Report on PFC's Description of its SimpliCD Brokered Certificate of Deposit Program and on the Suitability of the Design and Operating Effectiveness of its Controls

# Primary Financial Company LLC

For the Period October 1, 2018 through September 30, 2019

PrimaryFinancial®

GBQ

# CONTENTS

230 West Street
Suite 700
Columbus, OH 43215

tel 614.221.1120
fax 614.227.6999

www.gbq.com

GBQ Partners

# I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of
Primary Financial Company LLC
Dublin, Ohio

## *Scope*

We have examined Primary Financial Company LLC's ("PFC" or "service organization") description of its SimpliCD Brokered Certificate of Deposit Program ("SimpliCD" or "system") for processing user entities' transactions throughout the period October 1, 2018 to September 30, 2019 ("description") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the Assertion of PFC's Management ("assertion"). The controls and control objectives included in the description are those that management of PFC 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 PFC," is presented by management of PFC to provide additional information and is not a part of PFC's description of its system made available to user entities during the period October 1, 2018 to September 30, 2019. Information about PFC's business continuity planning and the data center provided by a subservice organization has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

As described in Section III, PFC uses various subservice organizations to enable certain aspects of the system. The description includes only the control objectives and related controls of PFC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by PFC can be achieved only if complementary subservice organization controls assumed in the design of PFC's controls are suitably designed and operating effectively, along with the related controls at PFC. 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.

To the Management of
Primary Financial Company LLC

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 PFC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

### *Service Organization's Responsibilities*

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

### *Service Auditor's Responsibilities*

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

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

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria referenced above.

- 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 therein, and suitability of the criteria specified by the service organization in its assertion.

### *Inherent Limitations*

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

### *Description of Tests of Controls*

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

PFC’s description discusses its controls implemented and operated to ensure that principal is received from failing issuer financial institutions and properly remitted to PFC’s customers. However, during the period October 1, 2018 through September 30, 2019, there were no financial institutions in a failure status with which PFC managed outstanding assets, which would have allowed those controls to operate; therefore, we were unable to test, and did not test, the design or operating effectiveness of controls related to control objective 10.

### *Opinion*

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

a. The description fairly presents the system that was designed and implemented throughout the period October 1, 2018 to September 30, 2019.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2018 to September 30, 2019, and the subservice organizations and user entities applied the complementary controls assumed in the design of PFC's controls throughout the period October 1, 2018 to September 30, 2019.

To the Management of
Primary Financial Company LLC

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2018 to September 30, 2019 if complementary subservice organization and user entity controls assumed in the design of PFC's controls operated effectively throughout the period October 1, 2018 to September 30, 2019.

***Restricted Use***

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of PFC, user entities of PFC's system during some or all of the period October 1, 2018 to September 30, 2019, 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.


Columbus, Ohio
January 30, 2020

## II. ASSERTION OF PFC'S MANAGEMENT

We have prepared the description of Primary Financial Company LLC's ("PFC" or "service organization") SimpliCD Brokered Certificate of Deposit Program ("system") entitled "Description of PFC's SimpliCD Brokered Certificate of Deposit Program" for processing user entities' transactions throughout the period October 1, 2018 to September 30, 2019, ("description") for user entities of the system during some or all of the period October 1, 2018 to September 30, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

PFC uses various subservice organizations to enable certain aspects of the system. The description includes only the control objectives and related controls of PFC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by PFC can be achieved only if complementary subservice organization controls assumed in the design of PFC's controls are suitably designed and operating effectively, along with the related controls at PFC. 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 PFC's controls are suitably designed and operating effectively, along with related controls at the service organizations. The description does not extend to controls of the user entities.

PFC's description discusses its controls implemented and operated to ensure that principal is received from failing issuer financial institutions and properly remitted to PFC's customers. However, during the period October 1, 2018 through September 30, 2019, there were no financial institutions in a failure status with which PFC managed outstanding assets, which would have allowed those controls to operate.

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

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

    a) 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,

        i) The types of services provided, including, as appropriate, the classes of transactions processed.

ii) 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.

iii) 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.

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

vi) The services performed by subservice organizations, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

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

viii) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the service organization's system during the period covered by the description.

c) Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively, except for the processes noted above where the circumstances that warrant the operation of the processes and associated controls did not occur, throughout the period October 1, 2018 to September 30, 2019, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of PFC's controls throughout the period October 1, 2018 to September 30, 2019. The criteria we used in making this assertion were that:

   a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

   b) 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.

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

Primary Financial Company LLC
January 30, 2020

# III. DESCRIPTION OF PFC'S SIMPLICD BROKERED CERTIFICATE OF DEPOSIT PROGRAM

## Company Overview

Primary Financial Company LLC ("PFC" or "service organization") was formed in 1996 and operates as a corporate credit union service organization (CUSO). As a corporate CUSO, PFC was established in accordance with the provisions of the National Credit Union Administration (NCUA) regulations and the Ohio Revised Code. PFC is governed by a board of directors (the Board). PFC offers a turnkey program, called SimpliCD, which enables its customers to invest in federally insured certificates of deposit (CDs). PFC earns a spread over the term of the CD for performing the services of the SimpliCD program. Through the SimpliCD program, customers have access to competitive rates from a nationwide pool of CD issuing financial institutions. Whether a customer is purchasing one CD or many, the entire amount is settled in one transaction.

Services provided as part of its SimpliCD Brokered Certificate of Deposit Program include:

- Trading
- Safekeeping
- Settlement

## Scope of the Description

This description addresses only PFC's SimpliCD Brokered Certificate of Deposit Program ("system" or "SimpliCD") provided to user entities and excludes other services provided by PFC. This description is intended to provide information for user entities of SimpliCD and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of SimpliCD and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of SimpliCD.

## Internal Control Framework

This section provides information about the five interrelated components of internal control at PFC, including its:

- Control environment
- Risk assessment process,
- Monitoring activities,
- Information and communications, and
- Control activities

### *Control Environment*

The control environment sets the tone of an organization, influencing the control awareness of the organization. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organization structure.

