

PAYCHEX, INC.

SOC 2® REPORT

Paychex, Inc.'s Description of Its Flex Retirement Services, Payroll, and Reporting Services System Throughout the Period October 1, 2021 to September 30, 2022

Prepared in accordance with AT-C Section 205

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

PAYCHEX, INC.

SOC 2 REPORT
PAYCHEX FLEX RETIREMENT SERVICES, PAYROLL, AND REPORTING SERVICES SYSTEM

THROUGHOUT THE PERIOD October 1, 2021 TO SEPTEMBER 30, 2022

TABLE OF CONTENTS

SECTION I **1**

The Independent Service Auditor's Report **2**

SECTION II **6**

Management of Paychex, Inc.'s Assertion **7**

SECTION III **8**

Paychex, Inc.’s Description Of Its Paychex Retirement Services, Payroll, and Reporting Services System **9**

Company Overview **9**

Subservice Organizations **10**

Scope of this Report **11**

Principal Service Commitments and System Requirements **12**

System Boundaries **13**

COMPONENTS OF THE SYSTEM **14**

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, AND MONITORING **38**

Monitoring **40**

Risk Assessment **42**

Information and Communication **44**

COMPLEMENTARY USER ENTITY CONTROLS **46**

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOC) **48**

SECTION IV **53**

TRUST SERVICES CRITERIA AND PAYCHEX, INC.’S RELATED CONTROLS **54**

SECTION V **126**

Management’s Response to Testing Exceptions **127**

Privacy Statement **127**

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY PwC LLP



The Independent Service Auditor's Report

To the Management of Paychex, Inc.

Scope

We have examined Paychex, Inc.'s (the "Service Organization") accompanying description of its Flex Retirement Services, Payroll, and Reporting Services system (the "system") titled "Paychex, Inc.'s Description of Its Flex Retirement Services, Payroll, and Reporting Services System" throughout the period October 1, 2021 to September 30, 2022 ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout that period, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and processing integrity ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V, "Other Information Provided by Paychex, Inc. That is Not Covered by the Service Auditors' Report" is presented by management of the Service Organization to provide additional information and is not a part of the description. Information about the Service Organization's privacy statement 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 Service Organization's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The Service Organization uses subservice organizations to provide trading related services, print and mail client statements, application development and maintenance, hosting services, monitoring of enterprise-wide security events and alerts, and assisting with incident management support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the Service Organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by 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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the Service Organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Service Organization's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service organization's responsibilities

The Service Organization is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved. In Section II, the Service Organization has provided the accompanying assertion titled



"Management of Paychex, Inc.'s Assertion" ("assertion"), about the description and the suitability of the design and operating effectiveness of controls stated therein. The Service Organization is also 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditors' responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls 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 our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service

commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

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,

a. the description presents the system that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that the Service Organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of the Service Organization’s controls operated effectively throughout that period.

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 Paychex, Inc., user entities of the system during some or all of the period October 1, 2021 to September 30, 2022, business partners of Paychex, Inc. subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following ("specified parties"), if applicable:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

pwc

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.



February 10, 2023

SECTION II

Management of Paychex, Inc.'s Assertion

PAYCHEX

HR | Payroll | Benefits | Insurance

Management of Paychex, Inc.'s Assertion

We have prepared the accompanying description of Paychex, Inc.'s Flex Retirement Services, Payroll, and Reporting Services system (the "system") titled "Paychex, Inc.'s Description of Its Flex Retirement Services, Payroll, and Reporting Services System" throughout the period October 1, 2021 to September 30, 2022, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide user entities with information about the system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that Paychex, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and processing integrity ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, *Trust Services Criteria*).

Paychex, Inc. uses subservice organizations to provide trading related services, print and mail client statements, application development and maintenance, hosting services, monitoring of enterprise-wide security events and alerts, and assisting with incident management support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Paychex, Inc., to achieve Paychex, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Paychex, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Paychex, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Paychex, Inc., to achieve Paychex, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Paychex, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Paychex, Inc.'s controls.

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

a. the description presents the system that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Paychex, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Paychex, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Paychex, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Paychex, Inc.'s controls operated effectively throughout that period.

SECTION III

PAYCHEX, INC.'S DESCRIPTION OF ITS FLEX RETIREMENT SERVICES, PAYROLL, AND REPORTING SERVICES SYSTEM

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Paychex, Inc.'s Description Of Its Paychex Retirement Services, Payroll, and Reporting Services System

Company Overview

Business Description

Paychex is a leading provider of integrated human capital management (HCM) solutions for human resource (HR), payroll, benefits, and insurance services for small to medium-sized businesses. As of May 31, 2022, Paychex served greater than 730,000 payroll and Professional Employer Organization (PEO) clients. In fiscal 2022, the Company reported over $4.55 billion in service revenues. Payroll processing is a key aspect of the Paychex service portfolio.

The Company's payroll services include the calculation, preparation, and delivery of employee payroll checks, and production of internal accounting records and management reports. Payroll services also include preparation and filing of federal, state, and local payroll tax returns, and the collection and remittance of clients' payroll obligations.

Paychex Flex®

Paychex Flex is the proprietary HCM software-as-a-service ("SaaS") platform that helps clients manage the employee life cycle from recruiting and hiring to retirement, providing an integrated suite of solutions including recruiting, onboarding, HR, time and attendance and employee benefits. It uses a single cloud-based platform, with single client and employee records. Clients can select the modules they need and easily add on additional services as they grow. In addition, Paychex Flex presents function-focused analytics throughout the platform, providing HR leaders with data to make informed business decisions. Paychex Flex uses a device-independent design throughout the HCM suite, which allows full functionality of all application components, regardless of device or screen size. Paychex mobile applications add greater value and convenience for clients and their employees by allowing them instant access on their mobile device.

Paychex Flex technology and 24/7 service platform make it simple to run payroll online; automatically calculate, pay, and file federal, state, and most local payroll taxes; and allows employees to initiate a wide range of self-service actions. Paychex Flex technology is delivered through various types of infrastructure technology and hosting services within the Paychex data centers. Paychex IT Operation teams and IT security teams monitor the infrastructure 24/7/365.

Paychex Flex Retirement Services, Payroll, and Reporting Services System

Paychex Flex Retirement Services, Payroll, and Reporting Services System is a subset of services offered to Paychex Flex clients consisting of Retirement Services, Payroll, and Reporting.

Retirement Services

Retirement Services is a recordkeeping and reporting service that includes plan installation; compliance testing; preparation of Form 5500; preparation of summary plan descriptions and summary annual reports; loan, contributions, distributions and asset transfer processing; and quarterly statements for both clients and plan participants. These quarterly statements, including the year-end statement, provide participants and clients with detailed information about their assets and how they are invested. The term client used throughout this report in connection with Retirement Services refers to both individual plan sponsors of single-employer plans record kept by Paychex, Inc. and employers who have adopted and participate in the Paychex Pooled Employer 401(k) Plan, as applicable

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Client participants can use the Paychex Flex application Retirement Services (Participant Web) to create or change their password, review investment balances, submit investment election changes, request transfers between available investment options, submit deferral percentage changes, request a distribution and/or distribution paperwork, request a loan and/or loan processing documentation, and make a one-time loan payment via ACH.

Payroll

Payroll services include the calculation, preparation, and delivery of employee payroll checks, and production of internal accounting records and management reports. Payroll checks, direct deposit summaries, and other output reports, including journals, summaries, and tax deposit notifications, are provided to clients. Payroll processing service is provided through the payroll application in Paychex Flex ("Payroll Center"). Payroll Center is a self-service internet payroll application which facilitates the submission of payroll online to be processed by the Core Payroll application.

Testing of Key Reports

Inquiry, observation and/or inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description to assess the accuracy and completeness (reliability) of the information utilized in the performance of our testing of the control activities.

The related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions, including the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities used within the operation of controls was assessed for the following listing of key reports prepared by Management.

Subservice Organizations

Paychex uses the following subservice organizations to perform a range of services. The controls for the services provided by the subservice organizations are not included in the scope of this report.

Subservice Organization Name	Service Provided
Merrill Lynch	Retirement Services: Trading-related services
Fidelity Investors	Retirement Services: Trading-related services
Federated Investors	Retirement Services: Trading-related services
Legg Mason Partners (10/1/2021-2/7/2022)	Retirement Services: Trading-related services
Transamerica	Retirement Services: Trading-related services
Mid Atlantic Trust Company	Retirement Services: Trading-related services, Custodial and Trust services
RR Donnelley (10/1/2021-6/30/2022)	Retirement Services: Print, and mail statements
Venture Solutions (7/1/2022-9/30/2022)	Retirement Services: Print, and mail statements
SunGard Data Systems ("SunGard")	Retirement Services: Develop and maintain the SunGard-OmniPlus application

Subservice Organization Name	Service Provided
Herjavec Group/ Cyderes	Monitoring of security events and alerts, and assisting with incident management support
Microsoft	Hosting services and support for Paychex Flex Assistant

Scope of this Report

Paychex, Inc.'s ("Paychex" or "the Company") management is responsible for identifying the systems and the trust services categories that are in scope for this report. This report has been prepared to provide information on the overall effectiveness of Paychex in areas that may be relevant in assessing the internal controls of the system used by clients of Paychex.

The scope of this report is limited to the Paychex Flex Retirement Services, Payroll, and Reporting Services System associated with Retirement Services, Payroll, and Reporting Services. These are made up of multiple end-user applications described below, along with the associated principal service commitments and system requirements, and the related controls to meet the applicable trust services criteria for the security, availability, and processing integrity categories as sets forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentially and Privacy (AICPA, Trust Services Criteria)* for the period October 1, 2021 through September 30, 2022. Subservice organizations, along with the technology and controls supporting their applications, are not in the scope of this report.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Principal Service Commitments and System Requirements

Paychex makes service commitments to its external users and has established system requirements as part of the Paychex Flex Retirement Services, Payroll, and Reporting Services system. Paychex is committed to protecting the security, availability, and processing integrity of their data for clients, employees, and partners. Paychex is responsible for its service commitments and system requirements, and for the design, implementation, and operating effectiveness of controls within the system to provide reasonable assurance that Paychex's service commitments and system requirements are achieved.

Paychex communicates its service commitments to external users through documentation of the description of its system and service offerings on Paychex's website, the Security Whitepaper document, and Paychex Service Agreements.

The principal service commitments related to the security, availability, and processing integrity categories include, but are not limited to:

- Logical access controls are designed so that only authorized users are permitted access to systems and applications. Formal processes and procedures guide system access requests for changes and removals.
- Use of domain controllers, firewalls, and intrusion detection systems, as well as anti-virus and anti-malware tools, and vulnerability assessments to protect customer data.
- Data replication controls for the availability of data.
- Disaster recovery and business continuity controls relating to continuation of business activity during an interruption in service.
- Responses to incidents are guided by priorities defined based on urgency and impact.
- The Paychex Fusion Center provides 24x7x365 monitoring to identify, analyze, and remediate security alerts.
- The Paychex IT Operations Center (ITOC) provides 24x7x365 network monitoring to identify and report disruptions on system performance and availability on a timely basis.
- Paychex processes client payroll information completely, accurately, and timely.
- Paychex processes plan activity and transactions for Retirement Services completely, accurately, and timely.
- Paychex provides complete, accurate, and timely reports.

The commitments outlined above are part of Paychex's principal service commitments which apply to the majority of their customers. Commitments that differ from these principal service commitments are not covered by this report.

Paychex establishes operational requirements that support the achievement of security, availability, and processing integrity commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Paychex's system policies and procedures and system design documentation. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of

the Paychex Flex Retirement Services, Payroll, and Reporting Services system. These requirements are further identified and described in the sections below and the associated controls are defined and mapped to the applicable AICPA Trust Services Criteria. The principal service commitments and system requirements drive the operation of the system and the evaluation of whether controls were in place and suitably designed, when considering the applicable Trust Services Criteria.

Paychex performs an assessment at least annually to identify and document key system information required to support internal controls and the achievement of Paychex's service commitments and system requirements (CC2.1.3).

System Boundaries

The boundary of the system is defined as the physical and logical perimeter of that portion of an entity's operations that is used to achieve management's specific business objectives of a system. The boundary includes the components of the system for which the entity is responsible and does not extend to the services provided by the carved-out subservice organizations.

Clients communicate their payroll information to Paychex for processing either via email, telephone, fax or via Payroll Center. The payroll submitted via all methods is processed through the Core Payroll application which is one of the Paychex Flex applications and is hosted by Paychex.

Retirement Services receives information from each Paychex payroll branch multiple times per day and directly from non-payroll clients. Client information, employee census information, notification of employee termination, and wages, hours, and deductions are transmitted to Retirement Services and stored in Retirement Services' systems, which are hosted by Paychex. These systems process the information transmitted from the branch or sent by the client and perform the necessary recordkeeping functions. Paychex uses subservice organizations to perform a range of services. The controls for the services provided by the subservice organizations are not included in the scope of this report.

Clients can access output reports via the Analytics and Reporting application, which pulls together data from Payroll Center and/or Retirement Services (PI1.4.3).

Paychex utilizes third-party subservice organization Microsoft Azure to provide hosting services and support for Paychex Flex Assistant. All other Paychex Flex Retirement Services, Payroll, and Reporting Services systems are hosted by Paychex. The controls of Microsoft Azure are not in the scope of this report.

The boundaries of the system addressed by this SOC 2 report are defined as the Paychex Flex Retirement Services, Payroll, and Reporting Services systems, which include the following layers of technology:

- The network that secures access to the system
- The hardware on which the system is housed
- The operating system used to manage the functionality of the hardware and systems installed therein
- The databases in which data is stored
- The applications in which data is processed

Network diagrams are reviewed and updated to ensure they accurately describe connections to wireless networks and sensitive information (CC2.1.4). Paychex posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users via procedures and control narratives, and on the internet, in-app

user guides and published white papers for external users (CC2.2.3). Additional information on system components are described below.

COMPONENTS OF THE SYSTEM

The components of the Paychex Flex Retirement Services, Payroll, and Reporting Services System used to provide the services within the scope of this report are as follows and described below:

- Infrastructure – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.
- Software – The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People – The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system.

Infrastructure

The Paychex Flex Retirement Services, Payroll, and Reporting Services System uses various software components as part of its hosting infrastructure, such as operating systems and internal management tools, to support its hosting operations. The internal tools deployed in the hosting environment support security, monitoring, incident management, and networking and utilize a range of operating system software. Paychex utilizes the third-party subservice organization Microsoft Azure to provide hosting services and support for Paychex Flex Assistant. The controls performed by Microsoft Azure are not in the scope of this report.

The Paychex team accesses the platform infrastructure through their organization-supplied laptops or mobile devices either by connecting to the network in offices directly or remotely through a Virtual Private Network (VPN) gateway using Advanced Encryption Standard (CC6.6.2). The Paychex network is based on Windows Active Directory.

Access to privileged accounts is through multifactor authentication and is automatically enforced on a time-limited basis.

Paychex has two production Data Centers (DCs) located near Rochester, NY. These DCs house all significant computer operations and data processing activities and maintain identical data for all in-scope applications. Paychex Flex Retirement Services, Payroll, and Reporting Services System applications span multiple systems residing in both DCs. Systems are comprised of enterprise class servers using a variety of operating systems such as Windows and Linux. Paychex maintains a data backup and a data restoration policy that defines procedures and standards for data backups for all critical IT systems (A1.2.6). Paychex

duplicates backup data from one DC to the other DC and is also able to failover to the alternate data center in the event of a disaster (A1.2.3 & A1.2.4).

Paychex identifies, documents, and reviews server inventory through the Foreman tool. Assets are tagged with an asset number which is used to log, track and maintain inventory (CC6.1.2). Equipment slated for disposal, return, or reuse is wiped of data via degauss, reformat, or destroyed as per Paychex Standards and tracked in ServiceNow tickets. Hard copy media slated for destruction is dropped into locked and labeled specialized media bins located through-out Paychex facilities, cross-shredded or burned, or securely delivered to third-party vendor collection and disposal services (CC6.5.1).

The DC facilities are managed by the Paychex PD&IT function described below.

Software

Paychex uses various applications to support the operations of Paychex Flex Retirement Services, Payroll, and Reporting Services System. The Retirement Services, Payroll, and Reporting Services are each supported by multiple applications described below.

Retirement Services

- Retirement Services (Participant Web), a Linux-based application using Oracle and MongoDB databases, covering a range of services over retirement plans, including plan set-up, administration, and enrollment. Also used by client participants to view and manage their plan information and elections.
- HRIS, a Windows-based application, is used as a recordkeeping product administration database in Retirement Services. This is the system of record that tracks plan-specific information for Paychex clients and client employees.
- TITAN, a Java process in a Linux environment, is used to receive and send pertinent data between Retirement Services and the payroll branches.
- SunGard-OmniPlus, a UNIX-based vendor application, is developed and maintained by SunGard Data Systems (“SunGard”). The vendor provides new releases and periodically updates existing releases of the applications. Changes to SunGard-OmniPlus (primarily limited to updates and patches) follow the standard Paychex change management process. The system infrastructure is maintained by Paychex. This is the system of record for financial transactions on all retirement plans at Paychex.

Payroll

- Core Payroll, a Linux-based application. Paychex employees connect to the Core Payroll application from their respective branch over the network and make updates to client payroll information for payroll processing.
- Payroll Center, a Linux-based application using an Oracle database which facilitates submission of payroll online to be processed by the Core Payroll application, and where clients can access payroll reports and data. Clients can enter employee hours, calculate payroll taxes, and keep up with wage and hour laws.

Reporting

- Analytics and Reporting, a Linux-based application using Oracle Enterprise Reporting Database (ERD), where users can generate data and reports. Paychex Flex offers 24/7 access to a library of over reports across payroll, HR, benefits, and accounting.
- Human Resources, a Windows-based application using a Microsoft SQL database, used for tracking performance reviews.
- People, a Linux-based application using an Oracle database, a directory used for accessing employee data such as name, address, salary, and employment status.
- User Access, a Linux-based application using an Oracle database, used for managing client user access. The Paychex Flex landing page offers a single sign on page for both employees and administrators to access multiple products.
- Company Details, a Linux-based application using an Oracle database, contains company details such as company logo, legal name, street address, federal ID, internal organizational structural, tax information, and bank accounts.
- Documents, a Linux-based application, is a document repository which allows end users to have access to documents from multiple Paychex Flex applications in a centralized area. This simplified process allows clients to easily convert and store their current physical forms and records to a centralized document storage repository.
- Paychex Flex Assistant, a chat bot program hosted using a third-party cloud service. Paychex Flex Assistant is available for clients to help answer a set of standard questions when users contact Paychex online via the Chat feature. Users will chat with Paychex Flex Assistant just like they would with a live person.

The ability to install software is restricted to privileged users only. Any exceptions to the policy must be requested in ServiceNow tickets and approved by the individual's manager and granted by Security (CC6.8.1). Paychex uses various tools to support the ongoing operations of the system. These tools are described in relevant sections below.

People

The Paychex Flex Retirement Services, Payroll, and Reporting Services system is supported by the following groups, described below:

Paychex Flex Retirement Services, Payroll, and Reporting Services System

Paychex Flex Retirement Services, Payroll, and Reporting services are provided by Paychex personnel. The Paychex teams are also dependent upon and supported by Paychex internal support services: Talent Acquisition (consists of all aspects of Human Resources (HR) including: recruiting, performance management, resource scheduling, etc.), Information Technology, Operations, Enterprise Security, Network Engineering, Security Fusion Center, and the Security Risk and Compliance team.

Paychex maintains the Enterprise Security department to oversee its security program. The Security department is headed by Paychex's Chief Information Security Office ("CISO"), who reports to the Paychex's Chief Information Officer ("CIO"). Responsibility for security and availability falls under the CISO to meet the responsibilities. The Enterprise Security Fusion Center (ESFC), Product Security, Security Engineering, and IT Governance, Risk & Compliance leaders report to the CISO.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Other Paychex teams provide a set of services that comprise Paychex Flex Retirement Services, Payroll, and Reporting Services System. These teams are described in relevant sections below.

Product Development & Information Technology (PD&IT) Function

The Paychex PD&IT function reports to the Senior Vice President of Product Development and Information Technology. The Paychex PD&IT function manages the DC facilities near Rochester, NY and supports the information technology services for various Paychex business units. These processes and controls are managed and delivered as a common set of services to various Paychex business units.

The Paychex PD&IT function is responsible for the charter creation, prioritization, backlog management, design, analysis, construction, testing, and deployment of both internal and external facing applications and websites. They are also responsible for infrastructure planning, server maintenance, web engineering, database administration, architecture, release management, performance testing, and internal support call center. The PD&IT department runs an Agile software development life cycle that consists of Agile teams of five to nine software developers and test engineers managed jointly by a product owner, a scrum master, and a solution lead.

The PD&IT function at Paychex consists of the following four areas responsible for the availability, security, and processing integrity of Paychex systems and applications:

- Product Development – Responsible for using the charter and daily collaborating with the product owner in an Agile software development life cycle to define, design, plan, build, and test user stories from a prioritized backlog in a series of two-week sprints. Each Agile team participates in defining user stories in conjunction with the Product Owner, designing the solution in conjunction with the solution lead, building the solution, creating automated test scripts, and performing manual testing through both defined test cases and exploratory testing. The Product Development teams include the Systems Development and Test Engineering teams, which are responsible for software, as well as testing and implementing software systems supporting the business units. The Systems Development and Test Engineering team members are organized by product and role. Developers and Testers are assigned to project teams based on project needs and priorities.
- IT Operations – Responsible for providing the physical and logical computing and network infrastructure to help ensure the availability, reliability, and flexibility of the DCs and the corporate facilities. The group encompasses Enterprise Support, IT Infrastructure and Architecture, Performance, and Tools, IT Release Services, and Corporate Business Applications. Enterprise Support is responsible for problem resolution, education, and project representation. Enterprise Support also serves as the Lead Contact during business continuity scenarios.
- Portfolio Strategy and Implementation – Responsible for managing business and technology projects using industry-accepted project management practices, standards, and techniques. The group identifies, communicates, and manages multiple projects and their impact on achieving future business or technology programs. The group encompasses Technical Product Management, the Program Office, User Experience Design, Usability Testing, IT Contract/Vendor and Financial Management, Business Process Automation, and Business Operations Migration and Load.
- Enterprise Data and Systems Security – Responsible for developing and managing best practice methods, procedures, and technologies necessary for the life cycle protection of information assets. This group is responsible for risk management, architecture, engineering, assessment, incident response, transmission, administration, and compliance management functions that monitor and defend data from inception through destruction.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Retirement Services

Paychex Retirement Services is organized into groups that support the administration of qualified, defined contribution retirement plans. Management teams consisting of managers and supervisors are established and monitor the quality of internal control performance as part of their normal job functions. Employees performing similar functions are grouped under the same management teams to help ensure consistent management monitoring and oversight practices. Performance management goals are established and evaluated to determine that employees and management teams understand and fulfill their control and monitoring responsibilities. Senior management teams are organized as follows:

- Sales Implementation – Conversion and plan activation (responsible for new/conversion plan setup)
- Customer Service – Responsible for servicing customers and plan participants
- Transaction Integrity – Responsible for processing contributions and loan repayments, distributions and loans, trading, pricing, dividends, and position reconciliation
- Engineering – Responsible for IT-related activities, including software development and database maintenance

The groups are overseen by either supervisors or managers who report to senior level management.

Payroll Services

Paychex offers payroll processing through different locations throughout the United States. Each location is similar in staffing and responsibilities and may offer multiple payroll products.

- Implementation Team – Completes the setup of the new client in the respective payroll application. The Implementation Team is responsible for the setup, training, and successful implementation of the new client.
- Payroll Specialist (PRS) – Responsible for all aspects of quality client service. The PRS assists the clients with payroll input, verifies totals, and resolves client issues.
- Client Service/Implementation Supervisors – Supervise and direct a group of PRSs and Implementation Specialists in providing payroll services to the clients. The Supervisors schedule staff, and assign, direct, and monitor the work of assigned personnel to help ensure quality client service.
- Client Service/Implementation Managers – Oversee the Client Service/Implementation Supervisors and all aspects of customer service and implementation, respectively.
- Branch Managers – Oversee all operations within the branch location and they establish, maintain, and oversee staffing, management systems, sales, and client relations. The Branch Manager reports on sales, losses, expenses, and business performance objectives. They monitor key processes in order to achieve branch sales and revenue targets such as expansion of client bases, client retention, and quality service.

Paychex has separate processing and fulfillment centers that serve multiple branches at one time. These processing and fulfillment centers are similar in staffing and responsibilities. Some branch locations may still process and print client payrolls directly in their own location instead of going through the separate processing and fulfillment centers.

- Computer Operators – Maintain and operate branch production computer processing and printing systems. They monitor the servers and process the incoming payrolls to successful conclusion. The

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Computer Operators identify payroll processing failures and report them to Enterprise Support and the Client Service/Implementation Supervisors for resolution. Computer Operators coordinate the payroll workflow with Fulfillment Specialists in order to meet daily production requirements.

