noted by management were implemented.	No Exception Noted.
2.7a	When a user submits a provisioning request in SailPoint IIQ, the system automatically routes it to the appropriate approvers and management provisions access as requested.	Inspected the provisioning approval workflow to determine that SailPoint IIQ user access requests are configured to route to the defined approvers.	No Exception Noted.
		For a selected user access request to an in-scope system, inspected system evidence to determine that the SailPoint IIQ access requests are automatically routed to the defined approvers.	No Exception Noted.
		For a selection of new users to in-scope systems, inspected access requests to determine that management approved the users before access was granted, and that access was granted as authorized.	No Exception Noted.
2.7b	When a user submits a provisioning request in SailPoint IIQ, the system automatically routes it to the appropriate approvers and provisions access as requested.	Inspected the provisioning approval workflow to determine that SailPoint IIQ user access requests are configured to route to the defined approvers.	No Exception Noted.
		For a selected user access request to an in-scope system, inspected system evidence to determine that the SailPoint IIQ access request was automatically routed to the defined approvers, and access was automatically provisioned as requested.	No Exception Noted.

Control Objective 2:

Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
2.8a	Work items in SailPoint IIQ are automatically created based on users’ termination date entered within Workday (for employees) or Boss (for contractors) to automatically de-provision Active Directory access and initiate the system de-provisioning process.	Inspected the terminated user workflow configuration to determine SailPoint IIQ creates de-provisioning work items and disables Active Directory access in accordance with the termination date from Workday/Boss.	No Exception Noted.
		For a selected terminated employee and contractor to an in-scope system, inspected system evidence to determine SailPoint IIQ automatically created a work item based on the users’ termination date from Workday/Boss and disabled Active Directory access.	No Exception Noted.
2.8b	Access privileges are disabled or removed for terminated employees and contractors in a timely manner.	For a selection of terminated employees and contractors to an in-scope systems, inspected termination work items and system access listings to determine that access privileges were disabled or removed within 14 days. .	No Exception Noted.
2.9	When a user changes roles within the organization, the new people leader must complete an Internal Transfer Certification review within 28 days to assess prior system access.	For a selection of transferred users from in-scope systems, inspected the Internal Transfer certification review to determine that new people leaders completed the access review within 28 calendar days of receiving the notification, or the user's prior non-birthright access was revoked.	No Exception Noted.

Physical Access

Control Objective 3:

Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
3.1	Physical access to the data center is restricted to users based on job responsibilities. Only approved users are granted access to the facilities.	Inspected Physical and Environmental IT Security Standard to determine that policies and standards were in place to govern physical access to sensitive areas, including data centers.	No Exception Noted.
		Inspected access requests forms for a sample of new hires that received access to the data center to determine that an access provisioning request was approved prior to access being provisioned.	No Exception Noted.
3.2	Access to the data center is reviewed monthly by management in accordance with documented policies/procedures.	Inspected a sample of monthly physical access security reviews to determine whether physical access to the in-scope facilities is reviewed and approved by management.	No Exception Noted.
		For the population of changes identified in the prior test, inspected physical access listings to determine that changes to physical access were implemented.	No Exception Noted.

Computer Operations

Control Objective 4:

Controls provide reasonable assurance that administrative and operational procedures are established within the systems operations group to provide for complete processing of jobs, and backup and retention of systems and data.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
4.1	Backups for key applications and databases are performed on a defined timeframe to mitigate the risk of data loss.	Inspected system-generated backup logs for in-scope applications to determine that backups were configured to run on defined timeframes.	No Exception Noted.
		Inspected backup failure configurations to determine that failures were routed to appropriate personnel for resolution.	No Exception Noted.
		For a selection of failed backups, inspected supporting documentation and backup logs to determine that failures were investigated and worked toward resolution.	No Exception Noted.
4.2	The ability to add, change, or delete jobs is restricted to computer operations personnel and is consistent with job responsibilities.	Inspected security files for job scheduling tools and job titles from Workday to determine that computer operations personnel with access to modify the jobs were appropriate based on the individuals job function.	No Exception Noted.
4.3	Computer operations, including job processing, are monitored to validate key tasks, scheduled jobs, and events, and expected outcomes are achieved.	Inspected the Nationwide Job Failure, Restarts & Reruns Procedures Job Aid to determine that instructions/information was documented for handling job abends.	No Exception Noted.
		For a selection of failed jobs, inspected supporting documentation and job rerun evidence to determine that failed jobs were investigated and worked toward resolution.	No Exception Noted.