The following are the primary elements of PFC's control environment:

1. Commitment to integrity and ethical values,
2. Oversight responsibility of the board of directors,
3. Assignment of authority and responsibility,
4. Commitment to competence, and
5. Accountability.

Commitment to Integrity and Ethical Values

PFC operates in a highly regulated environment. To this end, PFC has incorporated sections related to Standards of Conduct, Confidentiality, Conflicts of Interest and its Progressive Discipline Policy as part of its employee handbook. Employees are required to read and evidence their understanding and receipt of the service organization's employee handbook and various policies upon hire and periodically thereafter.

PFC offers its employees a number of channels through which potential breaches of ethical behavior may be reported. These channels include reporting any such incident to a supervisor, any member of management, or the Board of Directors.

Oversight Responsibility of the Board of Directors

The control environment at PFC originates with and is the responsibility of the Board of Directors (Board), Chief Executive Officer (CEO), and executive management. The Board provides oversight of PFC operations and activities. The Board is responsible for reviewing policies and practices related to accounting, financial, and operational controls, and financial reporting. The Board is also responsible for approving PFC's annual business plan, strategic goals and objectives, and annual budget.

PFC has established other functional groups dedicated to effective risk management and oversight, including an information technology and operations workgroup, including members of management, that meets monthly to review controls, manage risk, improve customer service and enhance overall business performance.

Assignment of Authority and Responsibility

There are various functional departments that manage and perform the daily operations related to SimpliCD. The trading department is primarily responsible for obtaining current rates from issuing institutions, performing financial reviews and insurance verification of issuing institutions, making rates available to SimpliCD customers and purchasing CD assets. The operations department is primarily responsible for processing all cash flows related to SimpliCD and ensuring that safekeeping receipts are received and reviewed for accuracy. PFC manages its own information systems, its payroll processes, its benefit administration and other human resource functions. The sales staff of SimpliCD is primarily made up of co-brokers, mainly corporate credit unions. The co-brokers earn a portion of the spread for CDs sold by them.

Commitment to Competence

PFC's hiring practices are designed to ensure that employees are qualified for the job responsibilities. Hiring policies include minimum education and experience requirements, and background and reference checks. The performance of personnel is evaluated on an on-going basis and must meet performance standards set by PFC. Failure to meet performance standards will result in disciplinary actions up to and including termination of employment. Employees are prohibited from divulging confidential information regarding client affairs or taking any action contrary to the best interest of clients.

Accountability

PFC's commitment to an effective system of internal control begins with its Board. The Board meets four times a year to fulfill its oversight responsibilities related to financial reporting, the system of internal control, and the service organization's process for managing risk and monitoring compliance with applicable laws, regulations, and internal policies and procedures. The Board also reviews financial performance on a monthly basis.

PFC's management team meets periodically to oversee critical business operations, and individual business unit managers have specific oversight responsibilities for information technology, trading activities, operations, accounting and financial reporting.

## *Risk Assessment Process*

Objectives

PFC's risk assessment approach involves an iterative process for identifying and assessing risks to the achievement of the service organization's objectives. This approach forms the basis for determining how risks will be managed by the service organization.

Identification and Analysis of Risks

The Board of Directors and management of PFC monitor risk and quality of operations through review of financial, operational, co-broker and customer reporting and feedback. There is also a formal strategic process that is updated on an annual basis to guide the long term objectives of the organization.

## *Monitoring Activities*

Ongoing Monitoring

Management regularly reviews and assesses business operations to determine that reporting and monitoring mechanisms are used and effective in managing the operations of the business, controls, and related risks.

Performance and Task Monitoring

Microsoft Azure Management Console provides continuous performance and capacity monitoring and displays both real-time and historical performance graphs. Performance and utilization data can be produced for defined historical periods and in real time. Management reviews performance and utilization to correlate tasks to utilization, and to troubleshoot problems.

SimpliCD is configured with a task processor and multiple queue workers. The task processor writes events to the logs when tasks commence and complete, including message content relevant to the task such as number of records processed and e-mail tasks. These tables are monitored at PFC for task scheduling and completion status. In addition, these event tables are used to manage task restarts, should a task fail. Monitoring these event tables helps ensure task completion throughout the day.

Periodic Assessments and Monitoring

In addition to ongoing monitoring activities described above, each business unit conducts specific evaluations of risks and controls to maximize the effectiveness of its operations.

The information technology and operations workgroup reviews operations and controls to assess the effectiveness of controls. The results of reviews and any identified deficiencies are reported to management. Management prepares and implements corrective measures to address any significant deficiencies.

Monitoring of the Subservice Organizations

PFC uses subservice organizations, Pershing LLC - BNY Mellon, UBS Financial Services, Inc., Financial Northeastern Companies, and Microsoft Azure, to provide clearing, execution, settlement, custody and trading services for a portion of the SimpliCD program deposit assets, and for hosting its public facing SimpliCD applications and platform architecture.

Through its daily operational activities, management of PFC monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented are functioning effectively. Management also holds periodic calls with the subservice organizations to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to the subservice organizations' management.

## *Information and Communications*

Management communicates with the various functional areas of the service organization through regular meetings and conferences. PFC communicates to its staff its policies and procedures and other information necessary to help achieve its business objectives through several means, including its Intranet, emails, newsletters, memoranda, meetings, and training sessions. PFC's policies and procedures enforce the importance of adherence to and compliance with rules and regulations that govern its business and operations.

PFC has also implemented various methods of communication to inform user entities of the role and responsibilities of PFC's responsibilities in processing their transactions and to communicate significant events to user entities in a timely manner. These methods include:

- Email, distribution list for corporate users
- Home screen on the application
- Direct phone calls
- Customer statements

User entities are encouraged to communicate questions and problems to their liaison, and such matters are logged and tracked until resolved by the appropriate PFC team member(s) with the resolution being reported back to the user entity and to the information technology and operations workgroup when applicable.