- Fulfillment Specialists – Assemble payroll packages for delivery and perform other fulfillment-related tasks. They assemble payroll packages according to client number and prepare for delivery based on client specifications. They coordinate and perform timely daily posting of mail and overnight labels and complete all package checklists and confirmations in order to maintain accurate tracking and the security of printed payroll packages.

- Quality Process Supervisors – Oversee all aspects of branch computer operations to help ensure the accuracy and quality of the final payroll products. They supervise a staff of Computer Operators and Fulfillment Specialists. They assign and monitor the work of assigned personnel to help ensure quality and productivity standards are met in the production, packing, and delivery of payrolls to clients. They assist with computer operations when necessary and address operational problems or calls to Enterprise Support to ensure proper resolution.

- Processing Center Managers – Supervise processing and fulfillment center staff and oversee all operations within the facility. They establish, maintain, and oversee staffing, management systems, computer processing, and payroll package fulfillment for multiple branches. They also create fulfillment and operating strategies to ensure that Paychex standards of product quality are met or surpassed.

Procedures

Paychex has documented policies and procedures that establish what is expected and required of its employees. These policies and standards are available on internal sites and can be accessed by Paychex employees at any time. Security policies and standards are updated and reviewed periodically, and approved by the CISO, Security Governance Counsel, senior officers, and CEO depending on significance of the updates being made (CC5.3.1).

Paychex maintains a comprehensive information security program which includes policies, standards, and procedures. This program is influenced by several industry guidelines and leading practices including NIST, COBIT, ITIL, SOC and the Shared Assessments Program. Paychex's CISO is responsible for this program. On a monthly basis, the CISO, CTO, and CIO are presented with a Security Program Update (SPU) including key security and availability metrics, events and incidents where relevant. As part of these meetings, risk assessment updates, risk assessment calendars and identified threats, and action items are also discussed (CC2.2.11).

Paychex IT leaders meet on a regular basis to consider strategic and tactical direction for the information security policies, standards, and procedures.

Information security policies are drafted with input from internal cyber security resources and are based upon industry leading practices. The drafts are reviewed and approved at least annually by Paychex's senior leadership, and the CISO. Once approved, the policies are published internally and communicated to personnel.

Written Paychex Flex Retirement Services, Payroll, and Reporting Services system processes and procedures for operations and security processes are provided to personnel responsible for operation of the system. Designated personnel update the processes and procedures based on changes to availability requirements and security policies.

Policies and procedures cover the following key lifecycle areas:

- Assessment of the business impact resulting from business impact analyses (CC2.2.15)
- Selection, design, documentation, and implementation of security controls (CC1.2.3)
- Authorization of, changes to, and termination of information system access (CC6.1.1)
- Monitoring for anomalous activity and cyber-related insider and external threats that pose risk to the business operations through various detection tool including an Enterprise Security SIEM
- Maintenance and support of the security system and necessary back-ups (A1.2.6)
- Security incident response (CC2.2.15)
- Maintenance of privileged access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
- Business use and data storage for mobile devices (CC6.7.2)

These policies and procedures are located on Paychex, Inc.'s intranet for appropriate access (CC5.3.1).

Accountability

Paychex personnel are accountable for understanding and adhering to the guidance contained in the Paychex Information Security Policy and any applicable supporting security standards. Any individual not employed by Paychex (e.g. visitors accessing guest network, contractors or vendors accessing Paychex VPN), but allowed to access, manage, or process information assets of Paychex environment, is also accountable for understanding and adhering to the guidance contained in the Policy and standards. Contractors are held to a professional standard and are supervised by Paychex employees to ensure quality work and professionalism (CC1.1.7).

Logical Access

System security, administration, and monitoring include those controls that prevent and detect unauthorized access to Paychex information systems and data. The Paychex Information Security Policy, approved by Executive Management, defines the fundamental principles for the protection of Paychex information resources and identifies the proper controls to meet or exceed the requirements for regulatory compliance. The Board of Directors and the Executive Management team endorses and enforces the Paychex Information Security Policy. In addition, a framework of security standards has been developed to support the objectives of the security policy. These standards have been implemented throughout the Company and address security issues such as logical access to applications and data, physical access to computing facilities, and monitoring activities (CC1.2.3 & CC6.4.11).

Logical access controls are designed so that only known, authorized users are permitted access to systems and applications based on job responsibilities. Formal processes and procedures exist to ensure system access requests are fulfilled based on the appropriate approvals by system and data owners (CC6.2.1). Unique IDs are provisioned as defined by Paychex's Account Administration Standard (CC6.1.15). Privileged activities are approved by authorized IT management and performed by appropriate individuals (CC6.3.4). All privileged activities are logged in the system and are available for review as required (CC7.1.3). All external client users are given unique user IDs and set up with multi-factor authentication to access Paychex Flex (CC6.2.5). Paychex has documented policies and standards supporting segregation of duties, Least Privileges and Role Based Access (CC6.3.6).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Access Review

Access and permissions are reviewed quarterly by the management team (CC6.2.4). Remote access to systems is allowed to users with permissions to do so and is granted using MFA and an encrypted authentication protocol (CC6.6.2). Terminated individuals' access is systematically removed through the integration between the HR system and AD. Once the AD account is disabled, access to Paychex's network are no longer possible (CC6.2.2).

The AD domain, which governs user account's passwords, and Operating system password policies are configured in line with Paychex Security Standards, which require strong password complexity settings, mandatory periodic password resets, and minimum length. Workstations are configured to automatically lock out after 15 minutes of inactivity (CC6.1.3).

Physical Access & Environmental Protections

Data Centers

Paychex has two production CDCs located near Rochester, NY. Paychex also has a third data center which is considered "warm" near Omaha, NE. These CDCs house all significant computer operations and data processing activities and maintain identical data for all in-scope applications. Applications spanning multiple systems reside in both CDCs. Systems are comprised of enterprise class servers using a variety of operating systems.

Physical access to the CDC facilities is limited to employees with a business need and is controlled by badges and a biometric scanner (CC6.4.1). During business hours, visitors are screened by a security guard or a receptionist located at the main entrances and escorted by an employee during the visit (CC6.4.3). Access to the CDC facilities is granted based upon job function and upon approval by the Network Service Field Engineering Manager (CC6.4.8). Upon termination, employee access to the CDC is removed through the integration between the third-party badge access tool and AD (CC6.4.9). Access to the badge access control system used to grant and revoke badge access is restricted to authorized users in the Facilities department. The Facilities department at Paychex reports up to the President and COO and is responsible for maintaining all of the buildings throughout Paychex. This includes granting and removing physical access to the buildings and the CDCs for new and terminated employees as well as vendors and visitors to Paychex. The Network Service Field Engineering Manager conducts a quarterly review of users with access to the CDC facilities and confirms that access is commensurate with job responsibilities. Discrepancies are resolved in a timely manner (CC6.4.10). Logical access to initiate, modify, or cancel scheduled application batch jobs is reviewed by the Data Center Production Manager on a monthly basis to confirm that access is commensurate with job responsibilities. Discrepancies are resolved in a timely manner (CC6.3.10).

Video cameras are present outside all CDC facilities and are used by security personnel to monitor access to the computer rooms (CC6.4.2). In addition, access to the storage location within each of the CDCs is also controlled through a biometric scanner; access to this location is assigned to employees according to their business function. Other computing facility rooms, including print rooms and communication closets, are secured by keypad locks or electronic card readers.

Preventative maintenance is performed according to schedule on the DC facilities' uninterruptible power supplies, generators, and heating, ventilation, and air conditioning (HVAC) systems (A1.2.1).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Environmental Systems

Each CDC includes temperature-controlled areas, fire suppression systems, an uninterruptible power supply, and a raised floor. The management of the CDCs, including the environmental controls, is the responsibility of PD&IT.

An environmental monitoring system is used to detect issues with the air conditioning, fire suppression, leak detection, and power systems. The monitoring system is configured to capture alarms, threshold, and maintenance alerts within the environment. If an alert occurs, a technician is automatically paged. The CDC acts as a backup to this process. The CDC monitors environmental alerts 24 hours a day, seven days a week. If a technician does not acknowledge an alert within 15 minutes, the CDC follows an escalation procedure to contact the necessary personnel.

The CDCs contain redundant equipment for air conditioning, power, and fire suppression systems. This equipment is tested through a series of preventative maintenance procedures and planned test procedures.

Check Printing, Check Stock, and Distribution Areas

Access to the payroll processing centers, including sensitive areas such as the check printing area, payroll package storage, and check stock rooms, is controlled by physical access systems (i.e., multi-level card access, PIN number). The processing centers are monitored by surveillance cameras and security guards (CC6.4.4).

Access to the sensitive areas is restricted to Paychex personnel and authorized vendors, and access is granted based upon job responsibilities. Payroll packages awaiting delivery by vendors are stored in courier rooms off the check printing area (CC6.4.5). The check stock room is separated from other areas in the payroll processing centers, and access is granted based upon job responsibilities (CC6.4.6).

Network Security, Operational Monitoring and Problem Management

Firewalls, Intrusion Detection Systems (IDS), and Network Address Translation (NAT) are deployed to control and monitor the network and critical networking equipment. These are maintained and monitored by the Security Engineering team, part of Enterprise Security noted above (CC6.1.9).

The Paychex firewall architecture encompasses multiple tiers of firewalls for defense-in-depth and defense-in-diversity. configuration control of the firewall architecture is performed by the Security Engineering team.

Rule sets (firewalls) are developed and maintained for each device to explicitly control authorized and unauthorized traffic. Authorized traffic is permitted, and unauthorized traffic is denied. Requests for comprehensive changes to rule sets are reviewed by the Enterprise Change Management team and, when approved, executed by the Security Engineering team (CC7.1.6).

Security Analysts monitor the operating system and database level alerts, and network-based IDS that are used at the CDCs and at selected nodes of the Paychex WAN. Security Engineering reports all identified security violations to management.

Intrusion Detection and Prevention Systems (IDS/IPS) are in place on the network and are updated for the latest rule set on a regular basis. Network scans are performed periodically to identify issues, which are remediated based on criticality. Remediation performed is validated during the next network scan. Identified security violations are reported to IT management. Violations are researched and addressed (CC7.2.4).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

PD&IT has defined and implemented an incident management system to ensure that operational issues (incidents, problems, and errors) are recorded, analyzed, and resolved in a timely manner (CC7.2.7). An Incident Management methodology is used to help PD&IT provide support for Information Technology products and services. All business unit personnel use a centralized single point of contact (incident management system) to report issues that are outside of standard operation (CC2.2.12). Responses to incidents are guided by priorities defined based on urgency and impact. These are negotiated with business units as part of a service level agreement for service call management between IT and the associated business unit.

Incident Response

Paychex has built an integrated incident response plan to address each type of incident related to security breaches in the Paychex Flex Retirement Services, Payroll, and Reporting Services system environment. The Incident Response Plan describes how various types of security incidents are handled. The Incident Response Plan identifies key resources and communications that will take place based on various incident types and severity levels and identifies to whom suspected incidents should be reported and describe the escalation path from the entry point in the process. Security awareness training is in place to make Paychex personnel aware of their responsibilities concerning the reporting of security incidents (A1.3.2 & CC2.2.14).

The Incident Response Plan is maintained, reviewed within 12 months (contains revision history), approved, includes organization structure, response procedures, timelines for incident resolution, and changes to the system follow the established change management policy (CC7.3.4).

Tabletop exercises are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post incident review is conducted to identify any areas for improvement as well as areas that went well. These findings are used to adjust and improve the procedures (CC7.5.5). On a periodic basis, Paychex engages with third parties to perform security review assessments and penetration testing (CC7.2.9).

For high severity security incidents, a root cause analysis is conducted and discussed with management. Based on the root cause analysis, change requests are prepared and the process and relevant data is updated to reflect the planned incident and problem resolution (CC7.3.4) Weekly meetings are held by the ESFC to discuss new playbooks and standard operating procedures relating to incident response. A Wiki is maintained containing playbooks, training materials and team knowledge articles (CC7.5.3).

Logging and Security Event Monitoring

The Paychex Enterprise Security Fusion Center (ESFC) monitors for anomalous activity and cyber-related insider and external threats that pose risk to the business operations through various detection tool including an Enterprise Security SIEM. The tools provide static log alerting, correlated log detection, anomalous activity, risk-based alerting, machine learning and behavioral analysis. A Managed Security Service Provider (MSSP), Cyderes provides monitoring of security events and alerts and assisting with incident management support (CC7.2.2).

Initial analyses of these alerts determine the priority and urgency for response. In all situations urgent conditions are reported to the Paychex Support organization and follow the problem management process. Less urgent issues are managed either by individual IT functional organizations or cross-functional teams that may create maintenance tasks, small projects, or large projects (CC7.4.4).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Data Encryption

Paychex requires all removable media to be encrypted and password protected as defined in the Encryption of Electronic Storage Devices Including Removable USB Security Standard (CC6.7.1). In addition, data stored on Paychex's storage arrays is encrypted at rest (CC6.1.8).

Paychex takes a risk-based approach to data security, based on data classification and other factors. All data must be secured according to the guidance in ATCS-024: Information Security Classification, ATCS-354: Security Zones and other applicable standards or regulatory requirements (CC3.2.7). Access to cryptographic keys is restricted to the fewest number of custodians necessary (CC6.1.16). Secure file transfer protocols (SFTP) for transmission of confidential and/or sensitive information over public networks are restricted based on job responsibility (CC6.7.4).

Vulnerability Management

Paychex's Security Assessment and Vulnerability management team performs annual penetration testing and regular vulnerability scans across the infrastructure and networking components. Vulnerability scans are conducted on internal and external networks to detect new and un-remediated vulnerabilities. IT Operations receives regular reports and any "Critical" or "High" rated vulnerabilities are researched and remediated timely (CC7.2.9).

Internal network vulnerability scans are performed daily, and weekly as scheduled, monthly database vulnerability scans are also performed. External scans are performed as needed. Results are assessed and triaged and vulnerabilities are documented as tickets and assigned to the appropriate teams and tracked through resolution (CC7.1.2).

Anti-virus and Anti-malware Management

Anti-virus solutions and anti-malware detection software are implemented on Paychex team members' computers and Virtual Machines (VMs) and updated frequently. Anti-malware alerts are reviewed individually on a risk-prioritized basis to identify potential anti-malware activity. The network operations group receives a report of devices that have not been updated in stipulated time and follows up on the devices.

Antivirus and malware technology is deployed to prevent malicious attacks. If required, vulnerability and security related incident tickets are opened, and corrective actions are implemented in accordance with defined policies and procedures (CC6.8.4).

Change Management

All changes to the production system (application, hardware, operating system software, and database changes) are controlled through a formal change management process to ensure that necessary review and approval occur. All significant modifications to the application infrastructure are managed within a project, using a defined Paychex Project Process. Portfolio Strategy and Implementation is responsible for identifying significant initiatives and aligning them with the appropriate project management methodology and standards (CC8.1.1). Changes are documented and tracked in a Change Request (CC8.1.2).

Typical change profiles include:

- Development of new software applications
- Installation of purchased software packages
- Deployment of technology infrastructure

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

- Periodic release of minor enhancements, bug fixes, maintenance, and regulatory changes

The Paychex Project Process is aligned with the formal change management process at key checkpoints throughout the project, with a Project Manager or Product Owner having responsibility for ensuring that changes are properly communicated and approved before implementation (CC8.1.9).

The Project Manager or Product Owner has ultimate responsibility for the delivery of the change. Projects follow an Agile software development life cycle model, which allows for customization depending on the needs of the project. There is a defined set of minimum Project Management Standards that includes a project definition, defined requirements, testing strategy, and a project work plan. The Project Office, part of the Portfolio Strategy and Implementation group described above, regularly monitors that all projects adhere to the defined set of minimum standards and a periodic review of compliance to the standards is performed by the Director of the Enterprise Program Office.

Projects are initiated by the respective business unit or by Product Management. They are then prioritized by a cross-functional group with input from executive management, Product Management, Sales, Operations, and Information Technology. Business units are represented throughout the project and participate in requirements sessions, requirements walkthroughs, project status updates, and user acceptance testing, as needed. Regular project status is provided to the business units by the Project Manager and through the monthly Portfolio Review conducted by the Enterprise Program Office.

Product Development is responsible for the design, development, and testing of software applications that support the Paychex business units. They follow a defined Software Development Process (SDP) that provides guidelines for making and testing program changes and allows for customization, depending on project need. This process documentation is accessible via the Paychex intranet. Additionally, Product Development uses version control tools to manage software development at Paychex (CC8.1.12). Managers within Product Development are responsible for reviewing projects within their application areas to confirm adherence to this process. In addition, there are published standards for developing systems and applications that can be referenced on the Paychex intranet. The Manager/Solution Lead is responsible for monitoring compliance with these standards; their approval within the change management process confirms that program changes comply with these standards. Members of the Product Development department also lead and participate in publishing and implementing standards for software development.

Product Development follows a defined testing process for all changes to application and operating systems. The Managers and Leads for each application area are responsible for reviewing and monitoring compliance with the testing process. Sign-off on completion of testing is monitored via the change management process.

The Development Agile Team is responsible for producing test scripts. The Test engineers on the team verify that the new functionality is working as documented in the requirements and that all known defects are identified and resolved. During this phase any applicable system, conversion, or regression testing is completed. The Test Engineering tests are performed using a test environment that is representative of the production environment. Program application changes are checked for errors and modified as needed through the formal change management process.

The business unit determines whether user acceptance testing is warranted. If so, the business unit is responsible for defining the test plan and performing the tests. The business unit is responsible for maintaining their test documentation for an appropriate period of time.

For projects where performance is critical or there is a high volume of transactions, load and stress testing is performed. The testing evaluates the compliance of a system or component with specified performance requirements. Often this is performed using an automated test tool to simulate a large number of users.

These tests are performed according to a test plan and are most often performed by the Architecture, Performance and Tools team within IT Operations (CC8.1.10).

Infrastructure changes, which include operating system and database changes, are managed by the respective IT Operations functional teams. Testing by IT Operations is performed and sign-off of testing activities is captured within the related ServiceNow change record. IT Operations management is responsible for reviewing and monitoring compliance with testing requirements.

After testing is complete, the software is ready for turnover to the Release Management group within IT Operations. This group is responsible for releasing application changes into the production environment. Changes are then migrated from the test environment to the production environment.

For all changes, after a period of time to monitor the change in the production environment, the change request is updated to indicate completion status, either complete with or without incident. This is performed by Change Management or Release Management and is typically done within a week of implementation (CC8.1.13).

All changes to the production environment follow the normal change management process, with the exception of emergency changes. Emergency changes are changes that require an immediate change to be made within the same business day or prior to the next business day, and which are required to either restore interruption in service or prevent an imminent interruption in service, and no sustainable work-around is in place. For all emergency changes, given the urgency of the situation, verbal, rather than written authorization and approvals may be granted before the change is implemented. After the change has been implemented, a formal Change Request is completed and signed off.

Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation (CC8.1.5).

Paychex has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements (CC8.1.8).

Change Advisory Board meetings are held daily. Meetings are held to review any comprehensive change requests submitted, including prior approvals and testing performed, and if approved are moved to production, any unapproved changes undergo further refinement. Approvals are documented within the ServiceNow ticket (CC8.1.14).

Security-based testing is performed to verify application code changes and identify code vulnerabilities as part of the change management process (CC8.1.11).

Patch Management

Operating system (OS) and database patches are applied to systems at Paychex to address issues or potential issues in the production processing and control environment. The OS patch management process is owned by the IT OPS – Infrastructure Systems team. The Database patch management process is owned by the IT OPS – Data Services team.

A system configuration tool (e.g. Microsoft SCCM, NetIQ SCM, etc.) and/or vendor alerts are used to identify available patches. The system configuration tools compare the current system patch configuration with the Paychex minimum security baseline and patch release list from the vendors. The results of that comparison are analyzed to determine what patches will be installed on the Paychex systems. Security patches are evaluated to ensure that relevant security vulnerabilities are mitigated as soon as possible (CC7.1.1 & CC7.1.2).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

The Paychex change management process is used to evaluate, test, and install operating system and database patches into the production environment (CC8.1.15).

Data Backup and Restoration

A Data Protection tool, NetBackup, is used to duplicate Paychex backup data from one Paychex Data Center location to a secondary Paychex Data Center. In the event a system restore is needed, the Offline team will recall the duplicated data from the secondary Data Center (A1.2.4).

Data Domain appliance storage systems and the backups stored within use EMC Data Domain Replicator technology which ensures the quality and effectiveness of backup media. With Data Domain Replicator technology, the replication of data occurs much faster than tape, without the risk inherent to tracking and handling tapes. The majority of the backup environment utilizes NetBackup appliances and uses Auto Image Replication (AIR). AIR enables the replication of backup images from one NetBackup domain to another and is managed through Storage Lifecycle Policies. Replication is more secure than physical tape and also allows for tertiary copies (A1.2.3).

Data Storage and Retention

A records and information management program is in place, which includes applicable record retention schedules defined and classified by record types, retention periods, and type of allowable storage media for each. The purpose of the Paychex Records Management Program ("RMP") is to:

- Provide an organized and effective life cycle management program of company business records, from generation or receipt to final disposition
- Protect records necessary to Paychex and subsidiary operations
- Support compliance with government regulations and legal requirements for data retention
- Reduce cost of maintaining and storing records
- Support industry best practices (CC6.5.2)

Disaster Recovery/Business Continuity Management

Business Continuity Plans (BCPs) have been developed and are maintained for all mission-critical and business-critical functions within Paychex. The BCPs document plans for the continuation of business activity during an interruption in service. All recovery plans for non-automated business processes are maintained in separate manuals by each business unit. Business unit plans help ensure that the business is prepared with the necessary communications and procedures in place to minimize impact. Within the plan, each point of failure is identified, and steps are documented to restore functionality, duplicate functionality, or provide suitable (even if reduced) alternate functionality. Technical components of the recovery plan, such as platform cutover steps, are stored electronically.

In addition, Paychex maintains a Paychex Recovery Command Team Guide. This guide is activated when the projected recovery time frame exceeds the maximum acceptable downtime or the recovery time frame for the production site or systems is not known for multiple critical functions at any Paychex facility. The objective of the Paychex Recovery Command Team Guide is to ensure that:

- An incident command team structure is in place to manage any size recovery effort.
- Essential personnel are identified and documented.
- Critical information, both electronic and hard copy, is copied and maintained off-site.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

- Critical equipment is monitored and recoverable.
- Employees have a place to perform critical functions.
- Voice communication is available and data connectivity is provided to LAN/WAN and mid-frame operations.
- A detailed plan, tested regularly, is in place for performing functions in recovery mode.
- Decision-makers and public relations personnel are available and ready to respond, as necessary.

Business continuity testing is performed every 18 months using live events, or realistic simulations. Every 18 months, disaster recovery tests including failover to alternate data centers are performed to ensure critical IT systems are tested to ensure resilience (A1.3.1).

Monitoring

The Paychex IT Operations Center (ITOC) monitors system availability on an ongoing basis through automated alerting and implements corrective action in a timely manner. Host availability, disk usage, CPU and memory are closely monitored by setting thresholds. If the threshold is passed, a ticket is opened and alerts the appropriate team of the issue, so the proper steps can be taken to resolve the issue (CC7.2.7). Paychex utilizes AppDynamics to monitor performance of applications as well as latency. Any flagged issues are documented in ServiceNow and resolved in a timely manner (A1.1.3). Paychex monitors significant movements of data using various data loss prevention and security management tools. Suspicious activity is flagged via automated rules which is investigated and entered into tickets for security incident response as applicable (CC6.7.3).

Paychex leverages the DCs to host primary and redundant network virtual appliances to create a highly available and resilient network and connectivity infrastructure.

Data input to applications and databases is validated via automated jobs to ensure that data is input complete and accurate. Issues are logged, researched, and corrected as needed (PI1.2.1). In accordance with a defined schedule, data input to applications and databases is validated via monitoring to ensure that data is processed. Failures trigger automated alerts and are investigated and resolved in a timely manner (PI1.3.1). Production job schedules are maintained and updated by the Scheduling Team. Job schedule modifications are requested by appropriate personnel based on job responsibilities (PI1.3.4). Management has defined and implemented an incident management system to monitor jobs and identify, log, and resolve failed jobs (i.e., incidents, problems, and errors) (PI1.3.2).

Processing Capacity and Usage

Paychex has documented capacity management procedures and best practices and communicates to procedures to employees via the Paychex intranet (A1.1.2). Paychex maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet usage requirements. Paychex monitors capacity in an internal dashboard that utilizes an 18 month backward perspective analysis used to forecast out for the next 6 months (A.1.1.1).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Processing Integrity

Retirement Services

Paychex Retirement Services uses an integrated and automated approach to process plan activity. Transaction processing includes various controls and documented procedures to help ensure the authorization, timeliness, and accuracy of transactions processing.

