SOC 1® Report on the Suitability of the Design and Operating Effectiveness of Controls

Description of ADP's Workforce Now Services System for the period April 1, 2019 to March 31, 2020

Always Designing for People™

Table of Contents

SECTION ONE **PAGE**

Independent Service Auditor's Report provided by Ernst & Young

SECTION TWO

Management Assertion

SECTION THREE

Description of ADP's Workforce Now Services System for the period April 1, 2019 to March 31, 2020

SECTION FOUR

Description of Control Objectives, Controls, Tests, and Results of Tests

SECTION FIVE

Other Information Provided by ADP

SECTION ONE

INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY ERNST & YOUNG

Ernst & Young LLP
200 Clarendon Street
Boston, MA 02116

Tel: +1 617 266 2000
Fax: +1 617 266 5843
ey.com

INDEPENDENT SERVICE AUDITOR'S REPORT

Management of Automatic Data Processing, Inc.

Scope

We have examined Automatic Data Processing, Inc.'s (ADP) description entitled "Description of ADP's Workforce Now Services System for the period April 1, 2019 to March 31, 2020" (Description) of its Workforce Now Services System (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in "ADP Management Assertion" (Assertion). The Control Objectives and controls included in the Description are those that management of ADP believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

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

ADP utilizes its Global Enterprise Technology & Solutions (GETS) US organization as a subservice organization to provide certain hosting operations, data center management, and network management services to support ADP's Workforce Now Services System. The Description includes only the Control Objectives and related controls of Workforce Now Services System and excludes the control objectives and related controls of the subservice organization.

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

The information included in Other Information Provided by ADP is presented by management of ADP to provide additional information and is not a part of ADP's Description. Information about ADP's Global Business Resiliency Program, its Global Security Organization and Prior Period Mapping have not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives and, accordingly, we express no opinion on it.

ADP's responsibilities
ADP has provided the accompanying assertion titled, ADP Management Assertion (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. ADP is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, 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, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period April 1, 2019 to March 31, 2020. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion.
- assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

Inherent limitations
The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation

of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying Description of Control Objectives, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion
In our opinion, in all material respects, based on the criteria described in ADP's Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period April 1, 2019 to March 31, 2020.
b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period April 1, 2019 to March 31, 2020 and if subservice organizations and user entities applied the complementary controls assumed in the design of ADP's controls throughout the period April 1, 2019 to March 31, 2020.
c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period April 1, 2019 to March 31, 2020, if complementary subservice organization and user entity controls assumed in the design of ADP's controls operated effectively throughout the period April 1, 2019 to March 31, 2020.

Restricted use
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of ADP, user entities of ADP's System during some or all of the period April 1, 2019 to March 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

June 29, 2020

SECTION TWO

MANAGEMENT ASSERTION

ADP MANAGEMENT ASSERTION

June 29, 2020

We have prepared the description of Automatic Data Processing, Inc.'s (ADP) Workforce Now Services System entitled, "Description of ADP's Workforce Now Services System for the period April 1, 2019 to March 31, 2020" (Description) for processing user entities' transactions throughout the period April 1, 2019 to March 31, 2020 for user entities of the system during some or all of the period April 1, 2019 to March 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

ADP utilizes its Global Enterprise Technology & Solutions (GETS) US organization as a subservice organization to provide certain hosting operations, data center management, and network management services to support its Workforce Now Services System. The Description includes only the control objectives and related controls of ADP and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

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

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

a. The Description fairly presents ADP's Workforce Now Services System (System) made available to user entities of the System during some or all of the period April 1, 2019 to March 31, 2020 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities of the System was designed and implemented to process relevant transactions, including, if applicable:

- the types of services provided, including, as appropriate, the classes of transactions processed;

- the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System;
- the information used in the performance of the procedures including, if applicable, related accounting records whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing and reporting transactions this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities;
- how the System captures and addresses significant events and conditions, other than transactions;
- the process used to prepare reports and other information for user entities;
- services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
- the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls; and
- other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring activities that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) Includes relevant details of changes to the System during the period covered by the Description.

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

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period April 1, 2019 to March 31, 2020 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of ADP's controls throughout the period April 1, 2019 to March 31, 2020. The criteria we used in making this assertion were that:

(1) the risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization;

(2) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

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

Automatic Data Processing, Inc.