Information Systems Overview

SimpliCD is developed and runs using the Microsoft .NET architecture. SimpliCD is hosted within Microsoft's Azure Cloud Computing Platform & Services ("Azure"). System development follows a structured development methodology based on Microsoft Team Foundation Server and Microsoft Visual Studio.

### *Control Activities*

PFC has developed a variety of policies and procedures including related control activities to help ensure their objectives are carried out and risks are mitigated. These control activities help ensure that products and services delivered to user entities via SimpliCD are administered in accordance with PFC's policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorization, reconciliation, and IT controls. Duties and responsibilities – such as duties related to the processing and recording of transactions, investment trading, reconciliation activities, application development, and control monitoring – are allocated among personnel to ensure that a proper segregation of duties is maintained, or that mitigating controls are identified and implemented.

A formal program is in place to review and update policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to employees.

## Transaction Processing Controls

Trading Activities

When orders are placed, SimpliCD sends instructions to the issuing financial institution to ensure that each CD purchased is properly titled and the terms of the transaction are accurately recorded. A customer's existing deposits at each financial institution are verified prior to purchase to prevent a customer from exceeding the insured limit amount from an issuing institution.

When PFC's trading desk attempts to match an open purchase request to a CD asset on SimpliCD, the system compares the dollar amounts and will not allow trades in excess of the asset. Once a purchase request is funded, the system will not allow the trade to be unlocked from the CD asset.

The system has embedded features that match the available CDs to the trades and prevent overselling of the same CD to more than one investor. The Operations team performs reconciliations to verify that CD assets from the prior day plus current day sales less current day maturities agree to the total CD asset balance on the system at the end of the day.

The issuer profile within SimpliCD requires the trading desk to obtain and enter the issuer's insurance number prior to PFC selling any CDs for the issuer. On a quarterly basis, the trading desk performs a review of all issuers to ensure that PFC has updated the issuer profile on the system for name changes or mergers.

Safekeeping Activities

Customer profiles are set-up in SimpliCD by the trading desk. Customer profiles are populated based on information from the customer agreements and include name, address, tax ID, routing and transit number and settlement instructions. SimpliCD generates the monthly statements based on the customer data associated with each trade.

The titling, dollar amount, rate, settlement date, maturity date and asset number on the safekeeping receipt is verified against the corresponding data on the system. Corrections to safekeeping receipts are worked manually by PFC's operations department before they are filed.

Reports are run regularly to determine which safekeeping receipts have not been received. Safekeeping receipts are filed and maintained for six years after the CD has matured.

The system does not allow PFC's operations department to make changes to customer profiles.

Settlement Activities - Purchases

Each day, a balancing process is followed to ensure all incoming and outgoing funds are matched and reconciled to ensure that all funds are properly accounted for. The system also identifies all CDs maturing on a given day so that any funds not received are properly identified and controlled. PFC's operations department researches and resolves unfunded customer purchase requests and CD asset purchases throughout the day.

Settlement Activities - Interest

Interest is remitted to investors on an automated basis using the contractual terms agreed to by the investor, regardless of when the funds are actually received from the issuer. Monitoring systems are in place to assure the related income is received from the issuer as well. Each investor is provided a monthly statement detailing interest and principal payments.

All issued CDs are individually accounted for in the system and expected interest income is calculated. As interest is received it is posted to the respective CD in the system. This provides for the monitoring by both CD and issuer of interest due.

Settlement Activities - Maturities

SimpliCD generates reports daily listing all CDs maturing that day. PFC's operations department manually works the report to determine which CDs are being renewed versus actually maturing. PFC's operations department follows up on maturities for which funds have not been received from the issuer and remitted to the customer.

The incoming and outgoing wire account for principal is reconciled daily by PFC's operations department.

Settlement Activities – Financial Institution Failures

PFC has written procedures in place that are followed in connection with issuing institution failures, to ensure that the federal insurance is maintained. These procedures include communication protocol with the respective deposit insurer and monitoring to ensure all investor funds are received and remitted.

PFC is notified by FDIC/NCUA about any financial institution failures.

Once notification is received, a claims form is completed and filed with the appropriate regulatory authority to collect funds from the failed financial institution. Any changes in rates to be paid by the failing institution are communicated to the investing credit unions as soon as notification is received.

Monitoring of the collections status of failed institutions consists of ongoing communication within PFC and when appropriate with the regulators.

## Information Technology General Controls

Logical Access Controls

PFC has a documented process for granting Employees (internal users) new or changed access to SimpliCD, and for removing their access in a timely manner when terminated. User IDs are uniquely identifiable and granted based on assigned roles and responsibilities.

Each corporate credit union (user entity) has an Authorized Signer who is responsible for provisioning access to their investment and trading data for their employees and certain retail credit unions (external users). Standard roles that have been established include administrator, senior user and junior user. Authorized Signers are administrators who can assign senior and junior user roles to their employees.

Password constraints exist which are designed to facilitate the use of strong passwords. These controls include minimum length, complexity and account lockout for invalid password attempts. In addition, SimpliCD will time-out and return to the authentication screen after a period of inactivity. Clear-text passwords are not stored by SimpliCD; passwords are salted and hashed when stored.

PFC uses portable and desktop computers to access the application development and system management environments (Microsoft Team Foundation Server and Azure respectively). Workstation controls include:

- Workstation access is secured with a unique User ID and password.
- Local user profiles are limited to the primary workstation user and an administrator account.
- Anti-malware software is in use.
- Workstation patching is centrally managed using Microsoft InTune.
- Files are stored on the Azure storage system.
- Local workstation shares are not used.

Network Controls

Microsoft Azure provides the ability for system administrators to establish and manage certain firewall rules within the application's virtual database environment. Microsoft Azure provides additional system level controls which secure each subscribers virtual environment. Each subscription has a unique subscription ID. Access within the subscription's environment is granted only with access credentials for that subscription.

A system-control is in place which prevents external users from accessing investment, trading and user information that is not directly related to their sponsoring corporate credit union.