The following financial and non-financial transactions are processed:

- Plan Setup and Maintenance
- Participant Data/Enrollments
- Contributions/Loan Repayments
- Transfers Between Available Investment Options
- Distributions/Loan Issuance
- Dividend and Daily Earnings
- Daily Plan and Participant Account Valuation
- Daily Processing/Trading
- Reconciliations
- Reporting

Plan Setup and Maintenance

Working with the Paychex Sales Representative, the Plan Sponsor provides the data necessary for plan installation via the new client profile and a comprehensive electronic questionnaire. The Plan Sponsor selects plan features, authorizes a plan adoption agreement, and executes an administrative service agreement, which outlines the terms and conditions for the service. Once finalized, the electronic contract is automatically uploaded to the recordkeeping system where it is reviewed by a dedicated specialist prior to activation (PI1.1.9).

Retirement Services has dedicated specialists that set up new and converting clients. These specialists review documents and plan requirements and ensure authorizations are properly executed. Selected plan provisions are updated in the recordkeeping systems and data integrity checks are performed to verify the accuracy of the information (PI1.2.7). System access to set up new plans is provided to a limited number of Human Resource Services (HRS) Specialists. Upon completion, the client receives a welcome package and copies of the summary plan description and other plan materials. Authorized client personnel, usually the Plan Sponsor, contact the Client Service Center with any future plan changes and HRS Specialists execute the changes based on the request.

Participant Data/Enrollments

Once the participant has been set up in HRIS, subsequent participant-directed enrollment instructions, including deferral percentages and investment elections, are received directly via paper enrollment forms or online (Participant Web and mobile app enrollments). For participant elections requested through the Participant Web, the participant's username and password/PIN are required for authorization. The Participant Web and HRIS systems have built-in edit checks to verify the total investment election entered equals 100%, and that salary deferrals requested are within plan parameters (PI1.3.13). A confirmation summary of the participant's account elections and subsequent account changes is generated automatically

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

by the system and sent directly to the participant (via email or hard copy). Additionally, users of the Participant Web who initiate transactions receive an online confirmation statement summarizing investment elections and any changes made to their account after submitting a transaction online through the Participant Web (PI1.4.6). The majority of participant enrollments are submitted via the Participant Web. All subsequent enrollment changes by the participant are transmitted back to the respective Paychex payroll system. For non-Paychex payroll clients, Paychex sends notification of the change to the client with instructions to view the details on the specific participant's change via the website.

Retirement services transactions on SunGard and HRIS are accurately logged, including the date, time, and name of the individual who initiated the transaction. An HRS Specialist performs a monthly quality control review on a sample of investment elections and deferral percentage changes input manually to HRIS from the enrollment form. Any discrepancies are researched and corrected in a timely manner.

Contributions/Loan Repayments

Contribution transactions are identified as employee deferrals, employer contributions, catch-up contributions, or loan repayments. For tax purposes, these contributions are identified as pre-tax or after-tax.

Participants fund their accounts through salary deferrals. The relevant payroll information is received by Retirement Services directly from a Paychex payroll branch or directly from the client. Contributions for 401(k) deductions for each payroll are collected by Paychex through an EFT (Contribution EFT) from the client's designated bank account, typically on the date of the participant's paycheck that corresponds to the contributions. Generally, the Contribution EFT is deposited in the Master Custody Account on check date. Transmission activity is posted to HRIS with its respective effective date based on the file received from payroll (PI1.3.18). All wires containing contributions are deposited in the Master Custody Account and logged into Salesforce. Participant rollover contributions and accelerated loan repayments are received with written processing instructions from the participant. Checks are sent to a lockbox in the Master Custody Account. Any checks which are received by the Paychex Operations Center are logged in Salesforce where they are tracked until deposited in the Master Custody Account (PI1.2.8)

A listing of outstanding manual contributions is generated on a weekly basis and reviewed by the Client Asset Management Team for items outstanding for more than 10 days. Status updates for these items are documented and resolved (PI1.3.9). Contributions are recorded to participant accounts in HRIS based on the request from the participant or the instructions from the employers (PI1.2.8). Participant contributions, rollovers, loan repayments, and employer contributions are applied in HRIS based on the participants' specified election directions and percentages and/or the instructions received from the employers. Trades are posted to SunGard accordingly based on the information in HRIS (PI1.3.17). Identified discrepancies are researched and corrected in a timely manner (PI1.2.8).

The SunGard application rejects transactions based on pre-defined conditions (e.g., insufficient balance in account, discrepancy in funds data, missing/incorrect participant information) and lists the rejected transactions on the Transaction Reject Report. HRS Specialists review the Transaction Reject Report generated from SunGard and correct rejected transactions daily as necessary (PI1.3.11).

Transfers between Available Investment Options

Participants can request transfers using the Participant Web and can elect to transfer all or part of their balances among the investment options offered within their plan (PI1.3.19). Transfers are processed as the sale of one investment and the purchase of another. A confirmation letter is forwarded to the participant executing the transaction the next business day. Additionally, users of the Participant Web who initiate transactions receive an online confirmation statement summarizing transfer requests made within their account.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Distributions/Loan Issuance

Distribution

Distributions include retirement benefit payments, terminations, hardship withdrawals, and in-service withdrawals (each based on one or more qualifying events), plan rollovers, and loan distributions. Qualifying events are identified based on information the client provides to Paychex (i.e., employee status, disability or death, termination of the plan).

Participants can request distributions in accordance with federal law and their plan provisions through the Participant Web or by submitting the necessary paperwork (PI1.2.9). All distribution request paperwork must be approved by an authorized party prior to processing. For distributions requested through the Participant Web, the participant's username and password/PIN are required for authorization (PI1.3.6). HRIS performs edit checks to verify that the plan/participant distribution requests are eligible (PI1.2.10). Participants also receive distribution notices when it is time to take a Required Minimum Distribution or automatically when their termination date prompts the generation through the Paychex payroll process. Involuntary distributions, Qualified Domestic Relations Order (QDRO), death, and hardship distributions require written authorization from the trustee. Participant distributions, including loans, rollovers, and lump sums, are made completely and accurately based on the required information detailed in the distribution requests (PI1.2.9). The distribution process includes sale of the plan assets, formal reconciliation of the participant accounts, and issuance of the funds to the participant by check, or Automated Clearing House (ACH) credit. Distribution requests are logged in HRIS accurately and processed timely. Issues identified are investigated and resolved (PI1.3.16)

For taxable distributions or withdrawals, including retirement benefit payments, termination, hardship withdrawals, and in-service withdrawals (each based on qualifying events), applicable federal and state taxes are calculated and withheld from the distribution. Compliance monitors the tax rate updates from the federal and state/territory agencies. Tax rates are manually updated in HRIS and the application is configured to accurately apply tax withholding rate information (PI1.3.7). The appropriate tax notifications as well as the electronic transfer of funds to the applicable tax or regulatory agencies are prepared and processed by Paychex and are not within the scope of this report.

The non-vested amounts of the distributions are treated as forfeited funds. Vesting is automatically applied by HRIS based on the schedule authorized by the Plan Administrator in the Adoption Agreement, taking into account participant eligibility data. Quarterly, HRS Specialists review the accuracy of vesting percentages for a selection of clients using the Quarter End Package Verification checklists (PI1.3.15). Exceptions are documented and resolved. When a participant takes a distribution, the vesting percentage from HRIS is automatically sent to SunGard before the distribution is processed. Some distribution types are manually entered into SunGard (i.e., splits and partials) and require the HRS Specialist to update the vesting percentage in SunGard to ensure consistency with HRIS before the distribution is processed (PI1.3.15). When a terminated participant takes a distribution, all forfeitures (non-vested funds) are automatically calculated accurately based on the plan provisions and participant vesting and applied to the client's account timely. On an annual basis, the employer may choose to either have forfeiture funds allocated by Paychex to eligible participants according to their individual investment preferences or to offset plan expenses or annual employer contributions (PI1.3.22).

Loans

Participants can request loans in accordance with federal law and their Plan provisions either through the Participant Web or by submitting the necessary paperwork. Each loan must be approved by an authorized

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

party prior to processing (PI1.2.9). The loan request process includes the determination of participant eligibility and loan criteria in accordance with the Plan's Basic Plan Document and the service agreement defining roles and responsibilities for the Plan Loan Program. Relevant loan documents and disclosures are provided online. For loans not initiated via the Participant Web, all loan documents, consisting of the Loan Application, Truth-in-Lending Disclosure Statement, and basic approval forms for check issuance and repayment instructions, are directly mailed to the participant. Upon return receipt, the Loan Application is reviewed by Loan and Distribution Specialists, the trade instructions are completed, and the funds are distributed by check or ACH credit to the participant requesting the loan. HRIS performs edit checks to verify that the plan/participant distribution requests are eligible and that the requested amount of the loan is allowed (PI1.2.10). Participant distributions, including loans, rollovers, and lump sums, are made completely and accurately based on the required information detailed in the distribution requests (PI1.3.6). Loan requests are logged in HRIS accurately and processed timely. Issues identified are investigated and resolved (PI1.3.16). The participant payroll deduction order is created, and the loan balance is reduced when subsequent deductions are received. All loan repayment information is transmitted back to the respective Paychex payroll system. For non-Paychex payroll clients, Paychex sends notification of the participant loan to the client. Loans are documented on a Disbursement Register. Loan defaults are controlled systematically, and late payment notification letters are sent to the participant and the client. When defaults occur, they are reported to the participant on the IRS Form 1099R.

Dividend and Daily Earnings

The HRS Supervisor, Team Lead, or Senior Specialist reviews a random sample of funds monthly and compares the dividend information to an external source to ensure the accuracy of the information in HRIS. The HRS Supervisor, Team Lead, or Senior Specialist signs off that the review was completed (PI1.2.11). Dividends, daily interest income, and capital gain earnings are accrued and posted based on net asset value, record date, payable date, reinvest date, and beginning and ending accrual dates, as applicable. SunGard automatically calculates and posts dividend/earnings activity to participant accounts completely and accurately based on the participant accounts holding percentage (PI1.2.12). The recordkeeping system balances are reconciled with the trading partner balances daily.

Daily Plan and Participant Account Valuation

After the market closes each day, price information is received electronically from trading partners and trades are formatted and posted to participant accounts. Prices are applied to the transactions resulting from the current day's trades. Prices provided by the respective providers are used to value plan and participant accounts daily. A valuation is automatically performed by the SunGard application and updates are applied completely and accurately to HRIS plan and the participant accounts (PI1.1.8).

Daily Processing/Trading

Daily processing includes plan and employee maintenance, trade preparation, the trading process, trading partner instructions, and bank account and investment reconciliation.

The defined contribution retirement plans process trade instructions daily. Each trading partner receives trade files and confirms the receipt of buy and sell instructions. Purchase and Sales Blotters are systematically generated to allow for the reconciliation of trades and update of client records.

Contribution, Loan, and Distribution data are received for edit processing prior to trading each day. Plan updates and employee changes are included during the trading process. The Participant Web references the most current participant data.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Requests from the Participant Web are automatically processed in HRIS and traded through SunGard accurately and timely (PI1.3.20). Prior to the nightly trade process, fund transfers initiated through the Participant Web and not processed automatically (i.e. due to insufficient funds, self-directed brokerage accounts, etc.) are generated on the Transcompare Report reviewed by the HRS Specialist and resolved, as necessary, in a timely manner (PI1.3.8).

Reconciliations

After the trading partner has received and processed the trade file, a confirmation file is electronically delivered back to Paychex. A Purchase and Sales Blotter is generated. The Purchase and Sales Blotter indicates if each transaction from the prior day was confirmed or rejected by the trading partners. Trade Reconciliation Specialists reconcile purchase and sale activity with the trading partners daily. Transactions that are rejected are investigated and followed up on (PI1.3.15 & PI1.3.21). 401(k) trade purchase wires are prepared by a Trade Reconciliation Specialist, approved and released by Treasury Specialist. Some trading partners may net daily purchase and sale transactions, and a net wire may be received by Paychex.

Each day, the trading partners generate and send a position file to Paychex detailing the share balances they hold. Daily, the Trade Reconciliation team reconciles and investigates any discrepancies between this file and the balances in SunGard. A formal reconciliation report is produced for the last day of each month, noting the outstanding discrepancies as of that day. This monthly report is signed off by the Trade Reconciliation Specialist and the Trade Reconciliation Supervisor. Differences between this report and the balances Paychex has in SunGard are researched and corrected (PI1.3.12).

In addition, Client Funds Accounting Specialists reconcile HRIS, the bank statement, and the General Ledger monthly, and the reconciliation is reviewed by Client Funds Accounting Management. Discrepancies identified are tracked and resolution is documented (PI1.3.10).

Reporting

The HRIS application is configured to produce statement files completely and accurately using client and participant information stored in the application (PI1.4.5). Samples of client and participant statements are reviewed quarterly by HRS Specialists for completeness and accuracy. Exceptions are documented and resolved in a timely manner (PI1.4.4). An outside vendor, Venture Solutions, sends client summaries and individual participant statements to clients quarterly based upon information provided by Paychex. This information is automatically sent through IBM Transfer via Sterling, a cloud service for file-based business-to-business interactions, and includes the beginning and ending balances, employee and—if applicable—employer contributions, distributions, transfers between available investment options, loan issuance and repayments, investment earnings and performance, and investment allocations as of the ending date. On a quarterly basis, HRS Specialists reconcile the number of client level statements printed between the vendor invoices and the associated client statement files in HRIS. Discrepancies identified are researched and resolved in a timely manner (PI1.4.7). Individual account balances and participant statements are also available through the Participant Web.

Payroll

The New Client Setup Process begins after a sale has been made. The Sales Representative is the intercessor between the client and Branch personnel from the initial call through to the delivery of the first payroll. This includes preparing and submitting complete load information to the Implementation Team. The Implementation Team receives the new client information from the Sales Representative and then inputs the information in the payroll system. This includes both client- and employee-specific information. All

payroll clients are required to have at least one defined payroll contact in Core Payroll prior to activation (PI1.1.5). The Implementation Specialists reviews new client information for accuracy and completeness within five business days after generating the first payroll using a checklist and then signs off on each case, indicating that the client has been accepted and loaded per client specifications (PI1.2.6). The Implementation Team is responsible for helping the client become familiar with Paychex procedures and, if the data entry method selected is phone or fax, inputting the first few payrolls. The transition is then made to a Payroll Specialist (PRS), who becomes the client's primary contact at Paychex and is responsible for inputting the client payroll and making changes to the client master files as requested by the client.

Payroll Specialists receive changes authorized by the client and enter them into the Core Payroll application. Payrolls are processed one at a time as they become ready. The system then computes total compensation, taxes, adjustments, client tax liabilities, and client tax payments. Database files are then updated with the results of the calculations, and a reporting database is created. Payroll checks, direct deposit summaries, and other output reports, including journals, summaries, and tax deposit notifications, are printed.

The payroll process can be broken down into the following steps: input, payroll processing, and output.

Input Process

Payentry is a Paychex-developed entry system (part of the Core Payroll application) that is utilized for maintaining client and employee master file information. This system provides preformatted screens and has built-in, online logical edit checks to help ensure the accuracy of the client's payroll information and reduce input errors. During a payroll session, each active employee is presented in a pre-determined order, usually alphabetically by department, to ensure all active employees are considered for payment (PI1.2.2). The PRS confirms each employee's name, changes, and pay information based on the information provided by the client via email, phone, or fax. Clients are provided with a timesheet to help them organize their payroll information before it is reported to Paychex. Changes are processed through the Core Payroll application and update the database. Key payroll transactions are logged, including the date and time of the transaction and the name of the individual who initiated the transaction accurately (PI1.2.5).

The majority of Paychex payroll clients report their payroll each pay period by telephone or online to their assigned PRS. An online appointment schedule is produced for each PRS, listing the clients to be contacted for the day. PRSs use the daily appointment schedule contained within Payentry to guide their daily activities. At the scheduled time, the PRS calls the client and utilizes Payentry to enter the payroll information while talking directly to the client's authorized representative. The application automatically removes clients from the PRS's Electronic Appointment Schedule once their payroll has been input and submitted for processing. If clients do not provide payroll, the Payrun will move to the next day (PI1.1.3). Paychex policy restricts the discussion of payroll information to only the designated payroll contact(s) on file. All payroll information received from the authorized contact by Paychex are input by the PRS's through Payentry. Clients do not have access to Payentry.

Input Process – Paychex Flex Payroll Center

Paychex Flex Payroll is a web application that allows clients to enter payroll and employee information directly into the Core Payroll application using Transport Layer Security (TLS) protocol (CC6.7.5). The application requires the continued use of a unique username and password for authentication. In addition, Paychex requires the selection of a multi-factor authentication option to further confirm the identity of the user which can range from answering challenge questions to requiring a one-time password every time a user logs in (CC6.1.3). Finally, additional security controls such as the use of a PIN and challenge questions are required for subsequent changes to security information. Application edit checks reduce online data entry errors. Clients are required to identify an administrator to control security access rights for individuals within their company who can view and/or input payroll information. Each Paychex Flex Payroll client is

assigned to a PRS in the branch. The PRS is responsible for supporting the client and ensuring client needs are met.

Payroll Processing

Payroll processing can further be broken down into the following steps: system holds, payroll calculations, current pay run and YTD update totals, and reporting.

Once the payroll information has all been input and, if the payroll does not have any holds in place, the payroll will be submitted for processing. Payroll holds delay the processing of a client's payroll for a specific reason. Holds can be set automatically in the application, or set manually by Paychex accounting groups, PRSs, and Supervisors. For example, a payroll hold can be manually placed to require a review of the specific client payroll before processing. Holds automatically placed by the application include items such as backdated payrolls or 15-minute time delays. A client's payroll will not process until all holds have been cleared and removed from the system (PI1.3.3).

Once a payroll is ready (any applicable holds have been released) and the payroll starts to process, a series of payroll calculations is performed for each entry in the file. This process reads the employer (client) and employee master file information for each record and calculates, among other things, gross earnings, tax deductions, and net pay. Employer and employee year-to-date payroll and tax records are updated during the payroll process (PI1.1.4). The Core Payroll application automatically calculates control totals. The Payroll Specialist compares the control totals produced by the application to the information provided by the client to ensure the completeness and accuracy of payroll input (PI1.2.3).

During processing, the Core Payroll application applies edit checks to ensure the completeness and accuracy of payroll processing. Errors are resolved by the Computer Operators and through problem management. Examples of edit checks include:

- Negative check amounts
- Bank account number not matching to the account number noted in the application
- No direct deposit set up
- Back-dated check dates
- Payfile code not set up
- Duplicate payroll processing (PI1.3.3 & PI1.2.4)

The payroll process generates the client's payroll report output and also updates the client's payroll master files with the current pay period information. If the payroll process fails, an automated message is generated to Enterprise Support to resolve the failure and ensure the payroll will process correctly. Copies of the automated messages are also generated to the PRS and the Supervisor assigned to the client for follow-up. Computer Operations does not participate in the correction process. Once all of the failures have been resolved, the payroll automatically processes. A second automated message is generated to the PRS and the Supervisor, indicating the payroll process is complete (PI1.3.5).

The next step of the payroll process creates the payroll reports for each client. Standard payroll reports produced for each client include payroll journals and department summaries, and direct deposit summaries, along with employee payroll checks.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Output

Checks, deposit summaries, and other output reports, including journals, summaries, and tax deposit notifications, are printed at Paychex facilities and delivered to the client. Optionally, not editable payroll reports are available online. Standard payroll reports include:

- **Payroll Journal** – This report displays employee payroll activity for the current period, including earnings, net pay, tax deductions, and other earnings/deductions for each employee. Client totals are provided.
- **Department Summary** – This report displays payroll information for the current and month to date periods, summarized by organizational unit. The report also includes Quarter to Date and Year to Date totals by employee type and deduction type. The Department Summary usually contains the necessary information to post payroll transactions to the general ledger (PI1.4.3).

Checks are produced at the payroll processing locations. If a paper jam occurs during the check printing process, the Computer Operator intervenes and manually corrects the problem. The printer logic notes where the error occurred and resumes printing from that point. The printer will reprint the checks that were removed during the jam. The rejected checks are appropriately disposed of in locked document shredding bins by the Computer Operator. Unused check stock is kept in a secure area and access is limited to authorized personnel (CC6.4.6).

The design of Paychex payroll checks and stubs provides security protection against current color copy and scanner duplication systems. These features are included on both the front and back of each check (PI1.4.1). For clients who choose the Check Signing product, Paychex prints checks with a signature provided by the client. Paychex loads the signature image into a secure directory on the payroll processing server.

Reports are packaged, sealed, and delivered to clients by insured third-party couriers. A Delivery Report and manifest are used to monitor and control document the delivery of payroll information the distribution of payroll packages. Payroll packages (including checks or deposit reports) are distributed in accordance with client specifications (PI1.4.2). Payroll packages awaiting delivery are stored in secure areas (CC6.4.5).

As part of the payroll output process, data files are generated to update databases for ancillary products and services, such as Retirement Services. The payroll transaction records are updated to a separate history database. This allows previous payroll entries to be referenced and enables the client to receive a report of entries for each employee. Data files are backed up on a nightly basis and transported off-site. Print images of daily reports are compressed and stored on the local branch system and transmitted to a central online reports archive at the DC. The archive provides an internal reference copy of the reports and allows the replication of reports at the client's request. Clients also have the option of requesting online copies so that they can download their reports from Paychex Flex as softcopies once the payroll is processed. These are the same reports as the printed payroll reports.

Tax Withholding Calculations

Payroll Publications (CCH, BNA, and RIA), Westlaw (a legislative search engine), and industry news and articles are monitored to ensure compliance with agency legislative and regulatory requirements. Compliance is responsible for monitoring these communications, articles, and websites daily. In addition, Compliance has direct contact with each of the federal/state agencies to identify any upcoming withholding table changes. All contact information and agency responses are documented on a "Withholding Table Tracking Chart." This chart is organized by state/federal agency and includes columns indicating whether there is a withholding table change, if an application request (APR) was submitted to IT, and when the new table/withholding information will be available from the agency. It also includes the specific APR number for tracking purposes (if applicable). The phone call process with the federal/state agencies to identify

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

withholding rate changes usually begins in September and continues until a response is received from each of the agencies.

The majority of tax withholding calculation changes to the Core Payroll application are manually entered by the PD&IT Agile team in the staging environment and then sent to IT Operations to be packaged and deployed to the production environment. There are few changes that require modification to the program code, and these are typically on an exception basis, such as a change to expand or add a field in the Core Payroll application. If a system change is identified as needed, an application request is created using the ticketing system and submitted to IT. The request includes individual approvals, details of the change, and the effective date (CC3.4.8 & CC3.4.9).

PD&IT teams manually enter the withholding change in the staging environment for the Core Payroll application. Access to the statutory rate tables is limited to appropriate personnel through assigned user IDs and passwords. If any changes are needed, the document is rejected back to the original Agile team member that performed the coding. All withholding rate changes are tracked through ServiceNow and require approval from PD&IT Management before the change is executed in production. In addition, there is a second independent manual verification within the PD&IT Agile teams to ensure that the change has been coded correctly to the staging environment before it is scheduled for release to production. If all changes are coded correctly, Implementation approves the change for release into the production environment; the release into production follows the formal system development and maintenance process described earlier. The modified files are sent to the branches via an Application Release and overwrite any files in the current payroll system (PI1.1.7).

Data

Data, as defined for the scope of this report, constitutes Paychex customers' data, including employee information, as well as human resources and payroll details. The Paychex Flex Retirement Services, Payroll, and Reporting Services system allows clients and employees to access various applications in order to view and update basic employee data such as name, email address, address, phone number, employment status. Paychex payroll clients report their payroll each pay period via email, phone, or fax to their assigned PRS and provide employee names, changes, and pay information. Such data is input by the PRS into Core Payroll.

Retirement Services participants fund their accounts through salary deferrals. The relevant payroll information is received by Retirement Services directly from a Paychex payroll branch or directly from the client. Participant deferral percentages and investment elections for retirement services can be submitted to Paychex via Participant Web or paper enrollment forms. The majority of participant enrollments are submitted via the Participant Web. Enrollment changes by the participant are transmitted back to the respective Paychex payroll system. For non-Paychex payroll clients, Paychex sends notification of the change to the client with instructions to view the details on the specific participant's change via the website.

Data definitions, mapping and processing specifications required to support the system are documented. (PI1.1.1). Detailed design specifications are captured as part of the SDLC process. Development teams leverage Confluence for high level documentation and detailed acceptance criteria is captured in JIRA (PI1.1.2). Client data is logically segregated. Each client and their data are identified using a unique identifier, a combination of letters and numbers (CC6.7.9).

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Board of Directors

The Board of Directors, which is elected by the shareholders, is the ultimate decision-making body of the Company except with respect to the matters reserved to shareholders. It selects the senior management team, which is charged with the conduct of the Company's business. The Board acts as an advisor to senior management and ultimately monitors management's performance (CC1.2.1).

In general, major decisions of the Company shall be considered by the Board as a whole. However, where appropriate for effective and efficient governance, the Board may delegate authority to its five designated committees.