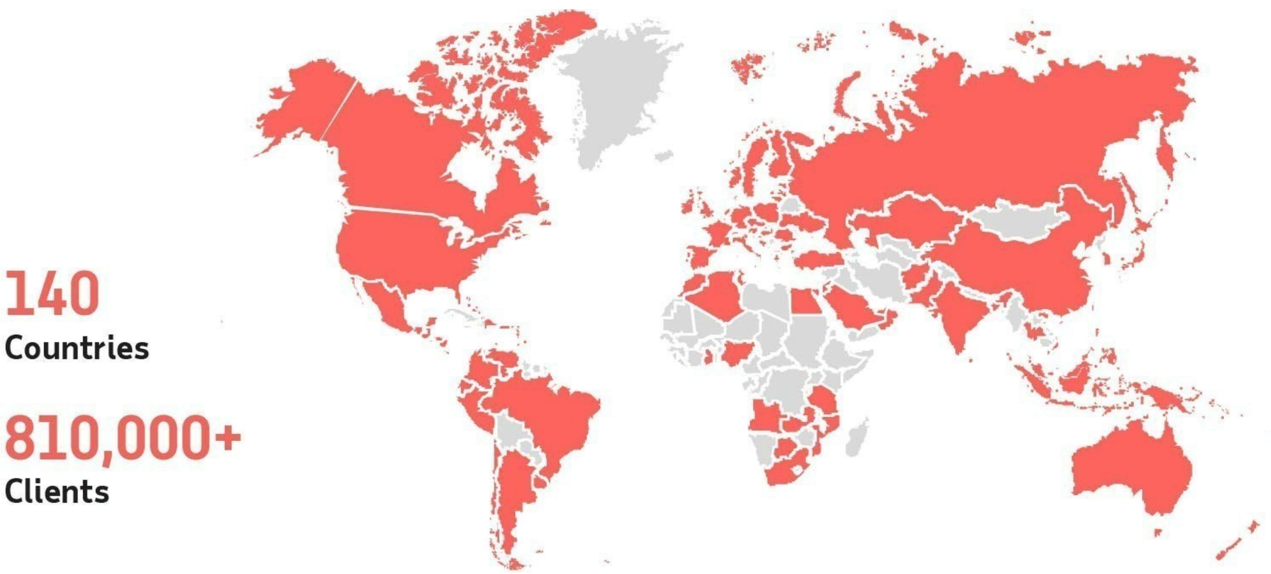
SECTION THREE

DESCRIPTION OF ADP'S WORKFORCE NOW SERVICES SYSTEM FOR THE PERIOD APRIL 1, 2019 TO MARCH 31, 2020

OVERVIEW OF OPERATIONS

General

ADP® was founded in 1949 on an innovative idea: to help business owners focus on core business activities by relieving them of certain non-core tasks such as payroll. Today ADP is one of the world's leading providers of cloud-based human capital management (HCM) solutions to employers, offering solutions to businesses of different sizes, whether they have simple or complex needs, and serves more than 810,000 clients in more than 140 countries and territories.



Business Overview

ADP's Mission

ADP's mission is to power organizations with insightful solutions that meet the changing needs of its clients and their employees. ADP's technology, industry and compliance expertise and data insights deliver measurable results, peace-of-mind and an enabled, productive workforce. ADP's leading technology and commitment to service excellence is at the core of its relationship with each one of its clients, whether it's a small, mid-sized or large organization operating in one or multiple countries around the world. ADP is constantly designing better ways to work through products, services and experiences.

ADP's Strategy - Strategic Pillars

ADP's business strategy is based on three strategic pillars, which are designed to position ADP as a global market leader in HCM technology and services:

HCM Solutions

Grow a complete suite of cloud-based HCM solutions - ADP develops cloud-based software and offers comprehensive solutions that assist employers in managing the entire worker spectrum and employment cycle - from full-time to freelancer and from hire to retire.

HRO Solutions

Grow and scale ADP's market-leading HR Outsourcing (HRO) solutions - ADP offers comprehensive HRO solutions in which it provides complete management solutions for HR administration, payroll administration, talent management, employee benefits, benefits administration, employer liability management, and other HCM and employee benefits functions.

Global Solutions

Leverage ADP's global presence to offer clients HCM solutions wherever they do business - ADP is expanding its international HCM and HRO businesses, comprised of ADP's established local, in-country software solutions and market-leading, cloud-based multi-country solution.

With a large and growing addressable market, ADP is strongly positioned to continue delivering sustainable long-term value across its strategic pillars. ADP does this by executing on product and technology innovation, providing industry-leading service and compliance expertise, and enhancing its distribution. ADP is focused on, and investing in, its next-gen platforms that are built for the future of work, and on providing market-leading product and technology solutions that solve the needs of its clients today, and anticipate the needs of its clients tomorrow.

ADP's platforms and multi-national solutions provide its clients with comprehensive HR and payroll capabilities that drive productivity and help enable compliance globally. ADP's cloud-based next-gen platforms are built to be person-centric, serve various worker types and support flexible work and on-demand pay, and to deliver global capabilities to dynamic, team-based organizations.

Digital technology is transforming today's workplace and workforce. ADP is accelerating its own digital transformation and leveraging digital technology to change how it engages with its clients and how their workers engage with ADP - and an important part of this includes delivering solutions wherever they are, whether at work or on the go. ADP offers a suite of complete HRO solutions coupled with dedicated and strategic HR services and local expertise.

These offerings can be tailored to meet the increasingly complex and sophisticated needs of ADP's clients and their workers. With its global footprint in the HCM industry together with its technology and deep in-country compliance expertise, ADP is positioned to continue to drive growth by delivering solutions to clients of different sizes wherever they do business.