System Administration and Development Authentication and Access

System administrators and application developers use the Azure Management Console for defining and establishing the cloud web services and database system configurations. These users are PFC employees and contractors. The Azure Management Console requires these users to authenticate with a unique user ID and password.

System administrators, administrative support employees and application developers use local Windows workstations and desktop applications to access documents and settlement files which are processed by SimpliCD. The desktop applications gain access to authorized data in Azure based on assigned access to virtual drive and folder system. Each user has a unique user ID and password and is granted appropriate access to SimpliCD applications and databases based on their job function and responsibilities.

Operating system authentication is independent of application access. Web browsers using HTTPS access SimpliCD applications in Azure. PFC employees use local Windows workstation authentication to access their workstations. Unique user ID and passwords are required for PFC employee workstation access. PFC system administrators use a generic administrative account to perform privileged desktop maintenance.

Physical Access Controls

The PFC office suite has one entrance; the entrance is locked during non-business hours at all times. The entrance is alarmed. A chime is sounded any time the door is opened during normal business hours. The staff arms the system when they leave at night, and disarm it when they arrive each morning. Logs are maintained by the security vendor that document daily activity including when alarm is enabled or disabled, and who accesses the suite after normal business hours. After-hours access to the suite is logged and available for forensic review when needed.

SimpliCD is hosted at Microsoft's Azure datacenters; however, PFC maintains its application development environment at the corporate headquarters which is located in a multi-tenant office building in Dublin, Ohio. The office building automatically locks and unlocks the doors at proscribed times to secure the building during non-business hours.

Application Development and Change Control

Application change requests are generated by PFC employees. Requests may originate in PFC or from a co-broker.

Microsoft Team Foundation and e-mails are used for communicating the request specifications, development, prototyping, approval and production staging.

Requests are reviewed by the Helpdesk and developer teams. This process defines the nature of the request and is used to determine the impact on all SimpliCD users. This process is also used to break a request into component phases if necessary.

Code development is managed in Microsoft Team Foundation Server (TFS). TFS provides management utilities to provide consistency and communication in the development, testing, and migration phases.

Code instances are named with a specific date and time to ensure developers select the latest code instance for changes.

A new environment instance is created in Azure for testing. The new environment is generated from a configuration file which exists in the project and defines the environment. Microsoft Visual Studio automatically builds the environment. The configuration files and the application package solution files used by TFS help ensure consistency and completeness.

Code review is done by a separate PFC developer and by a contracted third-party developer. Visual Studio provides a side-by-side code comparison feature which is used to review code changes. Code review and approval are communicated by e-mail.

A separate release branch exists in TFS that includes all approved code changes that are ready to be merged to production. When these changes are ready to be deployed, an authorized individual opens the release branch on their workstation and publishes the changes to production. The old version is swapped with this new version so that it is now in the Azure Management Portal production environment. Upon confirmation that the new version is working properly, the old version is deleted from the portal.

Production deployment is scheduled during non-business hours. The production staging process permits an update to be deployed while the application is running in production if necessary.

Database Processing Integrity

Database transaction processing often occurs in programmatic loops. Transaction integrity is implemented throughout the system with the use of "Commit" statements. Typical coding involves a looping or iterative process with a "Begin Work" statement and a "Commit" statement. This ensures all task work is complete prior to writing to the database.

Backup and Replication

The SimpliCD database is backed up via the SQL Azure Premium Tier, which provides 35 day point-in-time restore and up to 7 year long-term retention.

Application development packages are created and maintained by PFC and backed up into Azure storage managed by PFC, but located within the Microsoft Azure hosted environment. Each application build is named using the date and time of the build.

Encrypted Data Connections

SimpliCD web login and processing pages require an HTTPS connection. Attempts to access SimpliCD with http only will result in a "page not found" error. TLS v1.2 is required; TLS 1.1 and 1.0 and SSL 2 and 3 are not supported. A valid digital certificate is provided by a trusted certificate authority.

Azure console operations web login and operations pages require an HTTPS connection. Azure console operations attempted with http redirect to https. TLS v1.2 is required; TLS 1.1 and 1.0 and SSL 2 and 3 are not supported. A valid digital certificate is provided by a trusted certificate authority.

## Control Objectives and Related Controls

PFC has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in section IV, "Description of Control Objectives and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results", and are an integral component of PFC's description of its system.

## Complementary Subservice Organization Controls

PFC's controls related to the system cover only a portion of overall internal control for each user entity of PFC. It is not feasible for the control objectives related to clearing, execution, settlement, custody and trading services for a portion of SimpliCD deposit assets, and for hosting its public facing SimpliCD applications and platform architecture to be achieved solely by PFC. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with PFC's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls (CSOCs) expected to be implemented at the subservice organizations as described below.

| Subservice Organization | Nature of Services Provided |
|---|---|
| Pershing LLC - BNY Mellon | BNY provides clearing, execution, settlement, custody and trading services for a portion of SimpliCD deposit assets. |
| UBS Financial Services, Inc. | UBS provides clearing, execution, settlement, custody and trading services for a portion of SimpliCD deposit assets. |
| Financial Northeastern Companies | FNC provides clearing, execution, settlement, custody and trading services for a portion of SimpliCD deposit assets. |

| Subservice Organization | Nature of Services Provided |
|---|---|
| Microsoft Azure | Microsoft Azure's Cloud Computing Platform and Services are used to build, deploy and manage applications and services through a global network of Microsoft-managed datacenters. SimpliCD was developed, deployed and is managed through this Platform as an Application Service offering. Microsoft Azure provides for a physically secure and environmentally protected datacenter that provides high availability of our applications for our customers. |

| | Complementary Subservice Organization Controls | Related Control Objectives |
|---|---|---|
| 1 | BNY, UBS and FNC are responsible for ensuring clearing, executing, settlement, custody and trading services for a portion of the SimpliCD deposit assets are processed completely, accurately and timely. | CO 1<br>CO 5<br>CO 6<br>CO 9 |
| 2 | Microsoft Azure is responsible for maintaining physical security of its data center used to host the SimpliCD applications and for notifying PFC of any incidents related to the security or availability of the datacenter and/or PFC's SimpliCD applications. | CO 13<br>CO 15 |