Board members have free access to all members of management of the Company and, as appropriate, may consult with independent advisors, including legal or financial advisors, to assist in their duties to the Company and its shareholders.

The Corporate Governance Guidelines, published on Paychex's website, guide conduct principles for the Board of Directors and document size, selection, election, meeting attendance, term limits and board functions (CC1.2.2).

The Company's overall philosophy on professional conduct and operating style establishes the framework for other aspects of internal control. The control environment at Paychex involves the following areas:

- Integrity and Ethics
- Training Center

Administration Management and the Board of Directors meet quarterly to communicate information needed to fulfill their roles with respect to the achievement of Paychex's service commitments and system requirements (CC2.2.17). On a quarterly basis, the Board of Directors receives quarterly updates from the CISO including internal control deficiencies that are used to drive security-related objectives and functioning of internal control (CC1.2.5).

Integrity and Ethics

Paychex Mission Statement

Paychex is guided by the following mission statement "We will be the leading provider of payroll, human resource, and employee benefit services by being an essential partner with America's businesses."

Code of Business Ethics and Conduct

A set of standards for proper business conduct has been published to allow Paychex employees, clients, and suppliers to gain a better understanding of how Paychex wishes to conduct business. The areas addressed include gifts and amenities limits, avoiding misrepresentation, personal conduct, equitable practices, conflicts of interest, and proprietary information. Paychex also has a process for anyone to report corporate misconduct or communicate complaints or concerns. Anyone who has a concern about the conduct of a Paychex executive or other officer, or about the Company's accounting, internal accounting controls, or auditing matters, may communicate that concern directly to the Audit Committee Chairman of the Paychex

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Board of Directors. Employees may use a toll-free number published on the Company's website to initiate this communication (CC1.1.5). The Code of Business Ethics and Conduct is documented in the Employee Handbook and updates are communicated to employees annually (CC1.1.2). New employees receive the Code of Business Ethics and Conduct with their welcome package and must formally acknowledge its receipt via training, which is monitored and tracked by Human Resources. In addition, all employees are required to complete an online training class on the Code of Business Ethics and Conduct annually (CC1.1.3).

Conflict of Interest Statement

In general terms, a conflict of interest can be considered to exist if personal interests and activities would damage Paychex business interests and activities. Typical conflicts of interest are outlined in the Code of Business Ethics and Conduct. This communication to employees provides clear guidelines for addressing circumstances that may interfere with an employee's role at Paychex.

Training

Paychex provides compliance and role-based training opportunities to all employees. The Right Way Training is required annually for all Paychex personnel. The Right Way Training includes annual topics of ethics, security and internal controls, workplace harassment, and the Paychex Problem Solving Policy. All active Paychex personnel are required to complete these training courses and compliance with all mandatory courses is tracked on an annual basis (CC1.1.1).

New leaders (supervisor, manager, and senior managers) are required to complete the Leadership Essentials program to promote and develop competent skills and expertise and completion is tracked by management (CC1.4.2).

Paychex has implemented Right Way training and awareness programs for its personnel related to security policies, and ethics. Paychex personnel are required to complete this training during the new hire on-boarding process and annually thereafter. New Hires are required to acknowledge the Employee Handbook via training which includes acknowledgement of Paychex's Acceptable Use Policy (CC1.1.7).

Paychex has a dedicated Security Acquisitions, Crisis and Training team. The team is responsible for the security training and awareness roadmap. The team seeks to increase knowledge amongst Paychex employees both for Cyber Security and Physical Security. This team coordinates routine enterprise wide communications on security topics, coordinates the company's National Cyber Security Awareness Month programs, and routinely tests the organization with phishing simulations. Training results for phishing simulations are communicated to leaders across the organization and directed training is coordinated for any employee that fails these simulations (CC2.2.14).

Paychex personnel are required to acknowledge the Acceptable Use Policy upon hire and acknowledge the security policies at least once per year as part of annual Right Way training (CC1.1.7).

Administration

Policies

Personnel policies document the principles that guide the conduct of all Paychex employees. Periodic revisions and updates are released each year. All policies are available to employees in the Employee Handbook. The handbook includes policies on the security of information and assets, non-disclosure, conflict of interest, and standards of behavior (CC1.1.6 & CC1.1.7).

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Published Job Descriptions

Formal job descriptions communicate the general function and specific duties of a position. Job descriptions above a certain grade level are evaluated, graded, and approved by the Job Evaluation Committee. The Committee includes representatives from senior management and the Human Resources department. The manager responsible for a position is included in the process. Any employee hired is provided his/her respective job description, which includes written expectations of the position (CC1.3.3).

Hiring Practices and Performance Evaluations

Hiring managers of Paychex define appropriate job requirements prior to their recruiting, interviewing, and hiring for a position of employment. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Minimum education and prior work experience is also documented as part of the hiring requirement. These areas are documented for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability. Once the requirements are determined, managers create a job description, which is a profile of the job and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision (CC1.4.1).

Paychex personnel have defined and documented roles and responsibilities, which are communicated to such personnel upon hire or role change. A periodic performance management process is executed for Paychex personnel with a focus discussion on strengths and any identified challenges (CC1.4.5). Management monitors personnel compliance with code of business conduct and ethical standards via training and the performance review process. The process for disciplinary action is communicated to employees via the HR intranet site under the Corrective Action page (CC1.1.4).

Upon hire, personnel agree to comply with the policies of Paychex. In addition, all Paychex personnel are required to complete Right Way training during the new hire on-boarding process and annually thereafter (CC1.1.1).

Background Checks

Background investigations are conducted for employees prior to joining Paychex. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis by a dedicated team for resolution (CC1.1.8).

M o n i t o r i n g

Ethics and Compliance Hotline

Management has an anonymous third-party administered ethics hotline available to internal and external users. Depending on nature of complaint, appropriate entities will be engaged to conduct investigations regarding the complaint. (CC1.1.5). Personnel are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Code or other policies or guidelines of Paychex. The procedures to be followed for such a report are outlined on the Ethics and Compliance intranet page. Paychex personnel are also encouraged to communicate the issue using the Paychex Problem Solving Policy within the Code of Conduct.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Internal and External Reporting Objectives

Paychex communicates out its objectives and changes to objectives (i.e., technology changes, leadership changes, policy changes, etc.) through various channels such as a post on the Paychex Intranet, Yammer, Social Media and/or email (CC2.2.13).

Internal Audit

The Internal Audit department acts as an independent appraiser of the internal control system of Paychex. The primary objective of the department is to assist management with the effective execution of their responsibilities to customers and shareholders by providing management with assessments on internal control design and operating effectiveness as well as recommendations to enhance internal controls. Internal Audit individuals have the appropriate experience and expertise to conduct their work with proficiency and due professional care. Personnel resumes and/or certifications are documented and maintained (CC4.1.4).

The Internal Audit department reports directly to the Company's Audit Committee who oversees the Company's internal control structure. The department has been granted the authority to examine all Company records, reports, and documentation, and to use whatever audit procedures are deemed necessary to accomplish its objectives. Internal Audit has unrestricted access to the Audit Committee of the Board of Directors and senior management. Senior management is responsible for ensuring operating management gives adequate consideration to the findings and recommendations included in audit reports (CC1.2.7).

The Director of Internal Audit is a member of the Security Governance Council (SGC) (described below) and considers the subject matter discussed during those quarterly meetings when determining the nature, timing and extent of testing related to Information Technology and Information Security.

Internal audits are performed based on the annual risk-based internal audit plan. Identified internal controls deficiencies from IT assessments are communicated to management and tracked to appropriate resolution (CC1.2.4).

System Audits

Internal security control reviews are performed periodically based on the business impact of the systems. Paychex's internal audit team performs audits on various aspects of Paychex's systems, processes, and policies (CC4.1.2).

Cyber Security, Risk and Compliance

The Enterprise Security department headed by the CISO oversees the security program and is divided into the following groups:

- Cyber Security Operations Center
- Security Threat Intelligence & Threat Hunting
- Security Incident Response & Digital Forensics
- Application Security
- Security Architecture
- Security Assessment & Vulnerability Management
- Identity Management
- Security Engineering

- Enterprise Managed File Transfer Services
- Security Acquisitions, Crisis & Training
- Security Governance, Risk & Compliance
- Security Analytics
- Physical Security

Members of these groups hold various industry security and audit-based certifications (e.g., CISSP, CISM, CISA, ISSM, CRISC, CEH, OSCP and GCP Certified Solution Architects).

Organizational charts are created by senior leadership, are documented and communicated via the Paychex Blue Pages SharePoint site. The organizational charts and reporting lines, authorities, and responsibilities are reviewed and updated as needed based on organizational changes (CC1.3.1).

A formal risk governance program is implemented and includes a risk governance plan, risk policy and procedures, business assets to be evaluated, threat types, and risk evaluation criteria.

On a monthly basis, the CISO, CTO, and CIO are presented with a Security Program Update (SPU) including key security and availability metrics, events and incidents where relevant. As part of these meetings, risk assessment updates, risk assessment calendars and identified threats, and action items are also discussed (CC2.2.11). The risk management program includes the use of insurance to minimize the financial impact of any cybersecurity events (CC9.1.3).

Security Governance Council (SGC)

The Security Governance Council's mission is:

- To develop, coordinate, and sustain the organization's enterprise security program
- To coordinate and respond to security risks and incidents; and
- To develop, implement and maintain the organization's enterprise security strategy in alignment or support of business goals and objectives.

The success of the SGC depends upon an objective understanding of the Company's asset protection issues. The SGC meets on a quarterly basis and is chaired by the Chief Information Security Officer. The SGC is comprised of members who understand the business operations, including individuals from Information Technology, Internal Audit, Legal, Human Resources, and Organizational Development, and business unit executives. The recommendations of the SGC are considered when updating the information security policies, procedures, and standards at Paychex (CC1.2.6).

Risk Assessment

Paychex has placed into operation a risk assessment process to identify and manage risks that could affect the Company's ability to provide reliable information technology service to its customers. This process requires the Company to identify significant risks based on management's knowledge of its operations and input received from the Internal Audit group and the Company's external auditors. For any significant risks identified, management is responsible for implementing appropriate measures to monitor and manage these risks (CC3.1.1).

Paychex has an Audit Committee that oversees risk assessment and monitoring. Paychex management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine

part of their activities. To assist them in this monitoring, the Company has developed management reports that measure the results of various processes involved in processing their business units' transactions.

Paychex reviews risk through various levels of detailed assessments, to provide the organization with consistent enterprise-wide risk management processes and enable the aggregation and analysis of risk to create an enterprise view and understanding of risk. Paychex's Enterprise Risk Management team and Enterprise Security team assess, test and monitor in-scope systems, and devices for compliance with relevant policies and standards. Risk and Compliance leaders meet periodically to discuss developments in technology and the impact of applicable laws or regulations on Paychex. An inventory of known risks and risk attributes is maintained, and a risk response plan is developed which serves as the basis for risk-based decisions (CC3.2.5). A site-level threat assessment is conducted each fiscal year based on the actual threat environment and to identify environmental or physical threat changes. Relevant information resulting from IT assessments conducted by external parties is communicated to leadership as needed. Paychex Enterprise Security Risk and Compliance also performs periodic risk assessments for IT. Objectives incorporate service commitments and system requirements related to security, availability, and processing integrity. Assessments are documented and communicated to management in a final report, and monthly reporting meetings. These assessments are reviewed by senior management within IT for appropriate action (CC3.2.6). As part of periodic IT risk assessments, management links the identified risks to controls that have been designed and operated to address them (CC5.1.1).

Monthly risk assessment review meetings are held to revisit open risks and assess changes (business, external environment, changes in technology, leaderships or vendors) that may impact the company's risk profile. Separately, monthly Security Program Update (SPU) meetings are held where risk assessment updates, risk assessment calendars and identified threats, and action items are discussed (CC3.4.1).

Fraud Risk Assessment

The Credit Risk Management team is responsible for conducting periodic fraud risk assessments through a variety of initiatives as defined in the Know Your Customer and Anti-Money Laundering Operations Manual in order to identify the various ways that fraud and misconduct can occur (CC3.3.1). Additionally, fraud related risks are considered during the narrative review, which is a review of the controls and their operating effectiveness. Control narratives are stored in a centralized location and semi-annually, control owners review process narratives (CC5.2.2).

Paychex's Risk Management team performs an assessment for new customers onboarding to the system to identify risk and potential fraud schemes. A variety of external information regarding clients is identified during the assessment as well as information relevant to client onboarding in order to achieve objectives (CC3.3.4).

Subservice Organizations and Vendor/Third Party Assessments

Paychex management assesses the risks associated with the subservice organizations and has implemented management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner. The Security Risk team performs a review of the subservice organizations' Service Organization Controls (SOC) reports and evaluates the Subservice Organization Controls and Complementary User Entity Controls.

Paychex's relationship with each subservice organization is managed via a named contact through whom service concerns and expectations may be discussed. Additionally, each subservice organization provides email and online support channels through which contact may be made. Paychex utilizes a third party to perform security benchmarking and monitoring of its vendors. Paychex also performs reconciliations and service level reviews as part of monitoring over the subservice organizations (CC9.2.6).

Paychex has a Contract Management Policy for all vendor and business partner contracts. The policy covers processes related to the functioning of components of internal control and assists in the achievement of Paychex's business and strategic objectives (CC3.1.2).

The organization has also established and assigned responsibility and accountability for the management of vendor/third party risks. Vendor/third party compliance requirements, and service levels are written into the contract with that vendor as necessary based on the service provided (CC9.2.5). Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity (CC9.2.1). Agreements are established with service providers to mitigate risks and are reviewed by relevant Legal and Security personnel as needed. Security addendums are included in the agreement where necessary to define responsibilities of vendors (CC2.3.3).

Vendors/third parties are subjected to an initial security risk evaluation before the establishment of a relationship. They are then monitored on an ongoing basis based on the level of risk associated with the external party. The Vendor Assessment process is designed to reduce vendor-related risks by:

- Building a repository of acceptable vendors
- Assessing the security posture of such vendors
- Reviewing and assisting with the negotiation of variances to our standard security language in contracts with vendors

Initial vendor risk assessments are performed for vendors that have access to confidential data or could impact the service of the system and are documented within the third party vendor management system. The vendor risk assessment evaluates criticality (business critical, key vendor, or non-key) and the type of data being impacted in order to establish a risk score – minor, low, high, critical. Annual tiering re-assessments are sent to the vendor relationship manager to confirm that the nature and scope of the data has not changed. If the scope has changed or the vendor is deemed “Key/Business Critical”, a full vendor re-assessment will be performed. (CC9.2.4).

Information and Communication

The information systems relevant to the scope of this report are described in the “Software” section of this report.

Internal Communication

Responsibilities around internal controls are communicated to appropriate users by various methods, including, but not limited to job descriptions, control narrative, policies and standards. Responsibilities for compliance with policies are set out in the Employee Handbook, which is acknowledged upon hire, and the code of conduct required to be acknowledged by Paychex personnel once a year (CC1.1.3). Various security awareness campaigns are conducted across the organization. Notification to appropriate users are sent directly by email for any time sensitive matters.

Written processes and procedures for operations and security processes are provided to personnel responsible for operation of the system. Designated personnel update the processes and procedures manuals based on changes to availability requirements and security policies.

As required by their Charters, the Board committees are required to formally report to the Board on their activities, in which they operate on behalf of the Board, as stewards of and specialists in particular areas, working closely with management and the full board.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Communication between senior and operations management includes updates when written communication is appropriate, periodic department meetings between each executive and their direct reporting managers, and other discussions as needed. Communication is encouraged at all levels of Paychex.

Planned software and infrastructure changes are communicated to internal users via the Change Calendar feature within ServiceNow. The calendar indicates the date and time of each change release on a given day (CC2.2.5).

Operating Procedures Manuals

Procedures help maintain consistent operations and provide a reference to employees in the conduct of their daily responsibilities. Procedures and documentation are maintained and updated online.

External Communication

Paychex provides the Information Security Program Overview to external users to provide an overview of Paychex's IT security and availability practices and commitments. Any changes to systems which may affect the security, availability and processing integrity aspects of commitments or user's responsibilities are communicated through system notifications or via email to impacted users (CC2.3.4). Policies and procedures for incident response are in place to facilitate communication for reporting issues, failures, and incidents through online support forums and their regular representatives (CC2.3.1). Online learning materials are accessible by customers. Onboarding materials are provided to new customers (CC2.3.5).

Communication with Clients

As part of the Company's commitment to providing quality customer service, Paychex has regular communication between clients and product specialists. Paychex uses and provides an array of communication methods including technical help desks, regular written and email updates on payroll regulation, retirement services, health care regulation and tax changes, client surveys, and access to www.paychex.com.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

COMPLEMENTARY USER ENTITY CONTROLS

Certain trust services categories and related criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Paychex's controls are suitably designed and operating effectively, along with related controls at the service organization. The system herein was designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. The list below should not be regarded as a comprehensive list of all internal controls that should be implemented by the user entity, nor do they represent procedures that may be necessary in all circumstances. User entity for this report are often referred to as the external users.

Complementary User Entity Controls	Related Trust Criteria
Logical Access	
— Clients should have controls in place to identify an administrator commensurate with job responsibilities to control security access rights for individuals within their company that can review and input data, and provision and deprovision access as needed. — Clients should have controls in place for designating payroll contacts who are available for payroll input and for communicating to Paychex changes in designated payroll contacts authorized to make changes on behalf of the client.	CC6.2, CC6.3
— Clients should have controls in place over completeness and accuracy of ACH transmissions.	CC6.7
Processing Integrity	
— Clients should have controls in place for designating payroll contacts who are available for payroll input and for communicating to Paychex changes in designated payroll contacts authorized to make changes on behalf of the client. — Clients should perform a detailed review of payrolls to verify the accuracy and completeness of withholdings.	PI1.1
— Clients should have controls in place to ensure the completeness and accuracy of any information provided by designated payroll contacts and/or client. — Clients should have controls in place for the calculation of payroll totals on the client timesheet prior to input at the branch. Clients should have controls in place for comparing these totals to the accumulated totals calculated and displayed on the branch payroll system. — Clients should have controls for ensuring control totals are complete and accurate. — Clients should have controls in place to ensure the Adoption Agreement and any subsequent changes to the Adoption Agreement is reviewed and approved by an appropriate and authorized member of client management. — Clients should have controls in place to ensure written notification of changes to individuals authorized to effect activities is communicated to Paychex timely.	PI1.2

Complementary User Entity Controls	Related Trust Criteria
— Clients should have controls in place to ensure the plan setup, or modifications after changes have been made, is verified by an appropriate and authorized member of client management. — Clients should have controls in place to ensure the hire, re-hire, and termination status and dates of all employees are verified by an appropriate and authorized member of client management and changes are communicated to Paychex.	
— Clients should have controls in place to ensure the accuracy of any information provided by designated payroll contacts and/or client. — New clients should have controls in place to perform a detailed review of the first payroll to verify the accuracy and completeness of the payroll run. — Clients should have controls in place to perform a detailed review of all payrolls to verify the accuracy and completeness of the payroll run. — Clients should have controls in place over the timely notification of payroll changes to Paychex. — Clients should have controls in place to verify the accuracy of changes to garnishment deductions. — Clients should have controls in place to review all reports and documents provided or made available by Paychex and inform Paychex of any inaccuracies in accordance with the provisions of the applicable governing agreements or documents between Paychex and the client.	PI1.1, PI1.2
— Clients should have controls in place to ensure qualifying events are identified and reported to Paychex in a timely manner. — Clients should have controls in place to ensure the plan transfer paperwork is reviewed and approved by an authorized member of client management. — Clients should have controls in place to ensure all distributions are reviewed for accuracy, including federal and state/territory tax withholdings on distributions, and discrepancies are reported timely to Paychex for correction. — Clients should have controls in place to ensure participants are provided instructions to review confirmations and to report discrepancies timely to Paychex for correction. — Clients should have controls in place to ensure their non-Paychex payroll systems are updated for participant changes. — Clients should have controls in place to ensure participants are provided instructions to review distributions for accuracy and to report discrepancies timely to Paychex for correction. — Clients should have controls in place to ensure participant terminations are identified and reported to Paychex in a timely manner. — Clients should have controls in place to ensure all vesting percentages for terminated participants are reviewed for accuracy and discrepancies are reported timely to Paychex for correction.	PI1.2, PI1.3

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Complementary User Entity Controls	Related Trust Criteria
— Clients should have controls in place to ensure the allocation of forfeitures applied to the client account is communicated to Paychex.	
— Clients should have controls in place to ensure reconciliations of client bank statement activity for 401(k) contributions to the payroll accounts are performed timely. — Clients should have controls in place to ensure reconciliations of client bank statement activity for 401(k) contributions sent via checks, wire transfers, and non-payroll ACH are performed timely. — Clients should have controls in place to ensure the updated banking account information is communicated to Paychex in a timely manner. — Clients should have controls in place to ensure sufficient funds are available in the specified bank account.	PI1.3
— Clients should have controls in place over access to payroll output, including electronic payroll data. — Clients should have controls in place over access to the client number, which is used as a means of identification. — Clients should have controls in place for the timely reconciliation of client bank statement activity. — Clients should have controls in place to verify direct deposit changes are made accurately and completely. — Clients that choose to print payroll checks at their location should have controls over access to check stock as well as printed checks. — Clients that create customized reports, or choose to generate reports in paper or electronic format, should have controls over reviewing these reports for completeness and accuracy. — Clients should have controls in place to ensure participants are provided instructions to review confirmations and to report discrepancies timely to Paychex for correction. — Clients should have controls in place for updating their non-Paychex payroll systems for participant changes. — Clients should have controls in place to ensure the timely review and reconciliation of reports provided by Paychex of plan accounts, and that written notice of any discrepancies is communicated to Paychex. — Clients should have controls in place to ensure plan administrators distribute participant statements in a timely manner.	PI1.4

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOC)

The Paychex Flex Retirement Services, Payroll, and Reporting Services system was designed with the assumption that certain criteria supporting Security, Availability, and Processing Integrity can be achieved only if complementary subservice organization controls assumed in the design of the Paychex Flex Retirement Services, Payroll, and Reporting Services system controls are suitably designed and operating

effectively, along with the related controls of the Paychex Flex Retirement Services, Payroll, and Reporting Services system.

The table below reflects the subservice organizations used by the Paychex Flex Retirement Services, Payroll, and Reporting Services system for certain functions and controls that are relevant to the in-scope trust service categories. For the subservice organizations, the table summarizes the complementary subservice organization controls that the Paychex Flex Retirement Services, Payroll, and Reporting Services system expects the subservice organizations to perform relevant to the in-scope trust services categories and criteria.

Subservice Organization	Services Provided	Related Trust Criteria	Complementary Subservice Organization Controls
Merrill Lynch, Fidelity Investors, Federated Investors, Legg Mason Partners, Transamerica and Mid Atlantic Trust Company	Retirement Services: Trading-related services	CC6.2	Controls should be established over logical access, including password configurations, user access, and encryption.
		CC6.6, CC6.7	Controls should be established over logical access security such as encryption, firewalls, and cyber and breach management.
		CC8.1	Controls should be established: — For change management over requesting, reviewing, approving, managing, testing, and applying infrastructure changes and upgrades to production — Over maintaining requirements for documentation, authorization, testing, approval and implementation of new programs/system components. — Over performing vulnerability assessments and penetration tests, and addressing the results — Over restrictions of access to make changes
		PI1.1 – PI 1.4	Controls should be established to ensure that accurate mutual fund prices and dividend rates are provided timely. Further, the subservice organization should have controls in place to ensure that trade instructions are executed and confirmed timely, and that accurate fund account balances are reported.
RR Donnelley, Venture Solutions	Retirement Services: print, and mail client statements	CC6.2	Controls should be established over logical access, including password configurations, user access, and encryption.

Subservice Organization	Services Provided	Related Trust Criteria	Complementary Subservice Organization Controls
		CC6.4 PI1.4	Controls should be established over physical access and security. Controls should be established to ensure complete, timely and accurate file processing for client and participant statements.
SunGard Data Systems ("SunGard")	Retirement Services: Develop and maintain the application SunGard-OmniPlus	CC6.2 CC8.1	Controls should be established over logical access, including restriction of access to make changes. Controls should be established for change management to support the complete, accurate, and timely processing and reporting of transactions.
Cyderes (Herjavec Group)	Monitoring of security events and alerts, and escalation if needed	CC6.2 CC6.8, CC7.2 CC7.4	Controls should be established for logical access to supporting tools and systems. Controls should be established to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. Controls should be established to monitor system components and the operation of those components for anomalies that are indicative of malicious acts, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
Microsoft Azure	Hosting services and support for Paychex Flex Assistant	CC2.2 CC4.1 CC4.2	Controls should be established: — Over communicating responsibilities, changes, and requirements to their employees whose roles affect system operation. — Over communicating application down-time/outages and significant changes that would affect system security and availability Controls should be established for performing assessments over changes that could impact system operation. Controls should be established over performing assessments and monitoring and taking action on issues identified.