New Plan Setup

Control Objective 5:

Controls provide reasonable assurance that new plans are approved by authorized individuals and processed accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
5.1	A Plan Analyst completes and authorizes a Pre-Production Checklist verifying required new plan documents are in good order, including that the document has been signed by the client and Nationwide personnel.	For a selection of new plan additions entered onto DCdirect (RPLink), inspected the corresponding plan documents to determine that an authorized person requested the new plan as evidenced by the Plan Analyst on the Pre- Production Checklist.	No Exception Noted.
		For a selection of new plan additions entered onto DCdirect (RPLink), compared the plan type, internal plan ID, and the legal name from the plan documents to that entered onto DCdirect (RPLink) to determine that the information matched.	No Exception Noted.
5.2	A secondary Plan Analyst performs a QC review using Pre-Production Checklist and QC Checklist also verifying required new plan documents are in good order.	For a selection of new plan additions entered onto DCdirect (RPLink), inspected corresponding Pre-Production Checklists to determine that a secondary Plan Analyst performed a QC review of the Pre-Production Checklist and QC Checklist for good order prior to activating the plan on DCdirect (RPLink).	No Exception Noted.

Fund Release

Control Objective 6:

Controls provide reasonable assurance that changes to funds are accurately documented, approved, and tested as part of a corresponding fund release.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
6.1	Fund addition/change activity is documented on an Intake Form and approved within the Fund Release Scope Process Document by Plan Relationship Manager.	For a selection of fund releases, inspected Intake Forms to determine that the fund additions/changes included within the fund release were documented and approved within the Scope Process Document.	No Exception Noted.
6.2	Fund additions are documented, and QC reviewed for accuracy upon being entered onto DCdirect (RPLink).	For a selection of new fund releases, inspected the corresponding Fund Release Scope Document to determine that fund additions were authorized, and QC reviewed by an independent processor prior to the fund release date.	No Exception Noted.
		For a selection of fund additions included in a Fund Release, compared the fund ticker, plan name and internal ID that were entered onto DCdirect (RPLink) to the Fund Release Scope Document to determine that the information matched.	No Exception Noted.
6.3	Fund changes are tested by reconciling inflows and outflows immediately after the funds are transferred and approved as part of the fund release process.	For a selection of new fund releases, inspected corresponding DCdirect (RPLink) Health Check reports on the day after the fund release to determine that reconciliations of inflows and outflows between funds were performed.	No Exception Noted.

Participant Enrollments

Control Objective 7:

Controls provide reasonable assurance that new participant enrollments are approved by authorized individuals and processed accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
7.1	Participant Agreement (PA) enrollment forms are completed and authorized by the participant.	For a selection of new participant enrollments on DCdirect (RPLink), inspected Participant Agreement (PA) forms to determine that they were completed and authorized by the enrolling participant.	No Exception Noted.
		For a selection of new participant enrollments on DCdirect (RPLink), compared the participant's name and address on the Participant Agreement (PA) enrollment form to the name and address listed on DCdirect (RPLink) to determine that the information matched.	No Exception Noted.
7.2	Participant Agreement (PA) enrollment forms are reviewed by a New Business Team member for "good order" data entry.	For a selection of enrollments, inspected the AWD Workflow tool to determine that participant data entered onto DCdirect (RPLink) by a New Business Team member was in good order as evidenced by electronic approval.	No Exception Noted.
7.3	The AWD Workflow tool is configured to send 25%, 50%, 70%, or 100% of transactions to a secondary QC reviewer for New Business Team members based on the team member's experience.	Inspected the configuration within the AWD Workflow tool to determine that it was configured to send transactions to a secondary QC reviewer based upon one of the noted percentages for new business team members.	No Exception Noted.
		For a selection of enrollments designated for a QC review, inspected the AWD Workflow tool to determine that participant data entered onto DCdirect (RPLink) by a New Business Team member was QC reviewed as evidenced by electronic approval.	No Exception Noted.

Control Objective 7:

Controls provide reasonable assurance that new participant enrollments are approved by authorized individuals and processed accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
7.4	DCdirect (RPLink) edit checks prevent enrollments from being processed with an invalid SSN, address format, enrollment attempts over 100%, and to an invalid or terminated account.	Observed the entry of four transactions (invalid SSN, invalid address, enrollment attempt over 100% and an invalid or terminated account) to determine that DCdirect (RPLink) edit checks rejected the transactions.	No Exception Noted.