Business Segments

ADP's two business segments are Employer Services and Professional Employer Organization Services:

Employer Services (ES) - ADP's Employer Services segment serves clients ranging from single-employee small businesses to large enterprises with tens of thousands of employees around the world, offering a comprehensive range of technology-based HCM solutions, including ADP's strategic, cloud-based platforms, and HRO (other than Professional Employer Organization) solutions. These solutions address critical client needs and include: Payroll Services, Benefits Administration, Talent Management, HR Management, Workforce Management, Compliance Services, Insurance Services and Retirement Services.

Professional Employer Organization (PEO) Services - ADP's PEO business, called ADP TotalSource®, provides clients with comprehensive employment administration outsourcing solutions through a relationship in which employees who work for a client (referred to as "worksite employees") are co-employed by ADP and the client.

ADP's Business Segments are based on the way that management reviews the performance of, and makes decisions about, its business. ADP's strategic pillars represent the strategic growth areas for its business. The results of ADP's business related to products and solutions within the HCM Solutions pillar, the HRO Solutions pillar (other than PEO products and solutions) and the Global Solutions pillar are contained within its Employer Services segment. The results of ADP's business within the HRO Solutions pillar related to its PEO products and solutions are contained within ADP's PEO Segment.

Products and Solutions

To serve the unique needs of diverse types of businesses and workforce models, ADP provides a range of solutions which businesses of different types, sizes, and across geographies can use to recruit, pay, manage, and retain their workforce. ADP addresses these broad market needs with its cloud-based strategic platforms: RUN Powered by ADP®, serving over 640,000 small businesses; ADP Workforce Now®, serving over 70,000 mid-sized and large businesses across ADP's strategic pillars; and ADP Vantage HCM®, serving over 500 large enterprise businesses. Each of these solutions can be combined with ADP SmartCompliance® to address the increasingly broad and complex needs of employers. Outside the United States, ADP addresses the needs of approximately 65,000 clients with premier global solutions consisting of local in-country solutions and multinational offerings, including ADP GlobalView®, ADP Celergo® and ADP Streamline®.

Through its acquisition of WorkMarket, a cloud-based workforce management solution, ADP helps enable clients manage their extended workforce through freelancer management functionality and reporting insights.

Wisely by ADP® is its latest advancement in the future of pay. ADP's payment offerings support an employer's need for flexible payment solutions to meet the individual needs of its workers. The Wisely Pay by ADP™ payroll card is a network-branded payroll card and digital account that helps enable employers to pay their employees, and helps enable employees to access their payroll funds immediately, including via a network member bank or an ATM, make purchases or pay bills, load additional funds onto the card, such as tax refunds and military pensions, and transfer funds to a bank account in the United States.

ADP also launched Wisely Direct by ADP®, a network-branded general purpose reloadable card and digital account, which provides similar features and functionality as Wisely Pay by ADP but is offered directly to consumers. ADP's digital card offerings are banking alternatives that feature services such as savings, budgeting, digital wallet and other personal financial management features. With Wisely by ADP, ADP received the "Awesome New Tech" award at the 2018 HR Technology Conference for a fourth straight year.

In addition, ADP's mobile apps simplify how work gets done by helping to enable clients to process their payroll, and giving millions of their employees' convenient access to their payroll and HR information around the world and in 29 languages. ADP has also opened access for developers and system integrators to some of its platforms' application programming interface libraries through ADP Marketplace.

With ADP Marketplace, clients can integrate employee data from ADP's core services across their other business systems or platforms. This access enables the exchange of client data housed in our databases, and creates a unified HCM ecosystem for clients informed by a single, comprehensive repository of their workforce data. Clients can choose from over 370 apps and integrations, allowing them to choose solutions that are tailored to their needs, industry requirements and preferences.

HCM Solutions

<u>Integrated HCM Solutions</u> - ADP's premier suite of HCM products offers complete solutions that assist employers of different types and sizes in every stage of the employment cycle, from recruitment to retirement. ADP's suite of HCM solutions are powered by its strategic, cloud-based platforms:

- RUN Powered by ADP combines a software platform for managing small business payroll, HR management and tax compliance administration, with 24/7 service and support from its team of small business experts. RUN Powered by ADP also integrates with other ADP solutions, such as workforce management, workers' compensation insurance premium payment plans, and retirement plan administration systems.

- ADP Workforce Now is a flexible HCM solution used across mid-sized and large businesses in North America to manage their employees.

- ADP Vantage HCM is a solution for large enterprises in the United States. It offers a comprehensive set of HCM capabilities within a single solution that unifies the five major areas of HCM: HR management, benefits administration, payroll services, time and attendance management, and talent management.