		CC6.1 – CC6.3	Controls should be established over logical access, including password configurations, user access, and encryption.
		CC6.4	Controls should be established over physical access, including physical security, environmental protection, and administration.
		CC6.5	Controls should be established over physical access, including physical security, environmental protection, and administration.
		CC6.6, CC6.7	Controls should be established over logical access security such as encryption, firewalls, and security monitoring.
		CC6.8	Controls should be established: — Over maintaining requirements for documentation, authorization, testing, approval and implementation of new programs/system components. — Over monitoring against malware and security breaches.
		CC7.1	Controls should be established: — Over performing vulnerability assessments and penetration tests and addressing the results. — Over monitoring for security incidents.
		CC7.2	Controls should be established: — Over performing vulnerability assessments and penetration tests, and addressing the results. — Over monitoring for security incidents.
		CC7.3	Controls should be established monitoring and evaluating security incidents.
		CC7.4	Controls should be established: — Over performing vulnerability assessments and penetration tests, and addressing the results. — Over monitoring for security incidents. — Over performing data backups.
		CC7.5	Controls should be established over data restoration.

Subservice Organization	Services Provided	Related Trust Criteria	Complementary Subservice Organization Controls
		CC8.1	Controls should be established: — For change management over requesting, reviewing, approving, managing, testing, and applying infrastructure changes and upgrades to production — Over maintaining requirements for documentation, authorization, testing, approval and implementation of new programs/system components. — Over performing vulnerability assessments and penetration tests, and addressing the results — Over restriction of access to make changes
		CC9.1	Controls should be established over disaster recovery planning and testing.
		A1.1	Controls should be established: — Over availability monitoring. — Notifying affected users of downtime — Over capacity planning
		A1.2	Controls should be established: — Over environmental protection — Over backups — Over access to backups — Over disaster recovery planning and testing — Over data restoration
		A1.3	Controls should be established: — Over disaster recovery planning and testing — Over data restoration

SECTION IV

PAYCHEX, INC.'S CRITERIA AND RELATED CONTROLS, AND PWC LLP'S TESTS OF CONTROLS AND RESULTS OF TESTS

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

TRUST SERVICES CRITERIA AND PAYCHEX, INC.'S RELATED CONTROLS

The following table represents the AICPA Trust Services Criteria related to Security, Availability, and Processing Integrity and the related control activities of Paychex supporting the Paychex Flex Retirement Services, Payroll, And Reporting Services system. Control number references included within the following table map to the control activities included within the Paychex, Inc. Control Activities Table.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Control Environment	CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	Ethics, Integrity and Security-based Training
		CC1.1.2	Code of Conduct and Ethical Standards
		CC1.1.3	Acknowledgement of Code of Conduct
		CC1.1.4	Disciplinary Process, Code of Conduct
		CC1.1.5	Ethics Hotline and Complaint Investigation
		CC1.1.6	HR Policies and Procedures
		CC1.1.7	Acceptable Use Policy and Acknowledgement
		CC9.2.5	Vendor Contracts and Terms
		CC9.2.1	Information Sharing Agreements
		CC1.2.1	Board Roles, Responsibilities, and Independence
	CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
		CC1.2.3	Information Security Standards Approval
		CC1.2.4	Internal Audit Department and Plans
		CC1.2.5	Quarterly Reporting to Board of Directors
		CC1.2.6	Security Governance Committee
		CC1.2.7	Audit Findings

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	Organizational Structure
		CC1.2.3	Information Security Standards Approval
		CC1.3.3	Job Descriptions
		CC9.2.5	Vendor Contracts and Terms
		CC1.2.6	Security Governance Committee
		CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
	CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.1	Job Applicant Screening
		CC1.4.2	Learning Development
		CC1.1.8	Background Screening
		CC1.1.1	Ethics, Integrity and Security-based Training
		CC1.4.5	Performance Reviews
		CC1.1.6	HR Policies and Procedures
		CC1.3.3	Job Descriptions
		CC3.4.1	Risk Assessment Review Meetings
	CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.3.3	Job Descriptions
		CC1.4.5	Performance Reviews
		CC1.1.4	Disciplinary Process, Code of Conduct
		CC1.2.4	Internal Audit Department and Plans
		CC1.2.7	Audit Findings
		CC1.3.1	Organizational Structure

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Communication and Information	CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC5.2.2	Narrative Review
		CC2.1.3	System Information
		CC2.1.4	Network Diagram
		CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
		CC1.2.4	Internal Audit Department and Plans
		CC2.3.1	Reporting Security Incidents – External
		CC5.3.1	Policies and Standards
		CC2.2.13	Changes to Commitments and System Requirements
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC1.1.1	Ethics, Integrity and Security-based Training
		CC7.2.7	Monitoring, Problem Identification, and Resolution

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC1.1.5	Ethics Hotline and Complaint Investigation
		CC5.3.1	Policies and Standards
		CC2.2.3	System Description
		CC1.3.3	Job Descriptions
		CC2.2.5	Communication of System Change – Internal
		CC1.2.3	Information Security Standards Approval
		CC5.2.2	Narrative Review
		CC1.2.5	Quarterly Reporting to Board of Directors
		CC1.2.7	Audit Findings
		CC1.1.1	Ethics, Integrity and Security-based Training
		CC2.2.11	Security Program Updates
		CC2.2.12	Reporting Security Incidents – Internal
		CC2.2.14	Information to Improve Security Knowledge and Awareness
		CC2.2.15	Incident Response Policies
		CC2.2.13	Changes to Commitments and System Requirements
		CC1.1.7	Acceptable Use Policy and Acknowledgement
		CC1.1.3	Acknowledgement of Code of Conduct
		CC2.2.17	Periodic Meeting to Communicate Necessary Information

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	Reporting Security Incidents – External
		CC2.2.3	System Description
		CC2.3.3	Third-party Agreements
		CC2.3.4	Communication of System Change – External
		CC2.3.5	Customer Learning
		CC7.3.4	Incident Response Plan
		CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
		CC1.1.5	Ethics Hotline and Complaint Investigation
		CC2.2.13	Changes to Commitments and System Requirements
Risk Assessment	CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	IT Risk Assessment Methodology and Risk Tolerance
		CC3.1.2	Contract Management Policy
		CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC3.3.1	Fraud Risk Assessment
		CC5.3.1	Policies and Standards

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC1.2.7	Audit Findings
		CC2.2.11	Security Program Updates
		CC1.2.6	Security Governance Committee
		CC3.2.5	Risk Register
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC3.3.1	Fraud Risk Assessment
		CC1.2.4	Internal Audit Department and Plans
		CC9.2.4	Vendor Risk Assessments
		CC3.1.1	IT Risk Assessment Methodology and Risk Tolerance
		CC6.1.2	System Component Inventory
	CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.3.1	Fraud Risk Assessment
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC1.1.5	Ethics Hotline and Complaint Investigation
		CC3.3.4	New Client Fraud Risk Assessment

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.4.1	Risk Assessment Review Meetings
		CC3.2.6	IT Risk Assessments
		CC1.3.1	Organizational Structure
		CC9.2.4	Vendor Risk Assessments
		CC7.1.2	Vulnerability Scans and Reporting
		CC7.2.2	System Security Monitoring
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC1.2.1	Board Roles, Responsibilities, and Independence
		CC1.2.2	Board of Directors Corporate Governance Guidelines
Monitoring Activities	CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC1.2.7	Audit Findings
		CC3.4.1	Risk Assessment Review Meetings
		CC3.2.6	IT Risk Assessments
		CC4.1.2	Compliance Checks
		CC1.2.4	Internal Audit Department and Plans
		CC4.1.4	Internal Audit Competencies and Specialized Skills
		CC7.1.2	Vulnerability Scans and Reporting
		CC7.2.9	Security and Penetration Assessments
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.2.4	IDS Monitoring

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC3.2.5 CC1.2.5 CC1.2.7 CC3.4.1 CC3.2.6 CC7.2.4	Risk Register Quarterly Reporting to Board of Directors Audit Findings Risk Assessment Review Meetings IT Risk Assessments IDS Monitoring
Control Activities	CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1 CC3.2.5 CC6.3.6 CC5.3.1 CC1.2.4 CC3.2.6	Risk to Controls Mapping and Risk Mitigation Risk Register Segregation of Duties Policies and Standards Internal Audit Department and Plans IT Risk Assessments
	CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.1.1 CC3.2.6 CC5.2.2 CC5.3.1	Risk to Controls Mapping and Risk Mitigation IT Risk Assessments Narrative Review Policies and Standards

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC5.3.1	Policies and Standards
		CC1.2.3	Information Security Standards Approval
		CC1.1.6	HR Policies and Procedures
		CC1.3.3	Job Descriptions
		CC1.2.4	Internal Audit Department and Plans
		CC1.4.5	Performance Reviews
		CC3.2.6	IT Risk Assessments
		CC1.4.1	Job Applicant Screening
		CC5.2.2	Narrative Review

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Logical and Physical Access Controls	CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.1	Logical Access Policy
		CC6.1.2	System Component Inventory
		CC6.1.3	User Authentication
		CC6.6.2	Remote Access
		CC6.7.5	Digital Server Certification and TLS Encryption
		CC6.1.8	Array Encryption
		CC6.1.9	Architecture and Security
		CC7.2.2	System Security Monitoring
		CC7.2.4	IDS Monitoring
		CC6.7.3	Ability to Transmit, Move, or Remove Information
		CC6.8.4	Antivirus and Malware Technology
		CC7.1.1	Baseline Configurations
		CC7.1.3	Privileged Activity Monitoring
		CC2.1.4	Network Diagram
		CC6.1.16	Cryptographic Keys
		CC6.7.4	SFTP Access
		CC6.1.15	Unique IDs
		CC6.7.9	Data Segregation

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2.1 CC6.2.2 CC6.2.4 CC6.2.5 CC6.3.4 CC7.1.3	User Management - Addition User Management - Revocation Periodic User Access Review External User Access Privileged Access Approval Privileged Activity Monitoring
	CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.2.1 CC6.2.2 CC6.3.4 CC6.2.4 CC6.3.6 CC6.3.10 CC7.1.3 CC6.2.5	User Management - Addition User Management - Revocation Privileged Access Approval Periodic User Access Review Segregation of Duties Access to Batch Jobs Privileged Activity Monitoring External User Access

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.4.1	Facilities Access
		CC6.4.2	Security Cameras
		CC6.4.3	Visitor Procedures
		CC6.4.4	Access to Physical Checks and Payroll Input
		CC6.4.5	Access to Payroll Packages
		CC6.4.6	Physical Access to Check Printing and Unused Checks
		CC6.4.8	Facility Access Authorization
		CC6.4.9	Facility Access Revocation
		CC6.4.10	Periodic Facility Access Review
	CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	Equipment No Longer Used
		CC6.1.2	System Component Inventory
		CC6.5.2	Data Retention and Disposal Procedures

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.1.9	Architecture and Security
		CC6.6.2	Remote Access
		CC7.2.4	IDS Monitoring
		CC7.1.2	Vulnerability Scans and Reporting
		CC7.1.6	Firewall Standards
		CC6.7.5	Digital Server Certification and TLS Encryption
		CC6.7.4	SFTP Access
	CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.7.1	Removable Media
		CC6.7.2	Mobile Device Policies and Procedures
		CC6.7.3	Ability to Transmit, Move, or Remove Information
		CC6.7.4	SFTP Access
		CC6.7.5	Digital Server Certification and TLS Encryption
		CC6.1.8	Array Encryption
		CC6.1.9	Architecture and Security
		CC7.2.4	IDS Monitoring
		CC7.2.7	Monitoring, Problem Identification, and Resolution

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC6.8.1	Ability to Install Software
		CC7.2.2	System Security Monitoring
		CC8.1.1	Change Management Policy
		CC6.8.4	Antivirus and Malware Technology
		CC8.1.15	Software Updates and Patch Management
		CC7.1.2	Vulnerability Scans and Reporting
		CC6.1.9	Architecture and Security
		CC7.1.6	Firewall Standards
		CC6.1.2	System Component Inventory
		CC8.1.2	Change Initiation and Authorization
		CC8.1.14	Change Advisory Board
		CC8.1.13	Production Migration
		CC8.1.5	Separate Environments
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.3.4	Incident Response Plan

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Systems Operations	CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.1	Baseline Configurations
		CC7.1.2	Vulnerability Scans and Reporting
		CC7.1.3	Privileged Activity Monitoring
		CC7.1.6	Firewall Standards
		CC6.1.9	Architecture and Security
		CC6.8.4	Antivirus and Malware Technology
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.3.4	Incident Response Plan
		CC8.1.2	Initiation / Authorization
		CC8.1.9	Project Management
		CC8.1.10	Testing
		CC8.1.13	Production Migration
		CC8.1.15	Software Updates and Patch Management

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC2.3.1	Reporting Security Incidents – External
		CC7.2.2	System Security Monitoring
		CC2.2.12	Reporting Security Incidents – Internal
		CC7.2.4	IDS Monitoring
		CC7.4.4	Security Incident Management
		CC1.1.5	Ethics Hotline and Complaint Investigation
		CC7.3.4	Incident Response Plan
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.2.9	Security and Penetration Assessments
		CC6.4.2	Security Cameras
	CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.2.4	IDS Monitoring
		CC2.2.11	Security Program Updates
		CC2.2.15	Incident Response Policies
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC2.3.1	Reporting Security Incidents – External
		CC2.2.12	Communication of Incidents – Internal
		CC3.4.1	Risk Assessment Review Meetings
		CC7.3.4	Incident Response Plan
		CC7.5.3	Assessment of Incident Response

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC7.5.3	Assessment of Incident Response
		A1.2.3	Database Backup Replication
		CC7.4.4	Security Incident Management
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.5.5	Incident Response Plan Testing
		CC7.3.4	Incident Response Plan
		A1.3.1	Business Continuity Planning and Disaster Recovery Documentation and Testing

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	CC8.1.2	Initiation / Authorization
		CC8.1.9	Project Management
		CC8.1.10	Testing
		CC8.1.13	Production Migration
		CC3.2.6	IT Risk Assessments
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.1.2	Vulnerability Scans and Reporting
		CC7.1.1	Baseline Configurations
		CC8.1.5	Separate Environments
		CC7.4.4	Security Incident Management
		CC7.5.3	Assessment of Incident Response
		CC7.3.4	Incident Response Plan
		CC7.5.5	Incident Response Plan Testing
		A1.2.3	Database Backup Replication
		A1.2.4	Backup Scheduling and Off-site Storage
		A1.3.1	Business Continuity Planning and Disaster Recovery Documentation and Testing

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Change Management	CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC3.4.8	Statutory Change Initiation
		CC3.4.9	Statutory Change Approval
		CC8.1.1	Change Management Policy
		CC8.1.2	Initiation / Authorization
		CC7.1.2	Vulnerability Scans and Reporting
		CC8.1.15	Software Updates and Patch Management
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		CC7.1.1	Baseline Configurations
		CC8.1.5	Separate Environments
		CC8.1.8	Systems Development Life Cycle Methodology
		CC8.1.9	Project Management
		CC8.1.10	Testing
		CC8.1.11	Security-based Testing
		CC8.1.12	Source Code Management
		CC8.1.13	Production Migration
		CC8.1.14	Change Advisory Board

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Risk Mitigation	CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC3.4.1	Risk Assessment Review Meetings
		CC3.2.6	IT Risk Assessments
		CC9.1.3	Use of Insurance
		CC7.5.5	Incident Response Plan Testing
		A1.1.3	Application Monitoring
		A1.2.3	Database Backup Replication
		A1.2.4	Backup Scheduling and Off-site Storage
		A1.3.1	Business Continuity Planning and Disaster Recovery Documentation and Testing
	CC9.2 The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	Information Sharing Agreements
		CC2.3.3	Third-party Agreements
		CC9.2.4	Vendor Risk Assessments
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		CC9.2.5	Vendor Contracts and Terms
		CC9.2.6	Service Level Assessment (SLA) Monitoring

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Additional Criteria For Availability	A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A1.1.1	Capacity Management and Planning
		A1.1.2	Capacity Management Policies and Procedures
		A1.1.3	Application Monitoring
		CC7.2.7	Monitoring, Problem Identification, and Resolution
	A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2.1	Equipment Maintenance
		A1.2.3	Database Backup Replication
		A1.2.4	Backup Scheduling and Off-site Storage
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		A1.2.6	Data Backup Standard
		CC3.2.6	IT Risk Assessments
		CC3.4.1	Risk Assessment Review Meetings
		A1.3.1	Business Continuity Planning and Disaster Recovery Documentation and Testing
	A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3.1	Business Continuity Planning and Disaster Recovery Documentation and Testing
		A1.3.2	Business Continuity Planning and Disaster Recovery Training
		A1.2.3	Database Backup Replication
		A1.2.4	Backup Scheduling and Off-site Storage

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
Additional Criteria for Processing Integrity	PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	PI1.1.1	Data Definitions and Mapping
		PI1.1.2	Design Specifications
		PI1.1.3	Core Payroll Electronic Appointment Schedule
		PI1.1.4	Employees Gross Pay and Net Pay Calculations
		PI1.1.5	Client Payroll Contact
		PI1.2.2	Payroll Input
		PI1.1.7	Tax Withholding Rate
		PI1.1.8	Plan and Participant Account Valuations
		PI1.1.9	Plan Authorization

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	PI1.2.1	Data Validation
		PI1.2.2	Payroll Input
		PI1.2.3	Control Totals Calculation
		PI1.2.4	Direct Deposit Edit Checks
		PI1.2.5	Transaction Logs – Payroll
		PI1.2.6	Client Setup
		PI1.2.7	Edit Checks
		PI1.2.8	Cash Receipt Processing
		PI1.2.9	Distributions Authorization
		PI1.2.10	Automated Edit Checks
		PI1.2.11	Dividend/Earnings Activity Processing
		PI1.2.12	Calculation and Posting of Dividend/Earnings
		PI 1.3.16	Loans and Distributions Processing
		CC7.2.7	Monitoring, Problem Identification, and Resolution
		PI1.2.13	Transaction Logs – Retirement Services

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

	PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	PI1.3.1	Data Processing
		PI1.3.2	Scheduled Job Monitoring and Problem Management
		PI1.3.3	Payroll Processing Checks
		PI1.3.4	Job Schedule Modification Requests
		PI1.3.5	Payroll Monitoring and Problem Management
		PI1.3.6	Distributions Details
		PI1.3.7	Tax Withholding Rates
		PI1.3.8	Participant Web Transactions
		PI1.3.9	Outstanding Manual Contributions
		PI1.3.10	Bank Statement Reconciliations
		PI1.3.11	Transaction Reject Report Review
		PI1.3.12	Daily Share Balance Reconciliation
		PI1.3.13	System Edit Checks
		PI1.3.14	Investment Elections Quality Control Review
		PI1.3.15	Vesting Percentage Review
		PI1.3.16	Loans and Distributions Processing
		PI1.3.17	Participant Contributions, Rollovers, Loan
		PI1.3.18	ACH Transaction Processing
		PI1.3.19	Plan Asset Transfer Requests
		PI1.3.20	Automated Participant Web Transactions
		PI1.3.21	Purchase and Sale Transactions
		PI1.3.22	Terminated Participant Distribution
		PI1.3.23	Monthly Share Balance Reconciliation
		CC7.2.7	Monitoring, Problem Identification, and Resolution

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	PI1.4.1	Check Stock
		PI1.4.2	Distribution of Payroll Packages
		PI1.4.3	Payroll Checks and Standard Reports
		PI1.4.4	Client and Participant Statement Review
		PI1.4.5	Statement Files
		PI1.4.6	Confirmations for Online Transactions
		PI1.4.7	Reconciliation of Vendor Invoices and Associated Statement Files
		CC6.7.2	Mobile Device Policies and Procedures
		CC6.7.1	Removable Media
		CC6.1.9	Architecture and Security
		CC6.2.4	Periodic User Access Review
		CC6.1.3	User Authentication
		CC6.1.8	Array Encryption
		CC6.7.4	SFTP Access
		CC6.7.5	Digital Server Certification and TLS Encryption

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

AICPA Trust Services Criteria (TSP Section 100) and Related Control Activity Mapping			
Category	**Criteria**	**Control Number Reference**	**Control Titles**
	PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	CC6.5.2	Data Retention and Disposal Procedures
		CC3.2.7	Information Security Classification Standard
		CC6.4.11	Physical Access Policy
		CC6.4.1	Facilities Access
		CC6.4.3	Visitor Procedures
		CC6.4.8	Facility Access Authorization
		CC6.4.9	Facility Access Revocation
		CC6.4.10	Periodic Facility Access Review
		CC6.4.2	Security Cameras
		A1.2.1	Equipment Maintenance
		A1.2.3	Database Backup Replication
		A1.2.4	Backup Scheduling and Off-site Storage
		CC6.7.2	Mobile Device Policies and Procedures
		CC6.7.1	Removable Media
		CC6.1.9	Architecture and Security
		CC6.2.4	Periodic User Access Review
		CC6.1.3	User Authentication
		CC6.1.8	Array Encryption
		CC6.7.4	SFTP Access
		CC6.7.5	Digital Server Certification and TLS Encryption

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

The following are the control activities designed and implemented within the Paychex control environment to meet the security, availability, and processing integrity categories as set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentially and Privacy (AICPA, Trust Services Criteria)*, and PwC LLP's tests of controls and results of tests:

Paychex, Inc. Control Activities Table

Completeness and Accuracy of Information Produced by the Entity: When using information produced by Paychex, Inc., PwC 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.