Contributions/Receipts

Control Objective 8:

Controls provide reasonable assurance that contributions/receipts are recorded completely and accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
8.1	Daily, the Recon Team reconciles deposits processed on DCdirect (RPLink) versus what was processed on the General Ledger. Month end reconciliations are reviewed and approved by Management.	For a selection of months, inspected a selection of month-end "40 CASS" reports to determine that the reconciliations were performed and NRS management approved the reconciliation.	No Exception Noted.
8.2	Weekly, a random sample of payroll contributions are QC reviewed for the previous week's transactions.	For a selection of participant payroll contributions compared the payroll amount entered in DCdirect (RPLink) to the incoming check (from the Plan Sponsor) and supporting participant detail to determine that the information matched.	No Exception Noted.
		For a selection of participant payroll contributions, inspected the NRS Workflow tool to determine that a payroll analyst QC reviewed the contribution data entered onto DCdirect (RPLink) as evidenced by electronic approval.	No Exception Noted.

Withdrawals/Disbursements

Control Objective 9:

Controls provide reasonable assurance that withdrawals/disbursements are properly authorized, completely, and accurately processed, and recorded in a timely manner.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
9.1	A Distributions Processor reviews Distribution Forms received from participants for good order prior to the distribution being entered onto DCdirect (RPLink).	For a selection of participant distributions, inspected the NRS Workflow tool to determine that each withdrawal option selected was reviewed for good order by a Distributions Processor prior to the withdrawal being entered onto DCdirect (RPLink) as evidenced by electronic approval.	No Exception Noted.
9.2	For death payouts, a Distributions Processor reviews Distribution Forms received from beneficiaries for good order prior to the distribution being entered onto DCdirect (RPLink).	For a selection of death payouts, inspected the NRS Workflow tool to determine that Distribution Processors reviewed the payout for beneficiary authorization as evidenced by electronic approval.	No Exception Noted.
		For a selection of death payouts, re-performed the good order review by comparing the beneficiary’s name on the distribution form to the name listed in DCdirect (RPLink) and comparing the death certificate to the participant’s name in DCdirect (RPLink) to determine that the names matched.	No Exception Noted.
9.3	A daily balancing reconciliation between aggregate participant withdrawals listed in DCdirect (RPLink) and aggregate participant distributions to be initiated within PMTS is performed by a Distributions Team member and QC reviewed by a Distributions Manager.	Inspected a selection of daily balancing approval sheets to determine that aggregate participant distributions within PMTS were reconciled to aggregate participant distributions listed in DCdirect (RPLink) by a Distributions Team member and QC reviewed by a Distributions Manager.	No Exception Noted.

Control Objective 9:

Controls provide reasonable assurance that withdrawals/disbursements are properly authorized, completely, and accurately processed, and recorded in a timely manner.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
9.4	A quarterly review of access and distribution limit authority to PMTS is conducted by user and IT management. Exceptions are identified, investigated, and resolved timely.	Inspected a selection of PMTS user access reviews to determine that management, on a quarterly basis, reviews the list of users with access to the application and their respective distribution limit authority.	No Exception Noted.
9.5	A Distributions Agent compares manual payment information entered into PMTS to the disbursement request for accuracy and authorization and evidences the review by signing the Request Form.	For a selection of participant withdrawals, inspected disbursement payments to determine that they were authorized by an agent (with an adequate distribution limit authority) on the Nationwide Distributions Team.	No Exception Noted.
9.6	A Treasury Services Accountant performs a review of manual payment requests by comparing payment information entered into PMTS to the disbursement request for accuracy and reviews the approving agent to verify they have an adequate approval limit for the request. The Treasury Services Accountant evidences the review by signing the Request Form.	For a selection of participant withdrawals, inspected disbursement requests to determine that they were authorized, and QC reviewed by a Treasury Services Accountant - as an acting Distributions Manager.	No Exception Noted.
		For a selection of participant withdrawals, compared the manual distribution amount to the amount in PMTS to determine that the distribution was entered correctly into PMTS.	No Exception Noted.
9.7	A Print Operator performs a daily comparison of the actual number of check sheets fed to the expected check sheet fed number and evidences review by authorizing the Balancing Report.	For a selection of days, inspected Balancing Reports to determine that the Report was authorized by a Print Operator and actual sheets fed and printed amount total matched to the expected sheets fed and expected printed amount total.	No Exception Noted.