Payroll Services - ADP pays approximately 26 million (approximately 1 out of every 6) workers in the United States. ADP provides flexible payroll services to employers of different sizes, including the preparation of employee paychecks, pay statements, supporting journals, summaries, and management reports. ADP provides employers with a wide range of payroll options, including using mobile technology, connecting their major enterprise resource planning (ERP) applications with ADP's payroll services or outsourcing their entire payroll process to ADP. Employers can choose a variety of payroll payment options including ADP's electronic wage payment and, in the United States, payroll card solutions and digital accounts. On behalf of ADP's clients in the United States, ADP prepares and files federal, state and local payroll tax returns and quarterly and annual Social Security, Medicare, and federal, state and local income tax withholding reports.

Benefits Administration - In the United States, ADP provides powerful and agile solutions for employee benefits administration. These options include health and welfare administration, leave administration services, insurance carrier enrollment services, employee communication services, and dependent verification services. In addition, ADP benefits administration solutions offer employers a simple and flexible cloud-based eligibility and enrollment system that provides their employees with tools, communications, and other resources they need to understand their benefits options and make informed choices.

Talent Management - ADP's Talent Management solutions simplify and improve the talent acquisition, management, and activation process from recruitment to ongoing employee engagement and development. Employers can also outsource their internal recruitment function to ADP. ADP's solutions provide performance, learning, succession and compensation management tools that help employers align goals to outcomes, and enable managers to identify and mitigate potential retention risks. ADP's talent activation solutions include ADP's StandOut® and Compass® solutions, which provide team leaders with data and insights to drive employee engagement and leadership development, which in turn help drive employee performance.

Workforce Management - ADP's Workforce Management offers a range of solutions to over 75,000 employers of all sizes, including time and attendance, absence management and scheduling tools. Time and attendance solutions include time capture via online timesheets, timeclocks with badge readers, biometrics and touch-screens, telephone/interactive voice response, and mobile smartphones and tablets. These tools automate the calculation and reporting of hours worked, helping employers prepare payroll, control costs and overtime, and manage compliance with wage and hour regulations. Absence management tools include accrued time off, attendance policy and leave case modules. ADP's employee scheduling tools simplify visibility, offer shift-swapping capabilities and can assist managers with optimizing schedules to boost productivity and minimize under- and over-staffing. ADP also offers analytics and reporting tools that provide clients with insights, benchmarks and performance metrics so they can better manage their workforce. In addition, industry-specific modules are available for labor forecasting, budgeting, activity and task management, grant and project tracking, and tips management.

Human Resources Management - Commonly referred to as Human Resource Information Systems, ADP's Human Resources Management Solutions provide employers with a single system of record to support the entry, validation, maintenance, and reporting of data required for effective HR management, including employee names, addresses, job types, salary grades, employment history, and educational background.

Insurance Services - ADP's Insurance Services business, in conjunction with its licensed insurance agency, Automatic Data Processing Insurance Agency, Inc., facilitates access in the United States to workers' compensation and group health insurance for small and mid-sized clients through a variety of insurance carriers. ADP's automated Pay-by-Pay® premium payment program calculates and collects workers' compensation premium payments each pay period, simplifying this task for employers.

Retirement Services - ADP Retirement Services helps employers in the United States administer various types of retirement plans, such as traditional and Roth 401(k)s, profit sharing (including new comparability), SIMPLE and SEP IRAs, and executive deferred compensation plans. ADP Retirement Services offers a full service 401(k) plan program which provides recordkeeping and administrative services, combined with an investment platform offered through ADP Broker-Dealer, Inc. that gives its clients' employees access to a wide range of non-proprietary investment options and online tools to monitor the performance of their investments. In addition, ADP Retirement Services offers investment management services to retirement plans through ADP Strategic Plan Services, LLC, a registered investment adviser under the Investment Advisers Act of 1940. ADP Retirement Services also offers trustee services through a third party.

Compliance Solutions - ADP's Compliance Solutions provides industry-leading expertise in payment compliance and employment-related tax matters that complement the payroll, HR and ERP systems of its clients:

- ADP SmartCompliance - In the United States, ADP SmartCompliance integrates client data delivered from its integrated HCM platforms or third party payroll, HR and financial systems into a single, cloud-based solution. ADP's specialized teams use the data to work with clients to help them manage changing and complex regulatory landscapes and improve business processes. ADP SmartCompliance includes HCM-related compliance solutions such as Employment Tax and Wage Payments, as well as Tax Credits, Health Compliance, Wage Garnishments, Employment Verifications, Unemployment Claims and W-2 Management.

- ADP SmartCompliance Employment Tax - As part of its full service employment tax services in the United States, ADP prepares and files employment tax returns on its clients' behalf and, in connection with these stand-alone services, collects employment taxes from clients and remits these taxes to more than 7,100 federal, state and local tax agencies. In its fiscal year ended June 30, 2019, in the United States, ADP processed and delivered approximately 67 million employee year-end tax statements, and moved more than $2.1 trillion in client funds to taxing and other agencies and to its clients' employees and other payees.