Control #	***Controls Specified by Paychex, Inc.***	***PwC LLP's Tests of Controls***	***Results of Tests***
CC1.1.1	*Ethics, Integrity and Security-based Training* On an annual basis, employees must complete the Right Way Training program which encourages integrity and ethics, as well as security and internal controls. Completion for all employees is monitored by management.	For a sample of employees, inspected training documents to determine whether the Right Way Training program was completed. Inspected supporting documentation to determine whether management monitored employee completion. Inspected the Right Way Training materials to determine whether the training included integrity and ethics as well as security and internal controls.	No exceptions noted.
CC1.1.2	*Code of Conduct and Ethical Standards* Paychex has a documented code of business conduct and ethical standards which are reviewed, updated if applicable, and approved by the Board of Directors on an annual basis.	Inspected the code of business conduct and ethical standards to determine whether the Board of Directors reviewed and approved them on an annual basis.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC1.1.3	*Acknowledgement of Code of Conduct* New hires are required to read and accept the code of business conduct and ethical standards upon their hire via training and formally reaffirm them annually thereafter via Right Way training.	For a sample of new hires inspected new hire training completion documentation to determine whether the business conduct and ethical standards was acknowledged upon hire. For a sample of employees, inspected training documents to determine whether the Right Way Training program was completed.	No exceptions noted.
CC1.1.4	*Disciplinary Process, Code of Conduct* Management monitors personnel compliance with code of business conduct and ethical standards via training and the performance review process. The process for disciplinary action is communicated to employees via the HR intranet site under the Corrective Action page.	Inspected the Corrective Action page via the HR intranet site to determine whether disciplinary action was communicated to employees. Inspected a sample of employee performance reviews to determine whether management monitored personnel compliance with the code of business conduct and ethical standards.	No exceptions noted.
CC1.1.5	*Ethics Hotline and Complaint Investigation* Management has an anonymous third-party administered ethics hotline available to internal and external users. Depending on nature of complaint, appropriate entities will be engaged to conduct investigations regarding the complaint.	Inspected the Ethics hotline page to determine whether the hotline was available and communicated to both internal and external users. Observed an individual call the ethics hotline to determine whether the hotline existed and was available for complaints. For a sample of complaints, inspected tickets to determine whether investigations were conducted and resolved.	No exceptions noted.
CC1.1.6	*HR Policies and Procedures* Policies related to ethics and compliance are communicated to all employees via Paychex's HR intranet site.	Inspected the HR intranet site documents to determine whether HR policies and procedures related to ethics and compliance were communicated, reviewed, and updated as needed.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC1.1.7	*Acceptable Use Policy and Acknowledgement* Paychex's Acceptable Use Policy (AUP) requires employees to be aware of and comply with the Employee Handbook to encourage acceptable behavior, ethics and fraud policies. New hires are required to acknowledge the Employee Handbook via training upon onboarding.	Inspected the Acceptable Use Policy (AUP) to determine whether the policy required employees to be aware and comply with the Employee Handbook. Inspected the Employee Handbook to determine whether it contained sections on acceptable behavior, ethics and fraud policies. For a sample of new hires, inspected new hiring training completion documentation to determine whether the Employee Handbook was acknowledged.	No exceptions noted.
CC1.1.8	*Background Screening* Background screening procedures are performed and documented for new employees, including vendors and contractors, as a part of the hiring process prior to onboarding.	For a sample of new employees, including vendors and contractors, inspected background screening documentation to determine whether it was performed as part of the hiring process prior to onboarding.	No exceptions noted.
CC1.2.1	*Board Roles, Responsibilities, and Independence* The Board of Directors, including roles, responsibilities, and expertise is appointed as outlined in the Corporate Governance Guidelines. The Board of Directors consists of independent members as per the guidelines to maintain independence.	Inspected the listing of all members of the Board of Directors to determine whether members were independent of management in accordance with Corporate Governance Guidelines. Inspected the Corporate Governance Guidelines to determine whether it included Board of Directors' roles, responsibilities, and expertise.	No exceptions noted.
CC1.2.2	*Board of Directors Corporate Governance Guidelines* The Corporate Governance Guidelines, published on Paychex's website, guide conduct principles for the Board of Directors and document size, selection, election, meeting attendance, term limits and board functions.	Inspected the Paychex website to determine whether the Corporate Governance Guidelines were published, available and included conduct principles, size, selection, election, meeting attendance, term limits, and board functions.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC1.2.3	*Information Security Standards Approval* Information security standards are established and approved by IT management and made available to employees via the intranet.	Inspected the information security standards to determine that the standards were established, documented, and made available to employees via the intranet. Inspected the information security standards to determine whether each standard was approved by IT management.	No exceptions noted.
CC1.2.4	*Internal Audit Department and Plans* The Internal Audit function develops a risk based Internal Audit Plan and performs periodic audits to provide independent, objective and timely assurance to management as well as identify potential changes to Paychex's risk profile.	Inspected the Internal Audit Plan and periodic audit reports to determine whether the risk based plan was developed and periodic audits were completed to provide independent, objective, timely assurance to management, and identified potential changes to Paychex's risk profile.	No exceptions noted.
CC1.2.5	*Quarterly Reporting to Board of Directors* On a quarterly basis, the Board of Directors receives quarterly updates from the CISO including internal control deficiencies that are used to drive security-related objectives and functioning of internal control.	For a sample of quarters, inspected board meeting agenda and minutes to determine whether the CISO and the Board of Directors met to communicate internal control deficiencies and security related objectives.	No exceptions noted.
CC1.2.6	*Security Governance Committee* The Security Governance Council (SGC), a subcommittee of the Audit Committee, is established to oversee key risks. The SGC meets on a quarterly basis to review how risks are managed, and is chaired by the CISO and comprised of all senior officers and key personnel to support cross-functional representation.	For a sample of quarters, inspected meeting invites and agendas to determine whether the SGC meetings were held, key risks were discussed, and the meeting was chaired by the CISO and included senior officers and key cross-functional personnel.	No exceptions noted.
CC1.2.7	*Audit Findings* Audit results, including findings, are documented and tracked in a central repository and shared with leadership in issued audit reports and quarterly Audit Committee meetings.	Inspected the central repository to determine whether audit results, including findings, were documented and tracked. For a sample of quarters, inspected the audit reports and Audit Committee meeting minutes to determine whether audit results, including findings, were shared with leadership.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC1.3.1	*Organizational Structure* Organizational charts are created by senior leadership, are documented and communicated via the Paychex Blue Pages SharePoint site. The organizational charts and reporting lines, authorities, and responsibilities are reviewed and updated as needed based on organizational changes.	Inspected the Paychex Blue Pages SharePoint site to determine whether organizational charts were established and communicated. Inspected the organizational charts to determine whether reporting lines, authorities, and responsibilities were established, reviewed, and updated as needed based on organizational changes.	No exceptions noted.
CC1.3.3	*Job Descriptions* Roles and responsibilities (including segregation of duties as necessary), required skills and educational experience are defined in written job descriptions and updated as necessary.	For a sample of new hires and contractors, inspected the associated job descriptions to determine whether a written job description outlining roles and responsibilities, required skills and educational experience was defined and updated as necessary.	No exceptions noted.
CC1.4.1	*Job Applicant Screening* Roles, responsibilities and required educational experience and skills are defined in written job descriptions as part of the hiring process and candidates are tracked in a centralized tool. Education and experience is evaluated as part of the HR background screening process to support the achievement of objectives.	For a sample of new hires and contractors, inspected documentation to determine whether education and experience is evaluated as part of the HR background checks process to support the achievement of objectives and candidates were tracked in a centralized tool. For a sample of new hires and contractors, inspected the associated job descriptions to determine whether a written job description outlining roles and responsibilities, required skills and educational experience was defined and updated as necessary.	No exceptions noted.
CC1.4.2	*Learning Development* A learning development program exists for a variety of business units to provide job skills training and knowledge sharing in LMS (Cornerstone).	Inspected LMS to determine whether a learning development program exists for business units to provide job skills training and the trainings are tracked by management.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC1.4.5	*Performance Reviews* Quarterly performance reviews are conducted for each Paychex employee via the Learning Management System (LMS) to evaluate performance of responsibilities and competency as well as commitment to integrity and ethical compliance. Paychex establishes measurable goals and performance evaluation criteria. Individuals create specific goals to align with the company's "Blue Chips" which are evaluated as part of performance.	For a sample of quarters and employees, inspected LMS to determine whether performance reviews were completed to evaluate performance of responsibilities, competency, and commitment to integrity and ethical compliance. For a sample of quarters and employees, inspected Blue Chips document to determine whether Paychex goals were specified, measured, and a component of the performance evaluation.	No exceptions noted.
CC2.1.3	*System Information* Paychex performs an assessment at least annually to identify and document key system information required to support internal controls and the achievement of Paychex's service commitments and system requirements.	Inspected the documentation to determine whether Paychex performed an annual assessment that identified and documented key system information supporting internal controls and achievement of Paychex's service commitments and system requirements.	No exceptions noted.
CC2.1.4	*Network Diagram* Network diagrams are reviewed and updated to ensure they accurately describe connections to wireless networks and sensitive information.	Inspected network diagrams to determine whether they were documented, reviewed, and updated to accurately describe connections to wireless networks and sensitive information.	No exceptions noted.
CC2.2.3	*System Description* Paychex posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users via procedures and control narratives, and on the internet, in-app user guides and published white papers for external users.	Inspected Paychex intranet site and website to determine whether procedures, control narratives, user guides and white papers were available for internal and external users and communicated the description of the system, system boundaries, and system processes that included infrastructure, software, people, and data.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC2.2.5	*Communication of System Change – Internal* Planned software and infrastructure changes are communicated to internal users via the Change Calendar feature within ServiceNow. The calendar indicates the date and time of each change release on a given day.	Observed the Change Calendar within ServiceNow to determine whether planned software and infrastructure changes were communicated to internal users and detailed the date and time of each change release on a given day.	No exceptions noted.
CC2.2.11	*Security Program Updates* On a monthly basis, the CISO, CTO, and CIO are presented with a Security Program Update (SPU) including key security and availability metrics, events and incidents where relevant. As part of these meetings, risk assessment updates, risk assessment calendars and identified threats, and action items are also discussed.	For a sample of months, inspected SPU meeting invitations and the meeting minutes/deck to determine whether the CISO, CTO, and CIO were presented with key metrics, events, and incidents, risk assessment updates, threats and action items.	No exceptions noted.
CC2.2.12	*Reporting Security Incidents – Internal* Internal users have been provided with a Paychex IT Security Incident Standard which details how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the Paychex IT Security Incident Standard and Paychex intranet to determine whether internal users were communicated ways to report security failures, incidents and concerns. For a sample of security incidents, inspected ServiceNow tickets to determine whether issues were tracked and corrective action is taken in accordance with policy.	No exceptions noted.
CC2.2.13	*Changes to Commitments and System Requirements* Changes to Paychex's commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose services are part of the system via the Paychex website.	Inspected the Paychex website to determine whether Paychex's commitments and system requirements, including changes, if any, are communicated as applicable to external users, vendors, and other third parties.	No exceptions noted.
CC2.2.14	*Information to Improve Security Knowledge and Awareness* Paychex communicates active security notifications on the public website such as current security threats or via internal articles posted on Paychex's intranet site in order to improve security knowledge and awareness.	Inspected Paychex website and intranet site to determine whether Paychex communicated active security notifications on the public website or via internal articles to improve security knowledge and awareness.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC2.2.15	*Incident Response Policies* Incident response standards are in place, and communicated to employees that includes escalation plan based on the nature and severity of the incident to senior management as necessary.	Inspected the incident response standards to determine whether they were documented, communicated to employees and included an escalation plan based on the nature and severity of the incident to senior management.	No exceptions noted.
CC2.2.17	*Periodic Meeting to Communicate Necessary Information* Management and the Board of Directors meet quarterly to communicate information needed to fulfill their roles with respect to the achievement of Paychex's service commitments and system requirements.	For a sample of quarters, inspected board meeting agenda and minutes to determine whether management and the Board of Directors met and whether information needed to fulfill roles with respect to the achievement of Paychex's service commitments and system requirements were discussed.	No exceptions noted.
CC2.3.1	*Reporting Security Incidents – External* Paychex has made various communication channels available to external users such as contact emails, phone numbers, and other feedback portals for reporting issues or security incidents. Security incidents are investigated and documented in a ServiceNow ticket.	Inspected Paychex website to determine whether external users are communicated contact emails, phone numbers, and other feedback portals to report security failures and, incidents. For a sample of security incidents, inspected ServiceNow tickets to determine whether issues were tracked and corrective action is taken in accordance with policy.	No exceptions noted.
CC2.3.3	*Third-party Agreements* Agreements are established with service providers to mitigate risks, and are reviewed by relevant Legal and Security personnel as needed. Security addendums are included in the agreement where necessary to define responsibilities of vendors.	For a sample of new vendors, inspected the third-party agreements to determine whether vendor responsibilities were defined and agreements were reviewed by Legal and Security personnel and whether security addendums were included where necessary.	No exceptions noted.
CC2.3.4	*Communication of System Change – External* Unplanned downtime for software and infrastructure changes are communicated to external users via login screen and in-app messaging. Planned downtime is managed through the change management process and communicated as needed via the login screen and in-app messaging.	Inspected an instance of software and infrastructure unplanned downtime to determine whether unplanned downtime is communicated to external users through login screens and in-app messaging. For a sample of changes, inspected tickets to determine whether changes causing planned downtime adhere to the standard change management process.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC2.3.5	*Customer Learning* Online learning materials are accessible by customers. Onboarding materials are provided to new customers.	Inspected learning and onboarding materials to determine whether they were made accessible to customers.	No exceptions noted.
CC3.1.1	*IT Risk Assessment Methodology and Risk Tolerance* A risk assessment methodology exists for conducting qualitative assessments and measuring risks including defined risk tolerances and acceptable levels of variances in pursuit of specified key business objectives. Risk tolerance and appetite statements are maintained by Enterprise Security and Enterprise Risk teams.	Inspected the Paychex IT risk assessment methodology and risk tolerance and appetite statements to determine whether they were maintained by Enterprise Security and Enterprise Risk teams and whether they defined requirements for conducting assessments and risk tolerances and acceptable levels of variances in pursuit of key business objectives.	No exceptions noted.
CC3.1.2	*Contract Management Policy* Paychex has a Contract Management Policy for all vendor and business partner contracts. The policy covers processes related to the functioning of components of internal control and assists in the achievement of Paychex's business and strategic objectives.	Inspected the Contract Management Policy to determine whether it covered processes for vendor and business partner contracts which included processes related to the functioning of components of internal control and achievement of Paychex's business and strategic objectives.	No exceptions noted.
CC3.2.5	*Risk Register* Paychex consolidates risks and vulnerabilities including emerging and legal risks, PCI, risk assessment and audit findings in a centralized enterprise risk register in Archer that is shared with the business.	Inspected Archer to determine whether an enterprise risk register was in place and whether it included risks related to vulnerabilities, legal, PCI, risk assessments, and audit findings.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC3.2.6	*IT Risk Assessments* Enterprise Security (ESEC) IT Risk and Compliance perform IT risk assessments periodically based on emerging business needs and threats. Objectives incorporate service commitments and system requirements related to security. Risks identified during the assessment are entered into Paychex's enterprise risk register within Archer for tracking where mitigating controls and business owners are documented.	Inspected the IT risk assessment to determine whether ESEC IT Risk and Compliance performed it periodically based on emerging business needs, threats, and whether it incorporated service commitments and system requirements related to security, availability, and processing integrity. For a sample of months, inspected monthly vulnerability meeting invite and meeting agendas to determine whether IT risk assessment report and results were communicated to management and reviewed. Inspected the enterprise risk register to determine whether risks identified as part of ongoing IT risk assessments were entered and whether mitigating controls and business owners were documented.	No exceptions noted.
CC3.2.7	*Information Security Classification Standard* Paychex's Information Security Classification standard is in place to help ensure that all Paychex, partner and client information is properly labelled, handled, and protected into one of the following classification levels; public, internal and sensitive in order to mitigate risk and keep information restricted to authorized personnel.	Inspected the Information Security Classification Standard to determine whether the standard defined that Paychex partner and client information is properly labelled, handled, and protected within one of the following classification levels public, internal, and sensitive to mitigate the risk and keep information restricted to authorized personnel.	No exceptions noted.
CC3.3.1	*Fraud Risk Assessment* The Risk Management team is responsible for conducting periodic fraud risk assessments through a variety of initiatives as defined in the Know Your Customer and Anti-Money Laundering Operations Manual in order to identify the various ways that fraud and misconduct can occur.	Inspected the Know Your Customer and Anti-Money Laundering Operations Manuals, to determine whether the manuals addressed fraud risk and whether they defined the various ways that fraud and misconduct can occur. For a sample of fraud risk assessments conducted during the report period, inspected fraud risk assessment documentation to determine whether the assessment was performed by the Risk Management team and if the various ways fraud and misconduct can occur were identified.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC3.3.4	*New Client Fraud Risk Assessment* Paychex's Risk Management team performs an assessment for new customers' onboarding to the system to identify risk of potential fraud schemes.	For a sample of new customers, inspected risk assessment documentation to determine whether Paychex's Risk Management team performed an assessment of the customer to identify risk of potential fraud schemes prior to onboarding.	No exceptions noted.
CC3.4.1	*Risk Assessment Review Meetings* Monthly risk assessment review meetings are held to revisit open risks and assess changes (business, external environment, changes in technology, leaderships or vendors) that may impact the company's risk profile. Separately, monthly Security Program Update (SPU) meetings are held where risk assessment updates, risk assessment calendars and identified threats, and action items are discussed.	For a sample of months, inspected risk assessment review meeting invites and meeting minutes, to determine whether the meetings were held to revisit open risks and assess changes (business, external environment, changes in technology, leaderships or vendors) that may impact the company's risk profile. For a sample of months, inspected Security Program Update meeting invites and meeting minutes, to determine whether risk assessment updates, risk assessment calendars, identified threats, and action items were discussed.	No exceptions noted.
CC3.4.8	*Statutory Change Initiation* Statutory change requests require PD&IT Management approval before the change is established.	For a sample of tax rate changes, inspected the change request forms to determine whether PD&IT approval was obtained before the change was established.	No exceptions noted.
CC3.4.9	*Statutory Change Approval* Statutory change requests require two verification reviews after the change has been input.	For a sample of tax rate changes, inspected the request forms to determine whether two verification reviews were completed subsequent to input of the change.	No exceptions noted.
CC4.1.2	*Compliance Checks* Internal controls are evaluated on a scheduled basis (i.e. monthly, quarterly, and annual) by the Security Compliance department and results are tracked in Archer.	For a sample of compliance evaluations, inspected compliance documentation and results in Archer to determine whether internal controls were evaluated in accordance with schedule.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC4.1.4	*Internal Audit Competencies and Specialized Skills* Internal Audit individuals have the appropriate experience and expertise to conduct their work with proficiency and due professional care. Personnel resumes and/or certifications are documented and maintained.	For a sample of internal audit team individuals, inspected individual resumes to determine whether internal audit team members had audit experience, expertise and certifications documented to conduct their work with proficiency and due professional care.	No exceptions noted.
CC5.1.1	*Risk to Controls Mapping and Risk Mitigation* As part of periodic IT risk assessments, management links the identified risks to controls that have been designed and operated to address them.	Inspected a sample of risks to determine whether, as part of the IT risk assessments, management linked identified risks to controls that have been designed and operate to address the risk.	No exceptions noted.
CC5.2.2	*Narrative Review* Control narratives are stored in a centralized location and semi-annually, control owners review process narratives including technology activities and consideration of security and fraud related risks. Updates are made if needed and tracked in revision history.	For a sample of narratives, inspected documentation to determine whether control narratives were stored in a central location, reviewed semi-annually by control owners and updates were tracked in revision history.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC5.3.1	*Policies and Standards* As defined by Paychex's Development and Management of Security Policy Standard, the Paychex CISO, Security Governance Council (SGC), and Standards Review Committee (SRC) are responsible for managing, developing, maintaining, and communicating comprehensive security policies, standards, and procedures. Policies and standards including roles, responsibilities and objectives are communicated via Paychex's intranet and are reviewed and stored in a centralized repository, Archer. Policies and standards include access security, data classification, risk assessments, change management, system development life cycle, business continuity planning, backups and security incidents.	Inspected Paychex's Development and Management of Security Policy Standard to determine whether it defined that the Paychex CISO, Security Governance Council (SGC), and Standards Review Committee (SRC) were responsible for managing, developing, maintaining, and communicating comprehensive security policies, standards, and procedures. Inspected security policies and standards to determine whether roles, responsibilities, and objectives were documented and reviewed by the Paychex CISO, Security Governance Council (SGC), or Standards Review Committee (SRC). Inspected Archer and the Paychex intranet to determine whether access security, data classification, risk assessments, change management, system development life cycle, business continuity planning, backups and security incidents policies and standards were stored and communicated to employees.	No exceptions noted.
CC6.1.1	*Logical Access Policy* Policies and standards have been documented and establish the standards for restricting logical access to Paychex systems.	Inspected policies and standards to determine whether standards restricting logical access to Paychex systems were established and documented.	No exceptions noted.
CC6.1.2	*System Component Inventory* Paychex identifies, documents, and reviews the server inventory. Assets are logged, tracked and maintained using inventory tracking tools.	Inspected the Foreman tool to determine whether IT assets were identified, documented, monitored, tracked and tagged with an asset number.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.1.3	*User Authentication* To gain access to the network, operating systems, applications, and databases, users are required to use a unique login identifier and passwords subject to length, expiration, history, and lockout settings in accordance with Company requirements. Workstations are configured to automatically lock out after 15 minutes of inactivity.	Observed a staff person authenticate to the network to determine whether a login identifier was required. Inspected the network, operating systems, applications, and databases password settings to determine whether password parameter settings for length, expiration, history, and lockout were in accordance with the Company requirements. Inspected configuration settings to determine whether workstations were configured to automatically lock out after 15 minutes of inactivity.	No exceptions noted.
CC6.1.8	*Array Encryption* Databases storing client data sit on virtual servers in which disks are stored on storage arrays. Arrays are protected by always on encryption.	Inspected storage array configurations to determine whether encryption was configured to be always on.	No exceptions noted.
CC6.1.9	*Architecture and Security* The network architecture is segregated into segments and security includes firewalls, network-based Intrusion Detection Systems (IDS) and Network Address Translation (NAT). The firewall rejects any unauthorized external connections requesting access to the internal network.	Observed the dashboard and network system settings to determine whether firewalls, network-based IDS and NAT were configured and deployed. Observed the firewall rule base to determine whether the firewalls were configured to reject external connections that were identified as unauthorized. Observed the alerting tool to determine whether alerts were sent for firewall, IDS, NAT incidents.	No exceptions noted.
CC6.1.15	*Unique IDs* Unique IDs are provisioned as defined by Paychex's Account Administration Standard.	For a sample of users, inspected the user ID to determine whether the IDs were unique to the user in accordance with Paychex's Account Administration Standard. Observed the login process to in scope applications to determine whether access was authenticated via a unique user ID and password.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.1.16	*Cryptographic Keys* Access to cryptographic keys is restricted to the fewest number of custodians necessary.	Inspected access to cryptographic keys to determine whether it was restricted to the fewest number of custodians necessary that require access based on their job function.	No exceptions noted.
CC6.2.1	*User Management - Addition* Access request forms are completed and authorized by data owners for establishing user accounts for access to the network, operating systems, applications, and databases.	For a sample of new and transferred employees and contingent workers, inspected supporting documents to determine whether the access request form was completed and authorized by data owners and access granted was consistent with the access requested on the form.	No exceptions noted.
CC6.2.2	*User Management - Revocation* For terminated or transferred users, including contingent workers, HR and/or management submits a notification of the termination and access to the network, operating systems, applications, and databases is removed on a timely basis.	For a sample of transferred and terminated employees and contingent workers, inspected supporting documents and system records to determine whether the notification of the termination was timely and whether access to the network, operating systems, applications, and databases was removed in a timely manner.	No exceptions noted.
CC6.2.4	*Periodic User Access Review* On a periodic basis, access rights for the network, applications, operating systems, and databases are confirmed by assigned data owners to determine that access is commensurate with job responsibilities. Discrepancies are tracked, followed up on, and resolved. Sign-off and resolutions are documented on the review reports.	For a sample of roles and managers, inspected periodic access review reports to determine whether the reviews were completed and signed off and resolutions were documented. For a sample of users, inspected the periodic access reviews to determine whether access was appropriate based upon job responsibilities.	No exceptions noted.
CC6.2.5	*External User Access* External client users are given unique user IDs and set up with multi-factor authentication to access Paychex Flex.	For a sample of external users, inspected the user ID to determine whether the IDs were unique to the user in accordance with Paychex's Account Administration Standard. Observed the external user login process to Paychex Flex to determine whether access was authenticated using multi-factor authentication and a unique user ID and password.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.3.4	*Privileged Access Approval* Access to perform privileged activities is restricted to authorized individuals and additional approval is not required before privileged access activities may be performed.	For a sample of quarters, inspected supporting documents to determine whether privileged access reviews were completed and signed off and resolutions were documented.	No exceptions noted.
CC6.3.6	*Segregation of Duties* Paychex has documented policies and standards supporting segregation of duties, Least Privileges and Role Based Access.	Inspected policies and standards to determine whether segregation of duties, Least Privileges and Role Based Access were documented.	No exceptions noted.
CC6.3.10	*Access to Batch Jobs* Logical access to initiate, modify, or cancel scheduled application batch jobs is reviewed by the Data Center Production Manager on a monthly basis to confirm that access is commensurate with job responsibilities. Discrepancies are resolved in a timely manner.	For a sample of months, inspected the batch job access review to determine whether the Data Center Production Manager reviewed individuals with access to initiate, modify, or cancel computer jobs to ensure access was commensurate with their job responsibilities and if there are discrepancies whether they are resolved in a timely manner.	No exceptions noted.
CC6.4.1	*Facilities Access* Access to the CDC facilities is controlled through a biometric scanner and badge.	Observed the CDC facilities to determine whether physical access was controlled by a biometric scanner and badge.	No exceptions noted.
CC6.4.2	*Security Cameras* Cameras are present outside all CDC facilities entrances and are monitored by security guards.	Observed the CDC facilities entrances to determine whether cameras were present in rooms outside the DC facilities and at CDC entrances and whether security guards were monitoring the cameras.	No exceptions noted.
CC6.4.3	*Visitor Procedures* CDC facilities visitors are required to be accompanied by authorized personnel.	Observed the CDC facilities to determine whether visitors were required to be escorted by authorized personnel.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.4.4	*Access to Physical Checks and Payroll Input* Physical access to print, pack, and deliver payroll checks, files and reports and logical access to input payroll information are appropriately restricted.	Observed the areas where users print, pack, and deliver payroll checks, files and reports to determine whether access to these areas was restricted by card access. For a sample of employees with physical access to print, pack, and deliver payroll checks, files, and reports, inspected supporting documentation to determine whether each employee that also had logical access to input payroll information required such access based upon job function.	No exceptions noted.
CC6.4.5	*Access to Payroll Packages* Access to the secured areas where payroll packages awaiting delivery are stored is limited through badge card readers to appropriate personnel.	For a sample of employees with access to the secured areas where payroll packages are stored, inspected supporting documents to determine whether access was appropriate based upon job responsibilities. Observed the areas where payroll packages are stored to determine whether access to these areas was restricted by card access.	No exceptions noted.
CC6.4.6	*Physical Access to Check Printing and Unused Checks* Access to the secured area where check printing equipment and unused check stock are stored is limited through badge card readers to appropriate personnel.	For a sample of employees with access to check printing equipment and unused check stock, inspected supporting documents to determine whether access was appropriate based upon job responsibilities. Observed the check stock room to determine whether access was restricted by card access.	No exceptions noted.
CC6.4.8	*Facility Access Authorization* Access to the CDC facilities is granted based upon job function and upon approval by the Network Service Field Engineering Manager.	For a sample of new employees and contractors with access to the CDC facilities, inspected supporting documents to determine whether access was granted based upon job function and upon approval by the Network Service Field Engineering Manager.	No exceptions noted.
CC6.4.9	*Facility Access Revocation* Access to the DC facilities is removed on a timely basis.	For a sample of terminated employees, inspected access termination requests and system-generated access reports to determine whether access to the CDC facilities was removed in a timely manner.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.4.10	*Periodic Facility Access Review* The Network Service Field Engineering Manager conducts a quarterly review of users with access to the CDC facilities and confirms that access is commensurate with job responsibilities. Discrepancies are resolved.	For a sample of quarters, inspected the CDC access reviews to determine whether they were performed by the Network Service Field Engineering Manager to confirm that access was commensurate with job responsibilities and whether discrepancies, if any, were followed up and resolved. For a sample of users, inspected the access reviews to determine whether access was appropriate based upon job responsibilities.	No exceptions noted.
CC6.4.11	*Physical Access Policy* Policies have been documented and establish the standards for restricting physical access to the facilities and data center.	Inspected policies to determine whether standards restricting physical access to the facilities and data center were established and documented.	No exceptions noted.
CC6.5.1	*Equipment No Longer Used* Equipment slated for disposal, return, or reuse is wiped of data via degauss, reformat, or destroyed as per Paychex Standards and tracked in ServiceNow tickets. Hard copy media slated for destruction is dropped into locked and labeled specialized media bins located through-out Paychex facilities, cross-shredded or burned, or securely delivered to third-party vendor collection and disposal services.	For a sample of assets disposed of during the period, inspected the ServiceNow asset disposal record and related documentation to determine whether IT assets were tracked and disposed of according to Paychex standards including confirmation of disposal from third party vendor collection and disposal services. Observed Paychex facilities to determine whether hard copy media could be dropped into locked labeled specialized media bins, shredded or burned.	No exceptions noted.
CC6.5.2	*Data Retention and Disposal Procedures* Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Inspected Paychex intranet to determine whether formal data retention and disposal procedures were documented and provided guidance for the secure disposal of the company's and customers' data.	No exceptions noted.
CC6.6.2	*Remote Access* Employees working remotely authenticate to the network using two-factor authentication.	Observed a staff person remotely authenticate to the network to determine whether two-factor authentication was required.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.7.1	*Removable Media* Paychex requires all removable media to be encrypted and password protected as defined in the Encryption of Electronic Storage Devices Including Removable USB Standard. Users with the ability to write to removable media are approved on an exception basis.	Inspected the Encryption of Electronic Storage Devices Standard to determine whether Paychex required all removable media to be encrypted and password protected. Inspected removable media configuration to determine whether encryption and password protection were enabled. For a sample of users who have exceptions to bypass for use of removable media inspected documentation encryption configuration inquired of management to determine whether access to write to bypass removable media was approved and was limited based on job responsibility.	No exceptions noted.
CC6.7.2	*Mobile Device Policies and Procedures* Paychex has documented policies and procedures for the business use and data storage for mobile devices in order to prevent unauthorized use.	Inspected the Mobile Computing Device Acceptable Use Policy and procedures to determine whether procedures related to mobile device acceptable use, data storage, and to prevent unauthorized use were documented.	No exceptions noted.
CC6.7.3	*Ability to Transmit, Move, or Remove Information* Paychex monitors significant movements of data using various data loss prevention and security management tools. Suspicious activity is flagged via automated rules which is investigated and entered into tickets for security incident response as applicable.	Inspected the data loss prevention and security management tools monitoring dashboard to determine whether Paychex monitored significant data movements. Inspected rule sets within data loss prevention and security management tools to determine whether automated rules are configured to flag suspicious activity. For a sample of security incidents, inspected ServiceNow tickets to determine whether incident tickets were opened and corrective actions were implemented in accordance with policy.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.7.4	*SFTP Access* Access to secure file transfer protocols (SFTP) for transmission of confidential and/or sensitive information over public networks are restricted based on job responsibility.	Observed a transmission to determine whether SFTP was in place and utilized for transmissions of confidential and/or sensitive information over public networks. Inspected a sample of users with access to transmit confidential and/or sensitive data via SFTP to determine whether transmissions are restricted to personnel based on job responsibility.	No exceptions noted.
CC6.7.5	*Digital Server Certification and TLS Encryption* The applications require digital server certificates and TLS encryption.	Inspected the client facing applications security certificates to determine whether TLS encryption was required.	No exceptions noted.
CC6.7.9	*Data Segregation* Client data is logically segregated. Each client and their data are identified using a unique identifier.	Inspected a sample of clients to determine whether each sampled client was assigned a unique identifier to logically segregate their data in the database.	No exceptions noted.
CC6.8.1	*Ability to Install Software* The ability to install software is restricted to developers, network and database administrators. Any exceptions to the policy must be requested in ServiceNow tickets and approved by the individual's manager and granted by Security.	Inspected Active Directory User Access Control (UAC) configuration to determine whether the ability to install software was restricted to users with administrative privileges. For a sample of local administrative rights requests, inspected ServiceNow tickets to determine whether the exceptions were requested, approval was documented, and access was granted as requested.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC6.8.4	*Antivirus and Malware Technology* Antivirus and malware technology is deployed to prevent malicious attacks and quarantine suspicious files. If required, vulnerability and security related incident tickets are opened, and corrective actions are implemented in accordance with defined policies and procedures.	Inspected antivirus and malware technology configuration settings to determine whether antivirus and malware technology is deployed and configured to prevent malicious attacks and quarantine suspicious files. Inspected antivirus and malware technology to ServiceNow/APIs to determine whether antivirus and malware technology is configured to create vulnerability and security related incident alerts within ServiceNow. For a sample of security incidents, inspected ServiceNow tickets to determine whether security incident tickets were opened, triaged, tracked, and corrective actions were implemented in accordance with policy.	No exceptions noted.
CC7.1.1	*Baseline Configurations* Paychex IT resources are configured in accordance with established and documented hardening standards, and the applicable platform-specific security baseline. Periodic baseline configuration monitoring is used to check infrastructure compliance and vulnerabilities identified are documented and tracked through resolution. Vulnerabilities are resolved either through change management or incident resolution. Minimum baseline compliance and updates are discussed during monthly SPU meetings.	Inspected hardening standards and applicable platform-specific security baseline standards to determine whether baseline standards were documented. Inspected monitoring tool dashboards and rulesets to determine whether baseline configuration monitoring is in place to check infrastructure compliance. For a sample of monthly SPU meetings, inspected meeting invites and agendas to determine whether minimum baseline compliance and updates were discussed. Inspected a sample of incidents to determine whether the incidents were documented, tracked, and resolved.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC7.1.2	*Vulnerability Scans and Reporting* Vulnerability scans are performed daily as scheduled. Results are assessed and triaged and vulnerabilities are documented as ServiceNow tickets and assigned to the appropriate teams and tracked through resolution. If a vulnerability cannot be remediated, the vulnerability follows the Vulnerability Exception process that is documented and is entered into Paychex's risk register. Vulnerabilities including vulnerability exceptions are reviewed as part of monthly vulnerability and risk meetings. If required, system changes based on identified vulnerabilities may be initiated.	For a sample of days, inspected vulnerability scan results and associated documentation to determine whether scans were completed, potential threats were identified, and risks were analyzed and remediated as needed. For vulnerabilities identified that cannot be remediated, if any, inspected Paychex risk register to determine whether the exception process was followed. For a sample of months, inspected monthly vulnerability & risk assessment review meeting invites and agendas to determine whether monthly meetings were held to review vulnerabilities, including exceptions, and associated risks and action any necessary system changes.	No exceptions noted.
CC7.1.3	*Privileged Activity Monitoring* Privileged activities (administrative or super user) are reviewed on a monthly basis by IT management. Issues, if any, are followed up and resolved.	For a sample of months, inspected supporting documents to determine whether privileged activities were reviewed by IT management, and issues, if any, were followed up and documented.	No exceptions noted.
CC7.1.6	*Firewall Standards* Firewall rules and maintenance procedures are documented and reviewed on a periodic basis.	Inspected firewall standards to determine whether firewall rules and maintenance procedures were documented and reviewed on a periodic basis.	No exceptions noted.
CC7.2.2	*System Security Monitoring* The Paychex Enterprise Security Fusion Center (ESFC) monitors for anomalous activity and cyber-related insider and external threats that pose risk to the business operations through various detection tools which provide static log alerting, correlated log detection, anomalous activity, risk-based alerting, machine learning and behavioral analysis. Alerts are monitored by Cyderes for triage, resolution, and escalation if required. If escalation is required, vulnerability and security related incident tickets are opened, and corrective actions are implemented by Paychex in accordance with defined policies and procedures.	Observed the cyber threat detections tools including Enterprise Security SIEM to determine whether cyber-related events were monitored by the ESFC. Inspected the cyber threat detection tools to determine whether the tools provided static log alerting, correlated log detection, anomalous activity, risk-based alerting, machine learning and behavioral analysis. For a sample of security incidents, inspected ServiceNow tickets to determine whether security incident tickets were opened, triaged, tracked, and corrective actions were implemented in accordance with policy.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC7.2.4	*IDS Monitoring* Security Analysts monitor the network-based IDS that are used at the CDCs and at selected nodes of the Paychex WAN. Identified security violations are reported to IT management and violations are researched and resolved.	Observed the Security Analyst monitor tools used for IDS to determine whether monitoring was in place that covered the CDCs and selected nodes of the Paychex WAN. For a sample of security violations, inspected documentation to determine whether identified security violations were reported to IT management and research and resolutions were documented.	No exceptions noted.
CC7.2.7	*Monitoring, Problem Identification, and Resolution* Paychex personnel monitor system availability, performance, hardware issues, security issues, and backup equipment. Issues identified are documented, reported, and followed through to resolution in a timely manner.	For a sample of incidents identified by the monitoring tools, inspected supporting documents to determine whether issues were documented, reported, and resolved timely.	No exceptions noted.
CC7.2.9	*Security and Penetration Assessments* On a periodic basis, Paychex engages with third parties to perform security review assessments and penetration testing. This process validates and tests the ESFC and incident response procedures and the detection control itself.	For a sample of third-party security review assessments and penetration tests, inspected results and related incident tickets to determine whether tests were performed and whether identified vulnerabilities were tracked and resolved as needed.	No exceptions noted.
CC7.3.4	*Incident Response Plan* Paychex maintains an incident response plan as well as various playbooks for different incident types. The Incident Response Plan documents the Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned (PICERL) methodology to resolve incidents. Procedures include notifying external users as determined by the plan, policy and procedures, and Paychex Legal and Executive Team. The Incident Response Plan documents established roles and responsibilities of the security response team which includes both internal and external parties.	Inspected the incident response plan to determine whether the incident response plan was documented, included the PICERL methodology to resolve incidents, procedures to notify external users of incidents when necessary, and established roles and responsibilities of the security response team. Inspected a sample of playbooks to determine whether different incident types had specific procedures defined for resolution of the incidents and were made available to employees.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC7.4.4	*Security Incident Management* The Security Incident Unit (SIU) identifies and detects security incidents from Endpoint Detection & Response (EDR), Security Orchestration, Automation & Response (SOAR), Entity & User Behavioral Analysis (EUBA), Security Event & Incident Manager (SEIM) tools. Security events are triaged and escalated as needed based on severity and impact. All security incidents are logged, tracked, and communicated to appropriate parties through resolution.	Observed the SIU security monitoring dashboards to determine whether security monitoring tools including Endpoint Detection & Response (EDR), Security Orchestration, Automation & Response (SOAR), Entity & User Behavioral Analysis (EUBA), Security Event & Incident Manager (SEIM) were deployed. For a sample of security incidents, inspected security incident tickets to determine whether security incidents were triaged, escalated based on severity, logged, tracked, and communicated to appropriate parties through resolution.	No exceptions noted.
CC7.5.3	*Assessment of Incident Response* The Enterprise Security Fusion Center (ESFC) is comprised of the following groups: Cyber Intelligence, Threat Hunt, Cyber Detection, Insider Threat, Security Investigation Unit (SIU), and the 24/7 Managed Service Security Provider. Weekly meetings are held to discuss new playbooks and standard operating procedures relating to incident response. A Wiki is maintained containing playbooks, training materials and team knowledge articles	Inspected the ESFC organization chart and internal wiki to determine whether ESFC was comprised of the required groups and playbooks and training materials were documented and maintained. For a sample of weeks, inspected meeting invites and agendas to determine whether playbooks and standard operating procedures related to incident management were discussed by the ESFC on a weekly basis.	No exceptions noted.
CC7.5.5	*Incident Response Plan Testing* The incident management process is tested on an annual basis and includes communications tests, establishment of roles, and creation of recovery teams. Improvement points are documented as part of postmortem.	Inspected incident response plan testing to determine whether the incident response plan was tested on an annual basis and improvement points were documented postmortem.	No exceptions noted.
CC8.1.1	*Change Management Policy* Paychex has a formal change management policy that outlines the requirements for making system changes (application, hardware, operating system software, and database). The change management policy is updated and approved, as necessary, and updates are communicated.	Inspected the change management policy to determine whether the procedures related to making system changes were documented and updates were approved and communicated.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC8.1.2	*Initiation / Authorization* Requests for application, operating system, and database changes, including emergency changes, are standardized, documented, and subject to formal change management procedures, including authorization.	For a sample of application, operating system, and database changes, including emergency changes, inspected change management documentation to determine whether the change was requested on a standard form and authorized as required.	No exceptions noted.
CC8.1.5	*Separate Environments* Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation.	Inspected system screenshots to determine whether development, test, and production environments were separate for the applications and supporting infrastructure.	No exceptions noted.
CC8.1.8	*Systems Development Life Cycle Methodology* Paychex has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	Inspected SDLC methodology procedures to determine whether procedures were documented and detailed the methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	No exceptions noted.
CC8.1.9	*Project Management* All significant application development activities follow a project plan through user stories that include a project definition, project requirements, work plans, and progress monitoring procedures.	For a sample of application, operating system, and database changes, inspected the project plan to determine whether it included project definitions, requirement documents, work plans, and progress monitoring procedures.	No exceptions noted.
CC8.1.10	*Testing* A testing strategy, based on the nature of the change, is developed and followed for all changes in applications, operating systems, and databases so that deployed systems operate as intended. Testing approval is documented.	For a sample of application, operating system, and database changes, inspected testing documentation to determine whether testing was performed and approved.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC8.1.11	*Security-based Testing* Security-based testing is performed to verify application code changes and identify code vulnerabilities as part of the change management process.	For a sample of applications releases, inspected security-based testing documentation to determine whether code changes were verified, and vulnerabilities were identified as part of the change management process.	No exceptions noted.
CC8.1.12	*Source Code Management* Version control tools are used for managing application source code. These tools are used for updating source code and tracking changes to the source code. Changes to the source code are logged by the version control tools.	Observed version control tools to determine whether such tools were used to manage application source code and changes to source code were logged by the version control tools. For a sample of application, operating system, and database changes, inspected system records and documentation to determine whether version control tools were used to manage source code.	No exceptions noted.
CC8.1.13	*Production Migration* All production migrations are approved prior to implementation. Post implementation reviews are completed if deemed necessary by management and the change ticket is closed to indicate completion. Changes are developed and migrated by different users in order to maintain segregation of duties.	For a sample of application, operating system, and database changes, inspected change management documents to determine whether the request to migrate to the production environment was approved prior to implementation, that the change was implemented, and post implementation reviews were completed if management deemed necessary. Observed the release management tool to determine whether a standard process and tool was used to migrate changes to production. For a sample of application, operating system, and database changes, inspected change management documents to determine whether development and migration of the change were performed by different users.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC8.1.14	*Change Advisory Board* Change Advisory Board meetings are held daily. Meetings are held to review any comprehensive change requests submitted, including prior approvals and testing performed, and if approved are moved to production, any unapproved changes undergo further refinement. Approvals are documented within the ServiceNow ticket. CAB approvals are not required for software releases and for emergency changes are documented retroactively.	For a sample of days, inspected CAB meeting invites to determine whether changes were reviewed and discussed during the CAB meeting. For a sample of changes, inspected ServiceNow tickets to determine whether changes were approved by the CAB according to policy.	No exceptions noted.
CC8.1.15	*Software Updates and Patch Management* Patches are applied through a mix of automated and manual patching techniques. Patching follows Paychex's standard change management process and may be applied as a result of the incident response process.	Inspected a sample of patches to determine whether patches were applied through automated and manual patching or as a result of the incident response process in accordance with Paychex's standard change management process.	No exceptions noted.
CC9.1.3	*Use of Insurance* The risk management program includes the use of insurance to minimize the financial impact of any cybersecurity events.	Inspected Paychex's risk management program and certificate of insurance to determine whether Paychex subscribes to cybersecurity events insurance.	No exceptions noted.
CC9.2.1	*Information Sharing Agreements* Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.	Inspected a sample of new third-party vendors to determine whether information sharing agreements were in place and included the scope of services and security commitments applicable to that entity.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
CC9.2.4	*Vendor Risk Assessments* Initial vendor risk assessments are performed for vendors that have access to confidential data or could impact the service of the system and are documented within the third party vendor management system. The vendor risk assessment evaluates criticality (business critical, key vendor, or non-key) and the type of data being impacted in order to establish a risk score – minor, low, high, critical. Annual tiering re-assessments are sent to the vendor relationship manager to confirm that the nature and scope of the data has not changed. If the scope has changed or the vendor is deemed "Key/Business Critical", a full vendor re-assessment will be performed.	Inspected a sample of new vendors to determine whether an initial vendor assessment was performed, documented in third party vendor management tool, and has a defined criticality (business critical, key vendor, or non-key) , type of data being impacted , and an established risk score of minor, low, high, and critical. Inspected a sample of vendors to determine whether annual tiering vendor risk re-assessments were documented in the third party vendor management system in accordance with the vendor criticality score, completed and included required attributes according to policy.	Exceptions noted, management was unable to provide evidence that new vendor and annual re-assessments were performed.
CC9.2.5	*Vendor Contracts and Terms* Management identifies a Relationship Manager for each vendor, who ensures together with Legal, that the Master Service Agreement together with any subsequent Work Authorizations, Statements of Work, Change Orders etc. state the specific scope of services, roles and responsibilities, compliance requirements and service levels.	Inspected a sample of new vendors to determine whether signed Master Service Agreements together with any subsequent Work Authorizations, Statements of Work, or Change Orders were in place and whether a relationship manager was assigned, and contracts and terms stated scope of services, roles and responsibilities, compliance requirements and service levels.	No exceptions noted.
CC9.2.6	*Service Level Assessment (SLA) Monitoring* Monthly service level assessments for vendors are performed by the functional heads of each department. These assessments include evaluation of the operation of key controls and the SLAs noted within the contracts.	For a sample of months, inspected monthly SLA assessments to determine whether assessments for vendors included evaluation of the operation of key controls and SLAs and are performed by the functional heads of each department on a monthly basis.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
A1.1.1	*Capacity Management and Planning* Paychex monitors capacity in an internal dashboard that utilizes an 18 month backward perspective analysis used to forecast out for the next 6 months. Any changes are documented in terms of why things have changed. Paychex documents Capacity Change Requests in ServiceNow tickets.	Inspected the monitoring tool to determine whether capacity is monitored, and alert thresholds are configured. Inspected the internal dashboard to determine whether Paychex utilized an 18-month backward perspective to forecast the next 6 months of capacity. Inspected a sample of changes to determine whether changes are documented within ServiceNow tickets and follow the change management process.	No exceptions noted.
A1.1.2	*Capacity Management Policies and Procedures* Paychex has documented capacity management procedures and best practices and communicates to procedures to employees via the Paychex intranet.	Inspected the Paychex intranet to determine whether capacity management procedures and best practices were documented and communicated to employees.	No exceptions noted.
A1.1.3	*Application Monitoring* Paychex utilizes AppDynamics to monitor performance of applications as well as latency. Paychex has established alerting thresholds in the monitoring tools to alert the Security Engineering team of any issues. Any flagged issues are documented in ServiceNow and resolved in a timely manner.	Inspected alert configurations within AppDynamics to determine whether alerting thresholds have been established and whether the Security Engineering team is notified of issues. For a sample of issues, inspected the ServiceNow ticket to determine whether issue was documented and resolved in a timely manner.	No exceptions noted.
A1.2.1	*Equipment Maintenance* Preventative maintenance is performed according to schedule on the DC facilities' uninterruptible power supplies, generators, and HVAC systems.	Observed the DC facilities and noted the presence of uninterruptible power supplies, generators, and HVAC systems. Inspected supporting documents to determine whether preventive maintenance was performed according to schedule on the DC facilities' uninterruptible power supplies, fire suppression, generators, and HVAC systems.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
A1.2.3	*Database Backup Replication* Database backups are replicated to a secondary location in order to restore an environment in case of incident.	For a sample of databases, inspected NetBackup tool settings and status of secondary images to determine whether they were automatically replicated to a secondary location.	No exceptions noted.
A1.2.4	*Backup Scheduling and Off-site Storage* Data is automatically backed up on a scheduled basis and duplicated via the NetBackup tool to a secondary location.	For a sample of systems, inspected backup system documentation to determine whether data was backed up according to schedule.	No exceptions noted.
A1.2.6	*Data Backup Standard* Paychex has a documented data backup standard that defines procedures and standards for data backups and made available to employees via the Paychex intranet.	Inspected the Paychex intranet to determine whether a data backup standard was documented, made available to employees and defined procedures for data backups.	No exceptions noted.
A1.3.1	*Business Continuity Planning and Disaster Recovery Documentation and Testing* Paychex maintains Business Continuity Plans as well as Disaster Recovery plans, which are updated annually or upon significant changes. Business continuity testing is performed every 18 months using live events, or realistic simulations in order to assess risk to availability commitments as well as application RTO/RPOs. Every 18 months, disaster recovery tests including failover to alternate data centers are performed to ensure critical IT systems are tested to ensure resilience.	Inspected Business Continuity Plans and Disaster Recovery Plans to determine whether plans were reviewed and updated on an annual basis. Inspected business continuity testing documentation to determine whether testing is performed on schedule at least every 18 months using live events, or realistic simulations in order to assess risk to availability commitments as well as RTO/RPOs. Inspected disaster recovery testing documentation to determine whether testing is performed on schedule at least every 18 months and whether the testing included failover to alternate data centers to ensure the resiliency of critical IT systems.	No exceptions noted.
A1.3.2	*Business Continuity Planning and Disaster Recovery Training* The BCP team provides training via quarterly meetings for both BCP planning and DR procedure protocols. Training is provided to both promote BCP awareness and to provide specific direction for creation of BCP plans.	For a sample of quarters, inspected the BCP meeting invites and agendas to determine whether the BCP team provided training and whether the training provided awareness and direct for the creation of BCP plans and DR procedure protocols.	No exceptions noted.