Control Objective 9:

Controls provide reasonable assurance that withdrawals/disbursements are properly authorized, completely, and accurately processed, and recorded in a timely manner.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
9.8	The PMTS system is configured with an automated workflow that requires electronic approval of manual ACH participant withdrawals, by authorized management personnel. Based upon the size of the disbursement and authorized approval level.	Inspected the PMTS system workflow associated with a check disbursement to determine that users who are set up with certain dollar limits are only able to view and approve PMTS distribution amounts less than or equal to the dollar amount they are assigned.	No Exception Noted.
		For each approval authority level, observed a selection of users accessing payment screens to determine that users could not view or approve payments greater than their approval limit.	No Exception Noted.

Exchanges/Investment Election Changes

Control Objective 10:

Controls provide reasonable assurance exchanges/investment changes are properly authorized and accurately recorded.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
10.1	For exchanges/investment changes to participant accounts received via hard copy, requests are reviewed by a New Business Processor for In Good Order (IGO) including proper participant authorization. This is evidenced in the NRS Workflow.	For a selection of exchanges/investment changes, inspected the NRS Workflow tool to determine that the New Business Processor reviewed the transaction for IGO (including participant authorization) as evidenced by electronic approval.	No Exception Noted.
		For a selection of exchanges/investment changes, re-performed the good order review by confirming the form was signed by the participant. Additionally, compared the exchange/investment request to DCdirect (RPLink) to determine that the request and the system matched.	No Exception Noted.
10.2	For changes to participant accounts received via the RSC, the application first requires the participant to establish an account profile with a username and password.	Observed an attempt to access the RSC using an invalid username and password to determine that access was not allowed.	No Exception Noted.
10.3	When utilizing the IVR system, the participant is prompted to enter his/her SSN or Account Number and PIN before accessing any account information or performing any transactions.	Observed both a successful and unsuccessful attempt to access the IVR to determine that the participant was prompted to enter their SSN and PIN before accessing account information or performing transactions.	No Exception Noted.

Control Objective 10:

Controls provide reasonable assurance exchanges/investment changes are properly authorized and accurately recorded.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
10.4	DCdirect (RPLink) is configured with edit checks to reject transactions if: • The transaction will result in a future allocation or exchange percentages not totaling 100%. • The transaction exceeds fixed fund money movement limits. • The transaction precedes purchase block limits.	Observed an attempt to enter the following transactions to determine that the transactions were rejected and displayed an error message: • The transaction will result in a future allocation or exchange percentages not totaling 100%. • The transaction exceeds fixed fund money movement limits. • The transaction precedes purchase block limits.	No Exception Noted.

Investment Transactions

Control Objective 11:

Controls provide reasonable assurance that investment transactions are recorded completely and accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
11.1	DCdirect (RPLink) interfaces daily trade information to UVC, and any errors that occur are identified and resolved.	Inspected trade data for one day from DCdirect (RPLink) and inspected the interface file from UVC to determine that daily trade data is automatically applied completely and accurately in UVC.	No Exception Noted.
11.2	Monthly, a staff accountant in the Portfolio Accounting Department manually reconciles Nationwide share balance totals in UVC to ending- month share balance totals provided on monthly fund statements. This reconciliation shows share balance variances being researched and reconciled by Portfolio Accounting. This reconciliation is evidenced via the Accounting Supervisor signature.	For the months of March, June, and September, inspected the reconciliation packets of the fund share balance total per the fund house and UVC to determine that they were completed and reviewed, and variances above the tolerable threshold were identified and resolved.	No Exception Noted.
		For a selection of funds, compared the market values between monthly fund statements and the UVC Share Balances Report to determine that the amounts on the reconciliation matched the source.	No Exception Noted.
		For a selection of investments held at unaffiliated custodians, confirmed with the fund house or unaffiliated transfer agent December 31, 2023 fund share balance totals to determine recorded fund share balances matched the custodians' records.	No Exception Noted.
11.3		For the March, June, and September reconciliations, inspected the summary worksheets to determine that a staff accountant reconciled the net liabilities from participant accounts in DCdirect to net assets value from the funds in UVC.	No Exception Noted.