### Complementary User Entity Controls

PFC's controls related to the system cover only a portion of overall internal control for each user entity of PFC. It is not feasible for the control objectives related to the system to be achieved solely by PFC. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with PFC's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls (CUECs) identified under each control objective, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls, as described below, have been implemented and are operating effectively.

| | Complementary User Entity Controls | Related Control Objective |
|---|---|---|
| 1 | User credit unions should review their monthly statements from SimpliCD for accuracy, including verification of the rate, amount and maturity date. | CO 6 |
| 2 | Users should reconcile their monthly receipt of interest and/or principal from SimpliCD to their own books and records and verify the amount of interest income received. | CO 7 |
| 3 | Users should perform their own review of the safety and soundness of the issuing financial institutions. | CO 10 |
| 4 | Users should review their portfolio of CDs, whether purchased through SimpliCD or otherwise, to ensure they do not exceed the insurance limit. | CO 2 |

| | Complementary User Entity Controls | Related Control Objective |
|---|---|---|
| 5 | Users are responsible for establishing controls to ensure they are aware of any duplicate investments they may have resulting in investments over the federal insurance limits. They are also responsible for evaluating the financials of issuing institutions. | CO 2 |
| 6 | Users are responsible for establishing controls to ensure their employees adhere to good password practices which include establishing strong passwords, periodically changing passwords and maintaining password confidentiality. | CO 12 |
| 7 | Users are responsible for establishing controls to ensure that their employees have proper roles with respect to their relationship with PFC and their access within SimpliCD. | CO 12 |
| 8 | Users are responsible for establishing a secure workstation and user configuration for devices which are used to connect to SimpliCD. | CO 15 |
| 9 | Users are responsible for establishing controls to ensure the physical and logical security of their records, infrastructure and computing devices. | CO 12, 13 & 15 |
| 10 | Users are responsible for establishing controls to ensure their workstation browser software is configured to use the highest level of encryption, which should minimally be TLS v1.2. | CO 16 |
| 11 | Users are responsible for establishing controls to ensure that their employees have up to date training to recognize and decrease cybersecurity risks. | CO 12 |

# IV. DESCRIPTION OF CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

## Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at PFC.

Our examination was limited to the control objectives and related controls specified by PFC in Sections II and IV of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, PFC's controls may not compensate for such weaknesses.

PFC's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by PFC. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by PFC, we considered aspects of PFC's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

| Test | Description |
|---|---|
| Inquiry | Inquiry of appropriate personnel and corroboration with management. |
| Observation | Observation of the application, performance, or existence of the control. |
| Inspection | Inspection of documents and reports indicating performance of the control. |
| Re-performance | Re-performance of the control. |

In addition, as required by Paragraph .35 of AT-C Section 205, Examination Engagements (AICPA, Professional Standards), and Paragraph .30 of AT-C Section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

## Transaction Processing Controls

Trading Activities

**Control Objective 1: Controls provide reasonable assurance that issuing financial institutions properly title each CD.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 1.1 | For each CD purchase, automated instructions are sent to each issuing institution confirming significant terms of each CD purchase transaction. | Randomly selected CDs from a population of all CDs issued from October 1, 2018 through September 30, 2019 and inspected safekeeping documents and trade confirmations to verify CDs were properly titled. | No exceptions noted. |

**Control Objective 2: Controls provide reasonable assurance that for each customer no more than $250,000 of investments can be purchased in any single financial institution.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 2.1 | The system has an embedded programmed feature that identifies and prevents a customer from exceeding the insured limit amount from an issuing institution.<br><br>No manual intervention or override capabilities exist. | Using the trade summary data (all trade activity during the year), inspected 100% of the population using pivot tables by issuer and investor to verify that no investor placed trades in aggregate in excess of $250,000 with any single issuer. | No exceptions noted. |

**Control Objective 3: Controls provide reasonable assurance that each CD is sold to only one customer.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 3.1 | The system has embedded features that match the available CDs to the trades, and prevent overselling of the same CD to more than one investor. | Using the trade summary data (all trade activity during the year), inspected 100% of assets by comparing total trades on each asset to the total principal from the issuer. | No exceptions noted. |
| 3.2 | Once a purchase request is funded, SimpliCD will not allow the trade to be unlocked from the CD asset. | Automated system configuration control - tested retrospectively by inspecting 100% of trades by comparing total trades on each asset to the total principal from the issuer. | No exceptions noted. |
| 3.3 | Operations performs daily a reconciliation to verify that CD assets from the prior day plus current day sales less current day maturities agree to the total CD asset balance on SimpliCD at the end of the day. | Selected a sample of days and inspected the daily reconciliations performed. Traced the balances reported in the reconciliation to supporting documentation. | No exceptions noted. |

| Control Objective 4: Controls provide reasonable assurance that CDs are only sold for FDIC/NCUSIF insured financial institutions. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 4.1 | Only issuers with federal deposit insurance are authorized issuers of CDs within the parameters of the system. | Selected a sample of issuers and determined the issuer was FDIC/NCUSIF insured. | No exceptions noted. |
| 4.2 | On a quarterly basis, the trading desk performs a review of all issuers to ensure that PFC has updated the issuer profile on SimpliCD for name changes or mergers. | Obtained and inspected the Veribanc report for one quarter. Selected a sample of updates for testing and inspected the issuer history log and determined that SimpliCD was updated timely for issuer changes. | No exceptions noted. |