Control #	Controls Specified by Paychex, Inc.	PwC LLP's Tests of Controls	Results of Tests
PI1.1.1	*Data Definitions and Mapping* Data definitions, mapping and processing specifications required to support the system are documented.	Inspected data definition, mapping, and processing specification documentation to determine whether documentation capturing requirements to support the system is maintained.	No exceptions noted.
PI1.1.2	*Design Specifications* Detailed design specifications are captured as part of the SDLC process. Development teams leverage Confluence for high level documentation and detailed acceptance criteria is captured in JIRA.	Inspected a sample of application, database, and operating system changes to determine whether design specifications were captured as part of the SDLC process within Confluence and/or JIRA.	No exceptions noted.
PI1.1.3	*Core Payroll Electronic Appointment Schedule* The application automatically removes clients from the PRS's Electronic Appointment Schedule once their payroll has been input and submitted for processing.	Inspected a sampled client within the application to determine whether Paychex clients appeared on the Service Specialist's Electronic Appointment Schedule prior to input and whether the client was removed from the Service Specialists Electronic Appointment Schedule after the client's payroll had been input and submitted for processing.	No exceptions noted.
PI1.1.4	*Employees Gross Pay and Net Pay Calculations* The applications are configured to accurately calculate employee gross pay and net pay based upon client-specified pay rates, deductions, and hours.	Reperformed the gross pay and net pay calculation for one client employee on the Core payroll and the Preview payroll processing applications to determine whether both applications accurately calculated employee gross pay and net pay based upon client specified pay rates, deductions, and hours.	No exceptions noted.
PI1.1.5	*Client Payroll Contact* All Core Payroll clients are required to have at least one defined payroll contact in the Core Payroll system prior to activation.	Observed a Service Specialist add a new client to the Core Payroll application and enter a defined payroll contact to determine whether a contact must be entered prior to the client being activated. Observed a Service Specialist add a new client to the Core Payroll application without a defined payroll contact to determine whether an error message is presented, and a contact must be entered prior to the client being activated.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.1.7	*Tax Withholding Rate* The applications are configured to accurately apply tax withholding rate information.	Reperformed the tax withholding rate information calculation for one client employee on each application to determine whether the application accurately applied tax withholding rate information.	No exceptions noted.
PI1.1.8	*Plan and Participant Account Valuations* On a daily basis, pricing information is received electronically from the trading partners and a valuation is automatically performed by the SunGard application and updates are applied completely and accurately to HRIS plan and the participant accounts.	For a sample of days and investments, inspected pricing documentation and system records to determine whether the values in HRIS agreed completely and accurately to the trading partners published price of the investment for the respective dates. For a sampled participant account, re-calculated the trading activity and account balance based on the pricing information received for that day to determine whether the SunGard application calculated the value of the trade and the account accurately using the received pricing information.	No exceptions noted.
PI1.1.9	*Plan Authorization* Prior to processing, the Adoption Agreement document is signed by an authorized party for new plans. Prior to processing, authorization is provided by an authorized party for modified plans.	For a sample of new or modified plans inspected the Adoption Agreement document to determine whether they were approved by an authorized party prior to processing.	No exceptions noted.
PI1.2.1	*Data Validation* Data input to applications and databases is validated via automated jobs to ensure that data is input complete and accurate. Issues are logged, researched, and corrected as needed.	Observed the computer operator monitoring scheduled jobs and inspected reports of success or failure and documentation of any follow-up needed to determine whether computer operators were monitoring scheduled jobs. For a sample of incidents identified by the monitoring tools, inspected supporting documents to determine whether issues were documented, reported and resolved timely.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.2.2	*Payroll Input* During payroll data input for the Core Payroll and Preview applications, edit checks verify that required fields are present and input data is accurate. Should any input fail these edit checks, the data is rejected, and an error message is displayed for the Payroll Specialist (PRS), Client Service Representative (CSR), or client entering the data to resolve. The following Core Payroll application edit checks ensure the accuracy of direct deposit information upon input: -Required reason for backdated payroll -Comment for backdated payroll The following Preview application edit checks ensure the accuracy of direct deposit information upon input: -Check date is not on the company calendar During a payroll session, each active employee is presented in a predetermined order.	Observed input screens and error messages from the Core Payroll application to determine whether edit checks were in place and error messages were displayed to require a reason and a comment for a backdated payrolls for the Payroll Specialist (PRS), Client Service Representative (CSR), or client entering the data to resolve. Observed input screens and error messages from the Preview application to determine whether edit checks were in place and error messages were displayed to restrict a check date being entered for a direct deposit that was not on the company calendar. Observed a payroll data input for the Core Payroll and Preview Applications with no errors to determine whether the system successfully processed without errors. Observed a payroll session to determine whether active employees were presented in a predetermined order.	No exceptions noted.
PI1.2.3	*Control Totals Calculation* The Core Payroll application automatically calculates control totals. The Payroll Specialist compares the control totals produced by the application to the information provided by the client to ensure the completeness and accuracy of payroll input.	Observed a Payroll Specialist input payroll data in the Core Payroll application and manually compare the control totals calculated by the application to the information provided by the client to determine whether the completeness and accuracy of the input based on the information provided by the client. For a client payroll, recalculated the control totals to determine whether control totals were accurately calculated by the Core Payroll application based on the information provided by the client.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.2.4	*Direct Deposit Edit Checks* The following Core Payroll application edit checks ensure the accuracy of direct deposit information upon input: • Confirmation of bank account number changes • Active bank relationship • Active bank account • Direct deposit allocation amounts between multiple bank accounts	Observed a Payroll Specialist receive error messages for each of the following Core Payroll application key edit checks to determine whether edit checks were implemented for accuracy of direct deposit information upon input and noted that errors must be resolved in order for the PRS to move forward in the payroll process: • Confirmation of bank account number changes • Active bank relationship • Active bank account • Direct deposit allocation amounts between multiple bank accounts Observed a direct deposit input for the Core Payroll with no errors to determine whether the system successfully processed without errors.	No exceptions noted.
PI1.2.5	*Transaction Logs – Payroll* Key payroll transactions are logged, including the date and time of the transaction and the name of the individual who initiated the transaction accurately.	Observed a staff person process a transaction on each payroll processing system to determine whether the payroll transaction, date and time of the transaction, and the name of the individual who initiated the transaction were logged accurately.	No exceptions noted.
PI1.2.6	*Client Setup* Implementation Specialists review new client information input into the application for completeness and accuracy within five business days after generating the first payroll and subsequent supporting documentation.	For a sample of new clients, inspected the supporting documents used to set up the client specifications to determine whether an Implementation Specialist reviewed client information for completeness and accuracy within five business days after generating the first payroll.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.2.7	*Edit Checks* HRIS performs edits on new plans and modifications of existing plans and participant information so that errors are identified and corrected prior to the implementation of the plan or modification.	Observed an HRS Specialist input new plans, modification to existing plans, and participant information to determine whether HRIS edit checks were in place and error messages were displayed for invalid data. Observed an HRS Specialist perform a plan setup that failed the edit checks to determine whether HRIS prevented the plan setup implementation until the HRS Specialists corrected the errors. Observed an HRS Specialist perform modifications of existing plans that failed the edit checks to determine whether HRIS prevented the plan modification implementation until the HRS Specialists corrected the errors. Observed an HRS Specialist perform a valid plan setup to determine whether HRS successfully processed the plan.	No exceptions noted.
PI1.2.8	*Cash Receipt Processing* Cash receipts (checks, wire transfers, and non-payroll ACH transactions) are recorded manually in Salesforce and HRIS is updated to process and post trades to SunGard accordingly. Contributions are recorded to participant accounts in HRIS based on the request from the participant or the instructions from the employers. Identified discrepancies are researched and corrected in a timely manner.	For a sample of cash receipts, inspected SalesForce, HRIS and SunGard records to determine whether the transaction amounts agreed to the bank statement and whether the contributions were recorded in HRIS as per the request from the participant or the instructions from the employers. If discrepancies were identified inspected evidence to determine whether they were researched and corrected in a timely manner.	No exceptions noted.
PI1.2.9	*Distributions Authorization* Distribution requests, including loans, rollovers, and lump sums, are approved by an authorized party prior to processing.	For a sample of distributions, inspected the requests to determine whether the distribution request including loans, rollovers, and lump sums were approved by an authorized party prior to being processed.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.2.10	*Automated Edit Checks* HRIS performs edit checks to verify that the plan/participant distribution requests are eligible and that the requested amount of the loan is allowed.	Observed an HRIS Specialist attempt to input a distribution request in the application to determine whether edit checks were in place to verify the eligibility of plan/participant distribution requests. Observed an HRIS Specialist attempt to process a loan dollar amount over the maximum dollar amount allowed for a participant to determine whether the system prevented the loan. Observed an HRIS Specialist attempt to process a loan over the number of loans allowed per participant to determine whether the system prevented the loan.	No exceptions noted.
PI1.2.11	*Dividend/Earnings Activity Processing* The HRS Supervisor, Team Lead, or Senior Specialist reviews a random sample of funds monthly and compares the dividend information to an external source to ensure the accuracy of the information in HRIS. The HRS Supervisor, Team Lead, or Senior Specialist signs off that the review was completed.	For a sample of months, inspected supporting documentation to determine whether the HRS Supervisor, Team Lead, or Senior Specialist reviewed a random sample of funds and compared the dividend information from HRIS to an external source for accuracy and whether they signed off evidencing that the review was completed.	No exceptions noted.
PI1.2.12	*Calculation and Posting of Dividend/Earnings* SunGard automatically calculates and posts dividend/earnings activity to participant accounts completely and accurately based on the participant accounts holding percentage.	For a sampled participant account, recalculated the dividends/earnings that were posted to the participant account to determine whether the SunGard application calculated the dividend/earnings completely and accurately based on the participant's account holding percentage.	No exceptions noted.
PI1.2.13	*Transaction Logs – Retirement Services* Retirement services transactions on SunGard and HRIS are logged, including the date, time, and name of the individual who initiated the transaction accurately.	Observed a staff person process a retirement services transaction on both SunGard and HRIS to determine whether the transaction logs accurately recorded the date, time, and name of the individual who initiated the transactions.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.1	*Data Processing* In accordance with a defined schedule, data input to applications and databases is validated via monitoring to ensure that data is processed. Failures trigger automated alerts and are investigated and resolved in a timely manner.	Inspected monitoring tools to determine whether data processing took place in accordance with a defined schedule and was monitored by management, Inspected a sample of failure alerts to determine whether alerts were investigated and resolved in a timely manner.	No exceptions noted.
PI1.3.2	*Scheduled Job Monitoring and Problem Management* Management has defined and implemented an incident management system to monitor jobs and identify, log, and resolve failed jobs (i.e., incidents, problems, and errors).	Observed the computer operator monitoring scheduled jobs and inspected reports of success or failure and documentation of any follow-up needed to determine whether computer operators were monitoring scheduled jobs. For a sample of incidents identified by the monitoring tools, inspected supporting documents to determine whether issues were identified, logged, and resolved timely.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.3	*Payroll Processing Checks* The following application payroll processing edit checks ensure the completeness and accuracy of payroll processing: • Bank account number not matching to the account number noted in the application • No direct deposit set up • Pay file code not set up • Duplicate payroll processing • Negative check amounts • Check date is not on the company calendar (confirmation that the check processing date is correct) Errors are resolved by the Computer Operators and through problem management.	Observed a Service Specialist attempt to process a payroll through the applications to determine whether checks related to payroll processing were implemented. Observed a Service Specialist receive an error message for each of the following edit checks: • Bank account number not matching to the account number noted in the application • No direct deposit set up • Pay file code not set up • Duplicate payroll processing • Negative check amounts • Check date is not on the company calendar (confirmation that the check processing date is correct) To determine whether checks related to payroll processing were implemented, and that the Service Specialist must communicate the error to the client payroll representative to resolve the error. Observed a PSR/CSR clicking off on the error message to determine whether the system did not resolve the error. Observed a payroll process with no errors to determine whether the system successfully processed the payroll.	No exceptions noted.
PI1.3.4	*Job Schedule Modification Requests* Production job schedules are maintained and updated by the Scheduling Team. Job schedule modifications are requested by appropriate personnel based on job responsibilities.	For a sample of job schedule modifications, inspected the associated request documentation to determine whether the request came from appropriate personnel, and the job modification requested was implemented.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.5	*Payroll Monitoring and Problem Management* Computer Operators monitor the servers and process incoming payrolls. The Computer Operators identify payroll processing failures and submit them to Enterprise Support, the Service Specialist, and/or the Supervisor for corrective action.	For a sample of payroll processing failures, inspected system errors and supporting documentation to determine whether payroll processing failures and the related error messages were communicated to Enterprise Support, the PRS/CSR, and/or the Supervisor for corrective action. For a sample of failures, inspected supporting documents to determine whether Computer Operators identified the failures and the failures had evidence of corrective action from Enterprise Support, the Service Specialist, and/or the Supervisor.	No exceptions noted.
PI1.3.6	*Distributions Details* Participant distributions, including loans, rollovers, and lump sums, are made completely and accurately based on the required information detailed in the distribution requests.	For a sample of distributions, inspected documentation to determine that the required distribution request was complete. For a sample of distributions, inspected documentation to determine the distribution details agreed to HRIS and the distributions were accurate.	No exceptions noted.
PI1.3.7	*Tax Withholding Rates* Compliance monitors the tax rate updates from the federal and state/territory agencies. Tax rates are manually updated in HRIS and the application is configured to accurately apply tax withholding rate information.	For a sample of states/territories, inspected HRIS and supporting documentation to determine whether compliance monitored tax rate updates from federal and state/territory agencies and whether HRIS was configured with the tax rates as per the respective state/territory agencies. For a sampled distribution, reperformed the state tax withholding rate information calculation to determine whether HRIS accurately calculated tax withholdings. For a sampled distribution, reperformed the federal tax withholding rate information calculation to determine whether HRIS accurately calculated tax withholdings.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.8	*Participant Web Transactions* Prior to the nightly trade process, fund transfers initiated through the Participant Web and not processed automatically (i.e. due to insufficient funds, self-directed brokerage accounts, etc.) are generated on the Transcompare Report reviewed by the HRS Specialist and resolved, as necessary, in a timely manner.	For a sample of days, inspected the Transcompare Report and supporting documents to determine whether all fund transfers initiated through the Participant Web but not processed automatically (i.e. due to insufficient funds, self-directed brokerage accounts, etc.) were reviewed by the HRS Specialist and resolved in a timely manner.	No exceptions noted.
PI1.3.9	*Outstanding Manual Contributions* The list of outstanding manual contributions is generated on a weekly basis and reviewed by the Client Asset Management Team for items outstanding for more than 10 days. Status updates for these items are documented and resolved.	For a sample of weeks, inspected the list of outstanding manual contributions and supporting evidence to determine whether they were reviewed, there were status updates for items outstanding for more than 10 days, and outstanding items were documented and resolved.	No exceptions noted.
PI1.3.10	*Bank Statement Reconciliations* Client Funds Accounting Specialists reconcile HRIS, the bank statement, and the General Ledger monthly, and the reconciliation is reviewed by Client Funds Accounting Management. Discrepancies identified are tracked and resolution is documented.	For a sample of months, inspected the HRIS, bank statement, and General Ledger reconciliation to determine whether the reconciliation was performed as scheduled, discrepancies were tracked, and resolution was documented.	No exceptions noted.
PI1.3.11	*Transaction Reject Report Review* The SunGard application rejects transactions based on pre-defined conditions (e.g., insufficient balance in account, discrepancy in funds data, missing/incorrect participant information) and lists the rejected transactions on the Transaction Reject Report. HRS Specialists review the Transaction Reject Report generated from SunGard and correct rejected transactions daily as necessary.	Observed a sampled insufficient balance in account, discrepancy in funds data, missing/incorrect participant transactions to determine whether the SunGard application rejected the transactions based on pre-defined conditions. For a sample of days, inspected the Transaction Reject Reports and supporting documentation from SunGard to determine whether the reports were reviewed by HRS Specialists and rejected items were corrected as necessary.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.12	*Daily Share Balance Reconciliation* Each day, the trading partners send a position file detailing the share balances they hold. Daily, the Trade Reconciliation team reconciles and investigates any discrepancies between this file and the balances in SunGard.	For a sample of days, inspected documentation to determine whether the Trade Reconciliation team reconciled the trading partner position files of share balances to balances in SunGard, discrepancies were investigated, and resolution was documented.	No exceptions noted.
PI1.3.13	*System Edit Checks* Participant investment election and salary deferral transactions are subject to the automated system edit checks: - Participant Web and HRIS prevent investment election percentages greater than and less than 100% - Participant Web and HRIS prevent salary deferral percentages greater than the amount specified by the client's plan.	Observed an HRS Specialist acting as a participant enter investment election percentages greater than and less than 100% to the Participant Web and HRIS to determine whether the system prevented an investment election percentage greater than or less than 100%. Observed an HRS Specialist acting as a participant enter salary deferral percentages greater than the amount specified by the client's plan to Participant Web and HRIS to determine whether the system prevented election salary deferral percentages greater than those allowed by the plan. Observed an HRS Specialist acting as a participant enter a salary deferral percentage equal to the amount specified in the client plan and an investment election percentage equal to 100% to Participant Web and HRIS to determine whether the system processed the salary deferral and investment election transactions.	No exceptions noted.
PI1.3.14	*Investment Elections Quality Control Review* An HRS Specialist performs a monthly quality control review on a sample of investment elections and deferral percentage changes input manually to HRIS from the enrollment form. Any discrepancies are researched and corrected in a timely manner.	For a sample of months, inspected the monthly quality control review and supporting documentation to determine whether the HR Specialist performed the quality review and whether a sample of investment elections and deferrals percentage changes input manually to HRIS were performed accurately in accordance with the enrollment form. For a sample of enrollment discrepancies identified on the quality control reviews, inspected follow-up supporting documents and/or records to determine whether they were researched and corrected in a timely manner.	No exceptions noted.