Control Objective 11:

Controls provide reasonable assurance that investment transactions are recorded completely and accurately.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
	Monthly, a staff accountant in the Portfolio Accounting Department manually reconciles the net assets of each investment fund per UVC to the corresponding net assets for the investment fund per DCdirect (RPLink). Variances are identified, reviewed, and resolved monthly by an Accounting Supervisor.	For a selection of reconciliations, inspected documentation showing that variances were documented and communicated.	No Exception Noted.
		For a selection of reconciliations, confirmed that sign-off was completed by management.	No Exception Noted.

Unit Valuation

Control Objective 12:

Controls provide reasonable assurance that variable and fixed investment option unit values are r accurately and completely, and that income from variable and fixed investment options is r accurately and timely.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
12.1	Monthly, a staff accountant in the Portfolio Accounting Department manually reconciles Nationwide share balance totals in UVC to ending- month share balance totals provided on monthly fund statements. This reconciliation shows share balance variances being researched and reconciled by Portfolio Accounting. This reconciliation is evidenced via the Accounting Supervisor signature.	For the months of March, June, and September, inspected the reconciliation packets of fund share balance total per the fund house and UVC to determine that they were completed and reviewed, and variances above the tolerable threshold were identified and resolved.	No Exception Noted.
		For a selection of funds, compared the market values between monthly fund statements and the UVC Share Balance Reports to determine that the amounts on the reconciliation matched the source.	No Exception Noted.
		For a selection of investments held at unaffiliated custodians, confirmed with the fund house or unaffiliated transfer agent December 31, 2023 fund share balance totals to determine recorded fund share balances matched the custodians' records.	No Exception Noted.
12.2	Monthly, a staff accountant in the Portfolio Accounting Department manually reconciles daily dividend income totals in UVC to daily dividend income totals obtained from the fund house. This reconciliation reflects daily dividend income differences over $500 researched and reconciled by Portfolio Accounting. This reconciliation is evidenced via Accounting Supervisor Signature.	Inspected a selection of reconciliation packets of daily dividend income totals in UVC to fund house daily dividend income totals to determine that reconciliations were completed and reviewed and variances above the tolerable threshold were identified and resolved.	No Exception Noted.
		For a selection of reconciliations and funds, compared the daily dividend income totals to UVC and to fund house statements to determine that the amounts on the reconciliation matched the source.	No Exception Noted.

Control Objective 12:

Controls provide reasonable assurance that variable and fixed investment option unit values are r accurately and completely, and that income from variable and fixed investment options is r accurately and timely.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
12.3	Quarterly, the AVP of Financial Reporting performs a reasonableness review of significant income statement accounts. Current quarter account balances are compared to actual from prior quarter, as well as current quarter forecast. Given these considerations, if actual performance is outside of expectations by the lower of 10% or $1M, additional investigation is performed to validate the accuracy of the reported numbers prior to the FRM.	Inspected a selection of quarterly earnings reviews to determine that a AVP of Financial Reporting performed a reasonableness review of significant income statement items compared to both the forecast and prior quarter actual amounts, and evidenced authorization.	No Exception Noted.
		For a selection of quarterly earnings reviews, recalculated both the forecast and prior quarter actual amounts to determine that those amounts on the reasonableness review were mathematically accurate.	No Exception Noted.
12.4	Monthly, a staff accountant in the Portfolio Accounting Department manually reconciles the net assets of each investment fund per UVC to the corresponding net assets for the investment fund per DCdirect (RPLink). Variances are identified, reviewed, and resolved monthly by an Accounting Supervisor.	For the March, June, and September reconciliations, inspected the summary worksheets to determine that a staff accountant reconciled the net liabilities from participant accounts in DCdirect (RP Link) to net assets value from the funds in UVC.	No Exception Noted.
		For a selection of reconciliations, inspected that variances were identified and documented and communicated.	No Exception Noted.
		For a selection of reconciliations, confirmed that sign-off was completed by management.	No Exception Noted.