Safekeeping Activities

| Control Objective 5: Controls provide reasonable assurance that PFC's safekeeping records for SimpliCD are complete and accurate. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 5.1 | When a trade ticket is opened for a new CD purchase, the customer data associated with the individual trade is automatically populated from the customer profile. | Selected a sample of trades and compared customer data to customer agreements and updated support. | No exceptions noted. |
| 5.2 | SimpliCD generates the customer's monthly statements based on the customer data associated with each trade. | Selected a sample of investors and months during the audit period and re-performed the reconciliation of activity from the statement to the trade summary. | No exceptions noted. |
| 5.3 | The titling, dollar amount, rate, settlement date, maturity date and asset number on the safekeeping receipt is verified against the corresponding data on SimpliCD. | Subjected all CDs issued from October 1, 2018 through September 30, 2019 to selection. Randomly selected a sample of CDs and inspected safekeeping documents. | No exceptions noted. |
| 5.4 | Reports are run regularly to identify transaction and safekeeping receipts that have not been received.<br>PFC's operations department performs manual follow up for safekeeping receipts not received. | For a sample of months, obtained the safekeeping receipt grid that is used to track outstanding safekeeping receipts. Reviewed the listing and noted there were minimal items outstanding. For items outstanding more than 48 days, obtained the letter sent to the issuer and determined follow-up was performed. | No exceptions noted. |

Settlement Activities – Purchases

| Control Objective 6: Controls provide reasonable assurance that incoming funds from customers are properly accounted for and principal is properly remitted to the issuers. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 6.1 | Real time checks are performed throughout the day to determine which trades PFC's customers have not funded. | Selected a sample of days and inspected the daily reconciliations performed. Traced the balances reported in the reconciliation to supporting documentation. | No exceptions noted. |
| 6.2 | The operations department verifies that the name on the wire of incoming customer principal agrees with the name on the original trade ticket. | Selected a sample of trades and traced the support from the trade summary to the applicable day's reconciliation and reconciled the purchases noted to funds received from investors. | No exceptions noted. |
| 6.3 | The incoming and outgoing wire account for principal is reconciled monthly by PFC's accounting department. | Selected a sample of months and obtained the month-end reconciliations, tracing to supporting statements and documentation. | No exceptions noted. |

Settlement Activities – Interest

| Control Objective 7: Controls provide reasonable assurance that payment of interest to customers is accurate and timely. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 7.1 | The calculation and payment of interest to customers is an automated process performed by the 5th day of every month by SimpliCD. | Selected a sample of investments and independently recalculated interest and compared to the interest paid per the account statement. | No exceptions noted. |

| Control Objective 8: Controls provide reasonable assurance that receipt of interest from issuers is accurate and timely. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 8.1 | Reports are generated regularly that compare expected interest calculated by SimpliCD versus actual interest received from the issuer. | Selected a sample of assets and recalculated interest and agreed the information from the asset summary to the safekeeping document. Recalculated interest based on the terms noted. Agreed the interest received from that asset to cash receipt detail. | No exceptions noted. |

Settlement Activities – Maturities

| Control Objective 9: Controls provide reasonable assurance that principal is received from issuers and properly remitted to PFCs customers. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 9.1 | PFC's operations department follows up on maturities for which funds have not been received from the issuer and remitted to the customer. | Selected a sample of investments that matured in the period under audit and obtained support detailing the pay out or rollover of the investment. Compared date of pay out/rollover to maturity date.<br><br>For the above-selected maturity dates, inspected the incoming wire detail from the issuer, noting whether the funds had been received. | No exceptions noted. |
| 9.2 | The incoming and outgoing wire account for principal is reconciled monthly by PFC's accounting department. | Selected a sample of months during the audit period and inspected the month-end reconciliations and supporting documentation. | No exceptions noted. |

Settlement Activities – Financial Institution Failures

| Control Objective 10: Controls provide reasonable assurance that principal is received from issuers and properly remitted to PFC's customers for financial institution failures. | | | |
|---|---|---|---|
| **Ref** | **Controls Specified by PFC** | **Tests of Controls** | **Results of Tests** |
| 10.1 | PFC is notified by the FDIC/NCUA about financial institution failures. | Obtain a listing of all failed financial institutions placed under conservatorship, as well as the written procedures. Selected a sample from the listing provided and inspected proper documentation related to the collecting of the funds. | No exceptions noted. |
| 10.2 | Once notification is received, a claims form is completed and filed with the appropriate regulatory authority to collect funds from the failed financial institution. | The operating effectiveness of this control has not been tested because there were no failed financial institutions doing business with PFC during the period under examination. | N/A |
| 10.3 | The funds for principle and interest from the failed institution are received via wires to PFC and forwarded through wires to appropriate investors with principle plus any interest. | The operating effectiveness of this control has not been tested because there were no failed financial institutions doing business with PFC during the period under examination. | N/A |
| 10.4 | Monitoring of the collections status of failed institutions consists of ongoing communication within PFC and when appropriate, with the regulators. | The operating effectiveness of this control has not been tested because there were no failed financial institutions doing business with PFC during the period under examination. | N/A |

## Information Technology General Controls

**Control Objective 11: Controls provide reasonable assurance that personnel policies are implemented and include performance of background investigations and confidentiality agreements.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 11.1 | Employment with PFC is contingent on the successful completion of a background investigation. | Inspected Personnel Files for a sample of new full time employees and determined that background investigations were successfully completed. | No exceptions noted. |
| 11.2 | Employees are required to sign a confidentiality agreement when hired indicating they have read and understand their obligations with respect to handling confidential information. | Inspected personnel files for a sample of new full time employees and determined that Confidentiality agreements were obtained when hired. | No exceptions noted. |