Control #	Controls Specified by Paychex, Inc.	PwC LLP's Tests of Controls	Results of Tests
PI1.3.15	*Vesting Percentage Review* HRS Specialists review the accuracy vesting percentages for a selection of clients using the Quarter End Package Verification checklists. Exceptions are documented and resolved.	For a sample of quarters, inspected the Quarter End Package Verification checklists to determine whether the vesting percentage review was conducted and whether exceptions identified were documented and resolved. For a sampled participant account for each sampled quarter, recalculated the participant's years of service/vesting credit noted in HRIS to determine whether the participant's vesting percentage was accurate based on the vesting schedule and the participant's years of service/vesting credits.	No exceptions noted.
PI1.3.16	*Loans and Distributions Processing* Loans and distribution requests are logged in HRIS accurately and processed timely. Issues identified are investigated and resolved.	For a sample of loans and distribution requests, inspected HRIS records and supporting documentation to determine whether the loans and distributions were logged accurately and paid in a timely manner or investigated as required.	No exceptions noted.
PI1.3.17	*Participant Contributions, Rollovers, Loan* Participant contributions, rollovers, loan repayments, and employer contributions are applied in HRIS based on the participants' specified election directions and percentages and/or the instructions received from the employers. Trades are posted to SunGard accordingly based on the information in HRIS.	For a sampled participant contribution, rollover, loan repayment, and employer contribution, inspected the participant / employer account records in HRIS and SunGard to determine whether they were applied and trades posted in accordance with participants' specified election directions and/or employer instructions.	No exceptions noted.
PI1.3.18	*ACH Transaction Processing* Contribution EFTs for 401(k) deductions are processed with payroll. Transmission activity is posted to HRIS with its respective effective date based on the file received from payroll. Trades are posted to SunGard accurately based on the information in HRIS and the request from the participant.	For a sample of payroll transmission, including contribution EFTs for 401(k) deductions, inspected transmission activity to determine whether the transmission was posted to HRIS with an effective date and accurately reflected the file received from payroll. Inspected a sampled trade to determine whether the trade posted to SunGard accurately in accordance with the information defined in HRIS and the request from the participant.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.19	*Plan Asset Transfer Requests* Plan asset transfers are requested by authorized personnel and processed accurately as per instructions on the Plan Asset Transfer Form.	For a sample of plan asset transfers, inspected the Plan Asset Transfer Form to determine whether the request was made by authorized personnel. For a sample of plan asset transfers, inspected the wire request and the bank statement to determine whether the plan asset transferred accurately in accordance with the Plan Asset Transfer Form.	No exceptions noted.
PI1.3.20	*Automated Participant Web Transactions* Requests from the Participant Web are automatically processed in HRIS and traded through SunGard accurately and timely.	For a request initiated through the Participant Web, inspected HRIS and SunGard system to determine whether the request was processed and recorded accurately and in a timely manner.	No exceptions noted.
PI1.3.21	*Purchase and Sale Transactions* Trade Reconciliation Specialists reconcile purchase and sale activity with the trading partners daily. Transactions that are rejected are investigated and followed up on. 401(k) trade purchase wires are prepared by a Trade Reconciliation Specialist, approved and released by Treasury Specialist. For trading partners that net daily purchase and sale transactions, a net wire may be received by Paychex and is agreed to the daily bank statement.	For a sample of days and trading partners, inspected the purchase and sale reconciliation to determine whether the transactions received by the trading partner were reconciled to the transactions sent by Paychex. For a sample of days and trading partners, obtained the daily reconciliations and, for a selection of rejected trades, inspected supporting documents to determine whether the rejected trades were investigated and followed up on. For a sample of days and trading partners, inspected supporting documents to determine whether the 401(k) trade purchase wires were prepared by a Trade Reconciliation Specialist, approved and released by a Treasury Specialist. For a sample of days and trading partners that net daily purchase and sale transactions where a net wire was received by Paychex, inspected the daily bank statement to determine whether the wire amount received was accurate.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.3.22	*Terminated Participant Distribution* When a terminated participant takes a distribution, all forfeitures (non-vested funds) are automatically calculated accurately based on the plan provisions and participant vesting, and applied to the client's account timely where they can be allocated to eligible employees or used to offset plan expenses.	For a sample of terminated participant forfeitures, inspected client and participant level accounts to determine whether the non-vested portion of the employer contributions were calculated accurately as per the plan documentation and applied to the client account timely.	No exceptions noted.
PI1.3.23	*Monthly Share Balance Reconciliation* A formal reconciliation report is produced for the last day of each month, noting the outstanding discrepancies as of that day. This monthly report is signed off by the Trade Reconciliation Specialist and the Trade Reconciliation Supervisor.	For a sample of months, inspected the reconciliation report to determine whether it was signed off by a Trade Reconciliation Specialist and a Trade Reconciliation Supervisor, outstanding discrepancies were investigated, and resolution was documented.	No exceptions noted.
PI1.4.1	*Check Stock* The Company uses check stock that incorporates security features.	Inspected the design of the check stock used by Paychex to determine whether security features were incorporated.	No exceptions noted.
PI1.4.2	*Distribution of Payroll Packages* Paychex personnel use courier logs or pickup/delivery logs and manifests to monitor and control the distribution of payroll packages. Payroll packages are distributed in accordance with client specifications.	For a sample of days and payrolls, inspected the courier or pickup/delivery logs and manifests to determine whether they were used to monitor and manage the distribution of payroll packages and whether packages were distributed in accordance with client specifications.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.4.3	*Payroll Checks and Standard Reports* The Core Payroll and Preview applications are configured to produce the following standard output reports using the client payroll input. Core Payroll: • Department Summary • Payroll Journal Preview: • Payroll Register • Payroll Tax Report • Payroll Taxable Wages	Observed the configuration and generation of the standard output reports produced to determine whether the Core Payroll and Preview applications were configured to produce the standard output reports completely and accurately. For the following key reports, inspected the system details and compared to the report to determine whether the Core Payroll and Preview applications generated the reports completely and accurately. • Core Payroll: • Department Summary • Payroll Journal Preview: • Payroll Register • Payroll Tax Report • Payroll Taxable Wages	No exceptions noted.
PI1.4.4	*Client and Participant Statement Review* Samples of client and participant statements are reviewed quarterly by HRS Specialists for completeness and accuracy. Exceptions are documented and resolved in a timely manner.	For a sample of clients, participants, and quarters, inspected the checklists and supporting documentation to determine the HRS Specialists reviewed a sample of statements for completeness and accuracy. If exceptions were identified inspected to determine whether they were documented and resolved in a timely manner.	No exceptions noted.
PI1.4.5	*Statement Files* The HRIS application is configured to produce statement files completely and accurately using client and participant information stored in the application.	Inspected the HRIS application configuration and generation of the statement file to determine whether the HRIS application produced the statement file with complete and accurate client and participant information stored in the application.	No exceptions noted.

Control #	*Controls Specified by Paychex, Inc.*	*PwC LLP's Tests of Controls*	*Results of Tests*
PI1.4.6	*Confirmations for Online Transactions* HRIS provides complete and accurate confirmation details to the participant after submitting a transaction online through the Participant Web.	Observed an HRS Specialist acting as a participant attempt to process a transaction using the Participant Web to determine whether HRIS presented the participant with complete and accurate transaction details in an online confirmation screen.	No exceptions noted.
PI1.4.7	*Reconciliation of Vendor Invoices and Associated Statement Files* On a quarterly basis, HRS Specialists reconcile the number of client level statements printed between the vendor invoices and the associated client statement files in HRIS. Discrepancies identified are researched and resolved in a timely manner.	For a sample of quarters, inspected the vendor invoices received and associated client statement files in HRIS to determine whether the number of client level statements printed agreed and was reconciled by HRS Specialists. If discrepancies were identified inspected evidence to determine whether they were researched and resolved timely.	No exceptions noted.

SECTION V

Other Information Provided by Paychex, Inc. That is Not Covered by the Service Auditors' Report

Management's Response to Testing Exceptions

Criteria	Control	Exception	Management Response
CC3.2 CC3.4 CC9.2	CC9.2.4: Initial vendor risk assessments are performed for vendors that have access to confidential data or could impact the service of the system and are documented within the third party vendor management system. The vendor risk assessment evaluates criticality (business critical, key vendor, or non-key) and the type of data being impacted in order to establish a risk score – minor, low, high, critical. Annual tiering re-assessments are sent to the vendor relationship manager to confirm that the nature and scope of the data has not changed. If the scope has changed or the vendor is deemed "Key/Business Critical", a full vendor re-assessment will be performed.	Exceptions noted, management was unable to provide evidence that new vendor and annual re-assessments were performed.	Paychex was in process of migrating the third-party management tool during the timeframe of this Audit which impacted the ability to review all evidence and resulted in the notation under CC9.2.4. All high tier vendors have been reviewed from intendent security score vendors along with the history of any breaches to ensure coverage was maintained.

Privacy Statement

Paychex is committed to providing cost-effective payroll, payroll tax preparation, human resources, and employee benefits for any size business. In an effort to meet that commitment, clients may have to provide Paychex with business, financial, and/or personal information about the client and their employees. Their privacy and the privacy of the information provided are extremely important to Paychex. Paychex protects the security of the client's business, financial, and personal information. Paychex uses reasonable care to protect data from loss, misuse, unauthorized access, disclosure, alteration, and untimely destruction. Paychex grants access to personal client information only to its employees, agents, and service providers so they can provide products or services, process and service client accounts, administer their business, offer additional services, perform analysis to determine qualification to receive future services, or collect amounts due.

Additionally, Paychex does not sell or disseminate client information to any third parties under any circumstances, except to fulfill legal and regulatory requirements and to facilitate client-requested transactions.

This report is intended solely for use by the management of Paychex, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.