User Entity Reporting

Control Objective 13:

Controls provide reasonable assurance that participant and tax statements are accurate.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
Statements			
13.1	The NRS Statement Unit Team performs a quarterly audit of outgoing participant statements and evidence review by preparing a Participant Statement Audit Checklist. Completed checklists are reviewed by the Unit Manager/Lead prior to release.	For a selection of quarterly statement audits, inspected corresponding Participant Statement Audit Checklists to determine that quarterly participant statement audits were performed, and QC reviewed by the NRS Statement Unit team.	No Exception Noted.
Taxes			
13.2	Withdrawal requests in DCdirect (RPLink) call Taxcalc (C/S), where tax withholding amounts are systematically calculated and provided to DCdirect (RPLink).	For a disbursement request from DCdirect (RPLink), re-calculated the tax withholding amount that is performed by Taxcalc (C/S) to determine that the amount systematically calculated is accurate.	No Exception Noted.
13.3	Changes to Taxcalc (C/S) tables are authorized and approved by Tax Management.	Inspected a system generated listing of users with access to update the tax table in Taxcalc (C/S) and through inquiry with Management determined that users on the list were authorized and access was consistent with the individual's job function.	No Exception Noted.
		Inspected a selection of tax changes to determine that Tax Management approved each change before it was promoted into production.	No Exception Noted.

Control Objective 13:

Controls provide reasonable assurance that participant and tax statements are accurate.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
13.4	DCdirect (RPLink) interfaces daily reportable tax transactions to PMTS.	Inspected the logic of the program that creates the interface file and the job scheduling system to determine that the system was configured to automatically interface reportable tax transactions from DCdirect (RP Link) into PMTS daily (Monday – Friday).	No Exception Noted.
		Inspected tax reportable transactions from DCdirect (RPLink) for one day and inspected the interface file from PMTS to determine that the daily tax reportable transactions from DCdirect (RPLink) was automatically applied completely and accurately in PMTS.	No Exception Noted.
13.5	Monthly, PMTS interfaces daily reportable tax transactions to Taxport.	Inspected the system configuration evidence of the interface job of daily reportable tax transactions from PMTS to Taxport to determine that the system is configured to automatically interface reportable tax transactions monthly into Taxport.	No Exception Noted.
		Inspected tax reportable transactions from PMTS for one month and inspected the interface file from Taxport to determine that the daily tax reportable transactions from PMTS are automatically applied completely and accurately in Taxport.	No Exception Noted.
13.6	Annually, the FinOps Tax Reporting Unit obtains rejection reports from Taxport for data not accepted by Taxport from DCdirect (RPLink). Statements will not generate until errors are corrected.	Inspected the rejection report from Taxport of the number of files not accepted and for a selected account with an error to determine that the tax form was not available for printing.	No Exception Noted.

Control Objective 13:

Controls provide reasonable assurance that participant and tax statements are accurate.

Control Number	Controls Tested	Tests of Controls by KPMG LLP	Test Results
13.7	The 1099 print files are forwarded to the Document Solutions area; forms are created, printed, and the participant copy is mailed by Document Solutions before the IRS deadline.	Inspected correspondence from Document Solutions to determine that Document Solutions provided Treasury Services with a sample of tax statements and received approval to print and mail the 1099 files before the IRS deadline.	No Exception Noted.
13.8	Treasury Services reviews correspondence from SOVOS to determine that the 1042-S and Puerto Rico Tax forms are printed and mailed before the IRS deadline.	Inspected correspondence from Sovos to Treasury Services of the total number of forms prepared, printed, and mailed by Sovos to determine that Sovos mailed 1042-S and Puerto Rico Tax forms before the IRS deadline.	No Exception Noted.

Section V.

Other Information Provided by Management

SEC Custody Rule Control Objectives

The Securities and Exchange Commission has adopted rules under the Investment Company Act of 1940 and the Investment Advisers Act of 1940 requiring registered Investment Companies (SEC Rule 38a-1) and registered Investment Advisers (SEC Rule 206(4)-7) to adopt and implement written policies and procedures relating to a variety of specified topics and to review those policies and procedures annually. Below is a summary of topics covered by SEC Rules 38a-1 and 206(4)-7. The intent of this exhibit is to provide clients with a summary of certain aspects of the SEC Rules and where certain aspects of the Nationwide SOC 1 examination scope may provide clients with information on Nationwide controls relevant to Rules 38a-1 and 206(4)-7. However, this summary does not replace client's evaluation of their written policies and procedures relevant to Rules 38a-1 and 206(4)-7.