**Control Objective 12: Controls provide reasonable assurance that logical access to applications, data files, and computer resources is restricted to properly authorized and appropriate individuals.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 12.1 | Requests for establishing new user access are documented, initiated and approved by persons with proper authority. | Inquired of the process for establishing and maintaining user accounts.<br><br>Inspected new user tickets used to request access and onboarding worksheet used to load and configure workstations with appropriate secure configurations. | No exceptions noted. |
| 12.2 | PFC Users have uniquely identifiable User IDs and are granted appropriate access to SimpliCD applications and databases based on their job function and responsibilities. | Obtained and inspected the Employee Census Report, related new user access request tickets and SimpliCD Users table and determined that 100% of new users added throughout the period received only access appropriate to their role and responsibilities. | No exceptions noted. |
| 12.3 | Corporate Credit Union Users have uniquely identifiable User IDs and are granted appropriate access to SimpliCD by authorized administrators at each Corporate Credit Union. | Inspected system generated list of SimpliCD user IDs and determined that except for an appropriate number approved maintenance accounts used by IT Administrators for user support purposes, internal & external user accounts are uniquely identifiable. Performed testing over new Corporate Credit Union Admins granted access during the period to determine if the access was properly granted. | No exceptions noted. |

**Control Objective 12: Controls provide reasonable assurance that logical access to applications, data files, and computer resources is restricted to properly authorized and appropriate individuals.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 12.4 | Corporate Credit Union Users can only access information in SimpliCD which is for their organization. System controls prevent access to other organizations. | Attempted to modify part of URL during an authenticated user session to test whether data for another Corporate Credit Union could be accessed. Noted URL reverted back to correct address/user.<br><br>On trade tabs attempted to search for wildcard investors, received message "no items to display".<br><br>Injected miscellaneous characters into search for another investor and at login screens and system rejected attempts at unauthorized access with appropriate error messages. | No exceptions noted. |
| 12.5 | User account passwords for access to SimpliCD applications are salted and hashed. | Inspected the SimpliCD Users SQL table which stores user account information and password salts and determined that all stored passwords were hashed and no clear text passwords were visible. | No exceptions noted. |
| 12.6 | Measures are in place to maintain the effectiveness of authentication and access mechanisms to SimpliCD. | Inspected Azure configurations and determined that appropriate password expiration and reuse parameters are configured and in place for Azure, SimpliCD and Team Foundation Servers. | No exceptions noted. |
| 12.7 | The access of terminated PFC users is removed or disabled by the IT security group in a timely manner following notification from the VP Operations that a termination has occurred or is pending. | Requested and obtained an Employee Census and inspected user access lists from Azure, SimpliCD and Team Foundation Servers and determined that access was timely removed. | No exceptions noted. |
| 12.8 | Access to the privileged role "Owner" of the Azure platform is restricted to persons who require this level of access to perform their job function and responsibilities. | Inspected multiple system generated lists of users with "Owner" role and determined that all users with assigned "Owner" role are employees or contractors and access is appropriately restricted. | No exceptions noted. |
| 12.9 | Only authorized employees and contractors can access Team Foundation development Server (TFS). | Inspected a sample of accounts on the PFC Team Foundation Server and traced the user ID to either the active employee census or active contractor list provided by HR. | No exceptions noted. |

**Control Objective 12: Controls provide reasonable assurance that logical access to applications, data files, and computer resources is restricted to properly authorized and appropriate individuals.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 12.10 | Firewalls located in Dublin, Ohio and Columbus, Indiana are appropriately configured to restrict access to the internal networks except that which is explicitly approved.<br><br>Access to Azure management functions is restricted to authorized IP address ranges belonging to PFC and authorized 3rd party development partners. | Inquired of management regarding network security among subscription accounts and with respect to services enabled in the Azure environment.<br><br>Examined firewall configurations in Azure and determined that authorized connections to the Azure management environment were restricted to authorized IP address or address ranges.<br><br>Examined perimeter firewall configurations for both Dublin, Ohio and Columbus, Indiana locations to determine whether access rulesets are configured to filter traffic and to protect the network. | No exceptions noted. |

**Control Objective 13: Controls provide reasonable assurance that physical access to the facilities and computer resources is restricted to authorized individuals based on job responsibilities and computer resources are protected from intentional or unintentional loss or impairment.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 13.1 | A security system requiring card keys is utilized at the Dublin, Ohio office to restrict access to building and floors in the building after hours. | Inspected key pads and cameras associated with the building's security system and determined that access to the building's lobbies, elevators and tenant floors requires use of a key card after normal business hours. | No exceptions noted. |
| 13.2 | A separate security system installed in PFC's Dublin, Ohio office suite requiring card keys is utilized to restrict access to the suite after hours. Logs are maintained that document daily activity including when alarm is enabled or disabled, and who accesses the suite after normal business hours. After-hours access to the suite is logged and available for forensic review when needed.<br><br>Office Suite in Columbus, Indiana is secured with card keys issued by the building landlord. | Observed the operation of the alarm system which alerts staff anytime the suite door is opened, and observed the arming and disarming of the alarm by staff in the morning and evening.<br><br>From a sample of days during the period under examination, inspected security access logs and determined that system was logging activity as designed. | No exceptions noted. |

**Control Objective 14: Controls provide reasonable assurance that changes to the SimpliCD applications are authorized, tested, approved, and documented.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 14.1 | PFC has documented written change request and application development workflows for systems development and change management processes. | Inquired of management regarding the processes for checking out code, establishing a test environment, migrating code changes into the production code branch, and publishing package updates to the production web server.<br><br>Inspected diagram of SimpliCD change control process and determined documented processes were consistent with management's description of processes and procedures. | No exceptions noted. |
| 14.2 | Requests for changes to SimpliCD applications are documented in a change request form and initiated or approved by appropriate business owner and IT management. | For a sample of SimpliCD change requests, inspected the change request form and determined the request was initiated or approved by appropriate business and IT management.<br><br>For a sample of migrations, traced back to Request Ticket List provided and determined all migrations tested were supported by request tickets. The random selection was based on checked-in change sets. | No exceptions noted. |
| 14.3 | Changes are tested by developer and moved to Team Foundation Server. | For a sample of SimpliCD change requests, inspected the testing documentation and determined code was migrated to TFS. | No exceptions noted. |
| 14.4 | A code review is performed by IT and a third party when appropriate and deployed to Azure Quality Assurance environment. | For a sample of SimpliCD change requests, inspected the Code Review documentation and determined code was migrated to Azure QA environment. | No exceptions noted. |
| 14.5 | Quality assurance testing is completed and the changes are deployed to an Azure user acceptance testing environment. | For a sample of SimpliCD change requests, inspected the QA testing documentation and determined code was migrated to Azure user acceptance testing environment. | No exceptions noted. |
| 14.6 | User acceptance testing is completed and changes are deployed into the production environment. | For a sample of SimpliCD change requests, inspected the UAT documentation and determined code was migrated to the production environment. | No exceptions noted. |