- ADP SmartCompliance Wage Payments - In the United States, ADP offer compliant pay solutions for today's workforce, including electronic payroll disbursement options such as payroll cards, digital accounts and direct deposit, as well as traditional payroll checks, which can be integrated with clients' ERP and payroll systems.

HRO Solutions

As a leader in the growing HR Outsourcing market, ADP partners with its clients to offer a full range of seamless technology and service solutions for HR administration, workforce management, payroll services, benefits administration and talent management. From small businesses to enterprises with thousands of employees, with HRO, ADP's clients gain proven technology and processes and service and support. Whether a client chooses ADP's PEO or other HR Outsourcing solutions, it offers solutions tailored to a client's specific needs and preferences - designed to meet the client's needs today, and as its business and needs evolve.

Professional Employer Organization - ADP TotalSource, ADP's PEO business, offers small and mid-sized businesses a comprehensive HR outsourcing solution through a co-employment model. With a PEO, both ADP and the client have a co-employment relationship with the client's employees. ADP assumes certain employer responsibilities such as payroll processing and tax filings, and the client maintains control of its business and management responsibilities. ADP TotalSource clients are able to offer their employees services and benefits on par with those of much larger enterprises, without the need to staff an enterprise-size HR department. With its cloud-based HCM software at the core, ADP serves more than 12,500 clients and approximately 562,000 worksite employees in the 50 U.S. states. ADP TotalSource is one of the largest PEOs certified by the Internal Revenue Service as meeting the requirements to operate as a Certified Professional Employer Organization under the Internal Revenue Code.

As a full service PEO, ADP TotalSource provides complete HR management and core administrative services while the client continues to direct the day-to-day job-related duties of the employees. With constantly changing business regulations, global economies and technology, ADP's clients benefit from partnering with ADP

TotalSource to help them protect their business and drive growth and success. Some of the offerings available through ADP TotalSource to address today's workplace challenges include:

- Better Benefits: Through its PEO, many of ADP's clients discover that they can offer a richer overall benefits package than they could afford to offer on their own. ADP gives clients access to a new patent-pending approach to help them target the best benefit plan offerings for their employees. They can compare plan options and make more educated decisions about what plan offering is best for their company and budget. In addition, ADP TotalSource integrates with ADP Marketplace to further tailor offerings, such as helping employees pay off student loans with payroll contributions and integrating a client's U.S. PEO population with its global workforce's HR system of record.

- Protection and Compliance: ADP TotalSource HR experts help clients manage the risks of being an employer by advising how to handle properly a range of issues - from HR and safety compliance to employee-relations. This includes access to workers' compensation coverage and expertise designed to help them handle both routine and unexpected incidents, including discrimination and harassment claims.

- Talent Engagement: Featuring a talent blueprint, ADP TotalSource HR experts work with clients to help them better engage and retain their workforce through solutions that support the core needs of an employee at work. In addition, ADP's full service recruitment team is dedicated to helping its clients find and hire new talent, while reducing the stress of uncovering top talent.

- Expertise: Each client is assigned a designated HR specialist for day-to-day and strategic guidance. Clients can also access data-driven benchmarks in areas such as turnover and overtime, staffing and understanding profit leaks, and have their ADP HR expert help tailor recommendations to continue to drive their business forward.

<u>ADP Comprehensive Services</u> - Leveraging its market-leading ADP Workforce Now platform, ADP Comprehensive Services partners with clients of different types and sizes to tackle their HR, talent, benefits administration and pay challenges with help from ADP's expertise, experience and best practices. ADP Comprehensive Services is flexible – helping to enable clients to partner with ADP for managed services for one, some or all areas across HR, talent, benefits administration and pay. ADP provides outsourced execution that combines processes, technology and a service and support team that acts as an extension of its client's in-house resources - so their HCM and pay operations are executed with confidence.

<u>ADP Comprehensive Outsourcing Services (ADP COS)</u> - Enabled by ADP Vantage HCM, ADP COS is designed for large business outsourcing for payroll, HR administration, workforce management, benefits administration and talent management. With COS, the day-to-day payroll process becomes ADP's responsibility, freeing up clients to address critical issues like employee engagement and retention. The combination of technology, expertise and data-driven insights that COS offers allows clients to focus on strategy and results.

ADP Recruitment Process Outsourcing Services (ADP RPO) - ADP RPO provides talent insights to help drive targeted recruitment strategies for attracting top talent. With global, customizable recruitment services, ADP RPO enables organizations to find and hire the best candidates for hourly, professional or executive positions. In addition, ADP delivers market analytics, sourcing strategies, candidate screening, selection and on-boarding solutions to help organizations connect their talent strategy to their business's priorities.

Global Solutions

ADP's global solutions consist of multi-country and local in-country solutions for employers of any type or size. ADP partners with clients to help them navigate the most complex HR and payroll scenarios using tailored and scalable technology supported by its compliance expertise.