Rule 206(4)-2 ("Custody Rule") Internal Controls Report Control Objectives Coverage Comparison	
Suggested Custodial Operations Control Objectives Per Custody Rule	**Relevant Control Objectives**
Controls provide reasonable assurance that physical securities are safeguarded from loss or misappropriation.	Nationwide does not accept physical securities; therefore, this control objective is not applicable.
Controls provide reasonable assurance that cash and security positions are reconciled completely, accurately, and on a timely basis between the custodian and depositories.	Nationwide's controls related to the reconciliation with custodians and depositories are included under the following control objectives: **Control Objective 11 (Investment Transactions):** Controls provide reasonable assurance that investment transactions are recorded completely and accurately. **Control Objective 12 (Unit Valuation):** Controls provide reasonable assurance that variable and fixed investment option unit values are recorded accurately and completely, and that income from variable and fixed investment options is recorded accurately and timely.
Controls provide reasonable assurance that client transactions, including contributions and withdrawals, are authorized, and processed in a complete, accurate, and timely manner.	**Control Objective 8 (Contributions/Receipts)** - Controls provide reasonable assurance that contributions/receipts are recorded completely and accurately in participant accounts. **Control Objective 10 (Exchanges)** - Controls provide reasonable assurance that plan changes and plan exchanges are authorized and recorded accurately and completely. **Control Objective 09 (Withdrawals)** - Controls provide reasonable assurance that withdrawals are authorized and are completely and accurately processed.

Rule 206(4)-2 ("Custody Rule") Internal Controls Report Control Objectives Coverage Comparison

Suggested Custodial Operations Control Objectives Per Custody Rule	Relevant Control Objectives
Controls provide reasonable assurance that securities income and corporate action transactions are processed to client accounts in a complete, accurate, and timely manner.	**Control Objective 11 (Investment Transactions):** Controls provide reasonable assurance that investment transactions are recorded completely and accurately. **Control Objective 12 (Unit Valuation):** Controls provide reasonable assurance that variable and fixed investment option unit values are recorded accurately and completely, and that income from variable and fixed investment options is recorded accurately and timely.
Controls provide reasonable assurance that trades are properly authorized, settled, and recorded completely, accurately, and timely in the client account.	**Control Objective 11 (Investment Transactions):** Controls provide reasonable assurance that investment transactions are recorded completely and accurately.
Controls provide reasonable assurance that documentation for the opening and modification of client accounts is received, authenticated, and established completely, accurately, and timely on the applicable system.	**Control Objective 7 (Participant Enrollments)** - Controls provide reasonable assurance that participant enrollments are processed completely, accurately and on a timely basis. **Control Objective 10 (Exchanges)** - Controls provide reasonable assurance that plan changes and plan exchanges are authorized and recorded accurately and completely.
Controls provide reasonable assurance that new securities and changes to securities are authorized and established in a complete, accurate, and timely manner.	**Control Objective 10 (Exchanges)** - Controls provide reasonable assurance that plan changes and plan exchanges are authorized and recorded accurately and completely. **Control Objective 11 (Investment Transactions):** Controls provide reasonable assurance that investment transactions are recorded completely and accurately. **Control Objective 12 (Unit Valuation):** Controls provide reasonable assurance that variable and fixed investment option unit values are recorded accurately and completely, and that income from variable and fixed investment options is recorded accurately and timely.
Controls provide reasonable assurance that account statements reflecting cash and security positions are provided to clients in a complete, accurate, and timely manner.	**Control Objective 13 (User Entity Reporting - Statement and Taxes):** Controls provide reasonable assurance that participant statements and tax statements (Forms 1099 1042S and480.7c) statements are accurate and distributed to authorized parties.

Rule 206(4)-2 ("Custody Rule") Internal Controls Report Control Objectives Coverage Comparison

Suggested Custodial Operations Control Objectives Per Custody Rule	Relevant Control Objectives
Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.	**Control Objective 2 (Logical Access):** Controls provide reasonable assurance that logical access to programs, data and data transmissions is limited to properly authorized individuals.
Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.	**Control Objective 1 (Program and System Software Change Control):** Controls provide reasonable assurance that new applications and changes to existing systems are authorized, tested, approved, properly implemented, and documented.
Controls provide reasonable assurance that network infrastructure is configured as authorized to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and protect data from unauthorized changes.	**Control Objective 1 (Program and System Software Change Control):** Controls provide reasonable assurance that changes to existing systems are authorized, tested, approved, properly implemented, and documented. **Control Objective 3 (Physical Access):** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals.
Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.	**Control Objective 4 (Computer Operations):** Controls provide reasonable assurance that administrative and operational procedures are established within the systems operations group to provide for complete processing of jobs and backup and retention of systems and data.
Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely.	**Control Objective 4 (Computer Operations):** Controls provide reasonable assurance that administrative and operational procedures are established within the systems operations group to provide for complete processing of jobs and backup and retention of systems and data.