**Control Objective 14: Controls provide reasonable assurance that changes to the SimpliCD applications are authorized, tested, approved, and documented.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 14.7 | Separate environments exist for development, testing and staging of application coding prior to being migrated to the production environment. | Inquired of management regarding program development and change control activities. Inspected SimpliCD Prod, QA, and UAT services subscribed in Azure. Identified separate services for Production, Quality Assurance/Test, and User Acceptance Testing.<br><br>Inspected diagram of SimpliCD change control process and confirmed existence of multiple environments while testing changes. | No exceptions noted. |
| 14.8 | Access to production application environment and change control migration platforms is restricted to authorized personnel. | Inspected a system generated list of Azure Administrators from the Management Console and for each name listed traced each user ID to either the active employee census or the active contractor list. | No exceptions noted. |

**Control Objective 15: Controls provide reasonable assurance that SimpliCD system processing is monitored, development server and workstation operating systems are updated, patched and protected from malware on a timely basis, and data is backed up daily.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 15.1 | PFC monitors systems performance, utilization, capacities and event logs to ensure operational availability and integrity of systems processing. | Observed management console visible on IT staff monitors multiple times throughout the year, and observed selected transaction processing logs. | No exceptions noted. |
| 15.2 | The Team Foundation Windows Server and user workstations are patched and virus/malware protections are updated on a timely basis. | Observed security policy configurations for the TFS server and observed that Windows updates are set to install automatically and the Windows End Point Protection definitions were updated on a timely basis. | No exceptions noted. |
| 15.3 | The SimpliCD database is backed up via the SQL Azure Premium Tier, which provides 35 day point-in-time restore and up to 7 year long-term retention. | Reviewed the Azure backup configurations to ensure the backup is in place and being utilized. Reviewed the backup logs and determined that backups occurred throughout the testing period. | No exceptions noted. |

**Control Objective 15: Controls provide reasonable assurance that SimpliCD system processing is monitored, development server and workstation operating systems are updated, patched and protected from malware on a timely basis, and data is backed up daily.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 15.4 | Access to backup job scheduler is appropriately restricted. | Inspected system generated lists of users with "Owner" role, which permits access to job scheduler and determined that all users with assigned "Owner" role are authorized employees or contractors and access is appropriately restricted. | No exceptions noted. |

**Control Objective 16: Controls provide reasonable assurance that data transmissions between SimpliCD Applications and its user entities and other outside entities are from authorized sources and are encrypted to ensure secure connections.**

| Ref | Controls Specified by PFC | Tests of Controls | Results of Tests |
|---|---|---|---|
| 16.1 | User connections to the SimpliCD applications are secured via HTTPS connections using public-private key cryptography. | Inspected SimpliCD web login page and determined that TLS v1.2 with 256 bit keys is required to login and that a valid certificate from a trusted authority is in use. | No exceptions noted. |
| 16.2 | Connections to Azure systems operations center from authorized locations are restricted to specific IP addresses and secured via HTTPS connections using public-private key cryptography. | Inspected Azure and firewall configurations and determined that access is restricted to specific IP addresses and secured using public-private key cryptography. | No exceptions noted. |

# V. OTHER INFORMATION PROVIDED BY PFC

## Business Recovery Plan

The following business applications, databases, file systems, application code, other software tools and backups are deployed and maintained with in the Microsoft Azure environment to provide high availability and facilitate recovery if and when needed:

- PFC public website
- SimpliCD applications, and SimpliCD SQL Reporting Server
- SQL Azure Database
- Application development testing and quality control environments

Other files related to SimpliCD like settlement, safekeeping and others are also hosted on Microsoft Azure storage platform and infrastructure.

These applications and data structures are backed up daily within the Azure infrastructure.

To guard against hardware failures and improve availability, all storage blobs are replicated across three servers within the hosting Microsoft Azure datacenter. Writing to a blob updates all three copies, so later reads won't see inconsistent results. Additionally, all Microsoft Azure blob and table storage is replicated between paired data centers hundreds of miles apart within a specific geographic region. Given the world class data centers Microsoft has made available and the extreme redundancy it provides, the risk of widespread loss is very low. We rely on Microsoft Azure for most common disaster recovery services. However, in the event of data center failure or internet connectivity failure in primary data center region, PFC has a documented recovery and continuity plan to enable continued operation of the business.

## Microsoft Azure Cloud Platform and Services

Microsoft Azure provides a physically secure data center environment. Microsoft Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity. In addition to data center, network, and personnel security practices, Microsoft Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators. Microsoft conducts regular penetration testing to improve Microsoft Azure security controls and processes. More information about Microsoft Azure Security can be found at https://azure.microsoft.com/en-us/overview/trusted-cloud/.

Microsoft's approach to security in its cloud environment is laid out in the white paper securing Microsoft's Cloud Infrastructure. To summarize, Microsoft applies security mechanisms at different layers of the cloud infrastructure to implement a defense-in-depth approach. These layered mechanisms include:

- Physical security of the data centers (locks, cameras, biometric devices, card readers, alarms)

- Firewalls, application gateways and IDS to protect the network

- Access Control Lists (ACLs) applied to virtual local area networks (VLANs) and applications
- Authentication and authorization of persons or processes that request access to data
- Hardening of the servers and operating system instances
- Redundant internal and external DNS infrastructure with restricted write access
- Securing of virtual machine objects
- Securing of static and dynamic storage containers

Assets are categorized as to the level of security required, based on the potential for damage. The principle of least privilege is followed, whereby persons and processes are given the lowest level of access that is required for them to do their jobs and no more.