ADP Global Payroll is a solution for multinational organizations of any size. As a highly scalable and flexible suite of products supported by a team of experts, ADP Global Payroll allows small and mid-sized companies, as well as the largest multinationals, to standardize their HCM strategies globally (including payroll, HR, talent, time and labor, and benefits management) and adapt to changing local needs, while helping to drive overall organizational agility and engagement.

ADP also offers comprehensive HCM solutions on local, country-specific platforms. These suites of services offer various combinations of payroll services, HR management, time and attendance management, talent management and benefits management, depending on the country in which the solution is provided. ADP pays approximately 15 million workers outside the United States with its local in-country solutions and with ADP GlobalView, ADP Celergo and ADP Streamline – ADP's multi-country payroll solutions.

As part of its global payroll services, ADP supply year-end regulatory and legislative tax statements and other forms to its clients' employees. ADP's global talent management solutions elevate the employee experience, from recruitment to ongoing employee engagement and development. ADP's configurable, automated time and attendance tools help global clients understand the work being performed and the resources being used, and help ensure the right people are in the right place at the right time.

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

CONTROL ENVIRONMENT

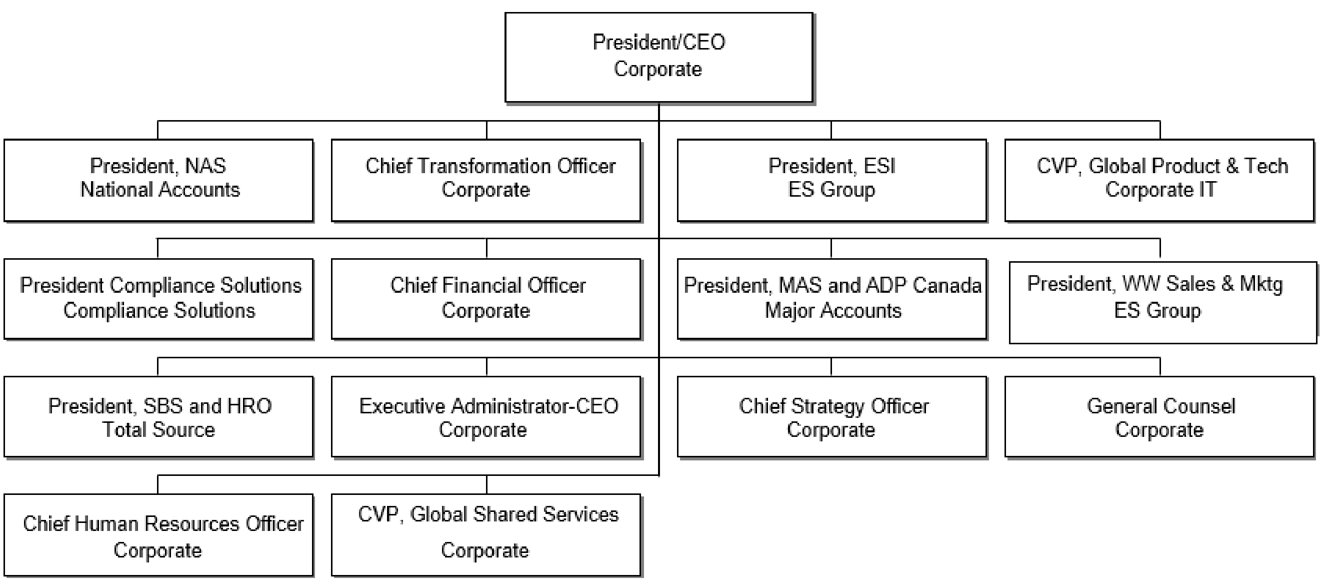
ADP's control environment reflects the position taken by the management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. Management takes seriously defects identified in internal and/or external audit reports and takes responsibility for remediation activities. The following is a description of the key elements of ADP's control environment related to supporting the services described in this Description.

Oversight by ADP's Board of Directors

ADP's Board of Directors has the ultimate responsibility for overseeing the business policies of ADP. The Board of Directors, composed of internal and external business executives, meets at least once per quarter to discuss matters pertinent to ADP's operations and to review financial results. The Board of Director's Audit Committee, composed of four independent directors, meets quarterly, and is responsible for reviewing: ADP's financial results, results of the audits of the independent external auditor, findings and recommendations identified as a result of internal and external audits; and major litigation.

Organizational Structure

Corporate Structure



Other ADP Corporate Supporting Groups

Global Product & Technology - ADP's Global Product & Technology team is divided into functional organizations to meet the technical needs of ADP's business units. All business units are supported by Global Product & Technology in some capacity, and the organization is responsible for hosting operations; data center management, and network management services that are common to ADP systems and services (common services). They are also responsible for the security administration of the network at ADP's Corporate Headquarters in New Jersey, various data centers, and Regional Business Unit locations and supporting/managing the logical and remote access to ADP's WAN and Corporate Network (ESNet).

ADP Global Security Organization - ADP's Global Security Organization (GSO) is responsible for developing and maintaining security policies and standards across the enterprise. The GSO has several vertical segments including Client Security Management Office (CSMO), Global Privacy & Risk Management Office, Converged Security Services Office, Technical Security Services, Business Security Office (BSO) Money Movement/Payroll, and BSO International. Policies are maintained on an intranet site available to all associates. Additionally, upon commencement of employment and annually, associates are required to review and acknowledge key corporate policies, including Information Security Responsibilities. Associates receive mandatory interactive training on specific security topics. During the current fiscal year, all associates worldwide receive privacy training. The GSO's activities are overseen by the Executive Security Committee, composed of the Chief Security Officer, the Chief Executive Officer, the Chief Financial Officer, the Chief Information Officer, and the General Counsel.

Human Resources Policies and Practices

Controls have been implemented covering critical employment aspects including: hiring, training and development, performance appraisals, advancement, and termination. Upon being hired, new employees are issued an employee packet documenting various procedural and administrative matters that is discussed during the new-hire orientation program.

The HR department is primarily responsible for recruiting and evaluating job applicants. Based on the sensitivity of the underlying job, various levels of background checks are performed on applicants prior to or following their employment. HR policies and procedures are posted on ADP's Intranet. These policies include, but are not limited to:

- Employment
- Equal Employment Opportunity
- Code of Corporate Responsibility
- Ethical Standards
- Honesty and Fair Dealing
- Conflicts of Interest

- Disclosure, Use, and Copying of ADP and Third Party Software
- Harassment
- Substance Abuse
- Confidentiality of Information
- Electronic Communication Systems
- Corrective Actions

ADP's core values are posted on ADP's Corporate Intranet and include Integrity is Everything, Service Excellence, Inspiring Innovation, Each Person Counts, Results Driven, and Social Responsibility. In-depth explanations of these values are available to all personnel and a user awareness program is in place to familiarize employees with these core values. All associates are required to participate in the new hire orientation program and contain information about ADP's general operating practices, policies and procedures, and assists employees in becoming acclimated to ADP's business philosophy. The orientation activities assist new associates in understanding ADP's overall mission and core values, departmental operation practices, and individual performance objectives.

ADP has a formal "Code of Conduct" that all employees must read and acknowledge as part of their new employee orientation. In addition, associates are required to disclose any previously unreported circumstances or events known by the employee that appear to be in violation of this Code. ADP provides communication channels for associates to report violations of policies and unethical behavior, including a third party administered ethics hotline. This Code of Conduct serves as an ethical guide for all directors, officers, and employees of ADP. This policy covers areas of business conduct and ethics when working with clients, suppliers, the public and other employees, and conflicts of interest that could arise between each associate's personal conduct and their positions with ADP. Associates who violate ADP's ethical standards and security policies are subject to progressive discipline, up to and including termination.

The HR Department coordinates yearly performance reviews and compensation adjustments in addition to setting hiring salary levels. Written employee position descriptions are maintained on file and are reviewed annually and revised, as necessary, by department managers. Employees are allowed an annual leave allowance based upon years of service. Each employee's manager must approve vacation time.

ADP has a written policy that deals with voluntary and involuntary employee terminations. Exit interviews are conducted and company property is collected. Procedures have been implemented for collecting company materials, deactivating card keys, and revoking physical and logical security access. Security or facilities personnel escort terminated employees out of the facility.

Corporate Internal Audit Function

The Corporate Internal Audit department is led from ADP's Corporate Headquarters in New Jersey, United States and has personnel located in Europe. Corporate Internal Audit employs financial, operational and information systems audit specialists. The department has an unlimited scope of operations and is responsible for auditing ADP globally. In addition to performing risk-based audits, the Corporate Internal Audit department performs a stand-alone Fraud Risk Assessment on an annual basis. Potential fraud risks are also incorporated into each audit that the department performs. The Corporate Internal Audit department reports to ADP's Audit Committee and administratively to the Chief Financial Officer.

RISK ASSESSMENT

Enterprise Risk Management Process

ADP's Corporate Internal Audit department conducts an annual risk assessment of ADP's business units. The model ranks each business unit based on the level of inherent risk and other elements associated with a unit's activity, and considers both internal and external risk factors. The annual audit plan is based on the risk assessment's results. The risk assessment's results become the basis for updates to the Critical Risk Profile (Profile). The Profile is validated annually as part of the Corporate Internal Audit department's risk assessment exercise and also as new risks emerge. This Profile is the inventory of risks applicable to the organization. It is used to categorize, communicate, and monitor these risks. Areas of focus include: Strategic Risk, Operational Risk, Compliance Risk, Information Technology Risk, and Financial Reporting Risk. The ADP Board of Directors reviews and approves the Profile and the risk assessment results annually and, along with its subcommittees, have risk oversight responsibilities that are executed in conjunction with their respective charters.

MONITORING

The Board of Directors has established an Audit Committee that oversees ADP's risk assessment and monitoring activities. Ongoing risk assessments and management feedback are used to determine specific internal and external audit activities needed. Management designates personnel to monitor selected projects during design and implementation to consider their impact on the control environment prior to implementation.

ADP management and supervisory personnel monitor internal control performance quality as a normal part of their activities. To assist them with these monitoring activities, the organization has implemented a variety of activity and exception reports that measure the results of various processes involved in providing services to client organizations including processing volume and system availability reports as well as processing logs. Exceptions to normal or scheduled processing due to hardware, software, or procedural problems are logged, reported, and resolved daily. The appropriate levels of management review these reports daily and action is taken as necessary.

Client Satisfaction Monitoring

Solution Center management communicates regularly with internal staff and clients to discuss issues and client satisfaction. In addition, clients are surveyed after implementation, and annually thereafter, to determine client satisfaction with ongoing service delivery and products.

Internal Audit Monitoring

ADP's business units are subject to periodic reviews by internal and external auditors. Internal auditor involvement may include, but is not limited to, gaining an understanding of, and evaluating:

- Management structure
- Systems development and programming
- Computer operations
- Physical and logical access
- Finance and accounting

Audit issues are reported to the relevant ADP senior management and, if appropriate, the relevant business unit President and/or Chief Financial Officer.

Facilities Management Services Vendor Monitoring

CBRE Monitoring

Through October 31, 2019, ADP contracted with CBRE, Inc. a facilities management services vendor, to provide specific functions (i.e., physical access and environmental safeguard monitoring) for select ADP locations in the United States under the direction of ADP management. As part of ADP's vendor risk management process, ADP has implemented some monitoring controls over the services provided by CBRE. A governance committee consisting of high-level ADP and CBRE portfolio executives has been established to oversee and track the service performance levels provided to ADP by CBRE. Routine facilities maintenance activities and incident requests are tracked via a job management tool (Service Insight and Incident Notification reports). In addition, CBRE's activity monitoring reports are generated for the governance committee to review.

ADP/CBRE governance committee members are senior leaders that have executive oversight responsibilities for contract performance and service level compliance. The ADP/CBRE governance committee members are key senior property management functional leaders (CBRE Alliance Director, Finance Director, Operations Director, and HR Manager). Governance committee meetings are held biweekly, schedule permitting. Performance issues or CBRE service failures are escalated and addressed at these meetings.

Sodexo Monitoring

Effective November 1, 2019, ADP has contracted with Sodexo a facilities management services vendor, to provide specific functions (i.e., Access is through GSO) environmental safeguard monitoring) for select ADP locations in the United States under the direction of ADP management. As part of ADP's vendor risk management process, ADP has implemented some monitoring controls over the services provided by Sodexo. A governance committee consisting of high-level ADP and Sodexo portfolio executives has been established to oversee and track the service performance levels provided to ADP by Sodexo. Routine facilities maintenance activities and incident requests are tracked via a job management tool (Maximo and Incident Notification reports). In addition, Sodexo's activity monitoring reports are generated for the governance committee to review.

ADP/ Sodexo governance committee members are senior leaders that have executive oversight responsibilities for contract performance and service level compliance. The ADP/ Sodexo governance committee members are key senior property management functional leaders (VP Operations, Finance Director, Operations Director, and HR Manager). Governance committee meetings are held biweekly, schedule permitting. Performance issues or Sodexo service failures are escalated and addressed at these meetings.

CONTROL ACTIVITIES

ADP has developed and implemented formal policies and procedures that address critical operational processes to help management ensure that directives are carried out to meet company objectives. Control activities, whether automated or manual, related to the achievement of specific control objectives are applied at various levels throughout the organization.

Specific control activities are provided in the *Transaction Processing* and *General Computer Control* sections within this Description as well as within Section Four: *Description of Control Objectives, Controls, Tests, and Results of Tests*.

INFORMATION AND COMMUNICATION

ADP's information system has been designed to capture relevant information to achieve the financial reporting objectives of its user entities. The information system also consists of procedures, whether automated or manual, and records to initiate, authorize, record, process and report user entity's transactions (as well as events and conditions) and maintain accountability for the related assets, liabilities, and equity. A description of the information system is provided within the *Overview of Operations* section of this Description.

Employees

ADP has implemented various communication methods to assist employees in understanding their individual roles and corporate controls, and to encourage timely communication of significant events. The particulars vary from region to region but include orientation and training programs for new employees. In addition, all new employees receive a copy of a handbook that describes ADP policies. Newsletters that summarize significant events and changes to corporate policy are issued regularly. Time sensitive information is communicated to employees by email. Managers hold staff meetings monthly or as needed. Employees have written job descriptions. ADP conducts background and security checks, and verifies references.

Clients
Client communication methods vary from region to region; however, each region sends newsletters and holds meetings and seminars to apprise their clients of system and regulatory changes that might affect the client organization. In addition, each client organization has a service representative who communicates with the client organization regularly by phone, fax, letter, and email.

CONTROL OBJECTIVES AND CONTROLS

The control objectives specified by ADP, the controls that achieve those control objectives, and management responses to deviations, if any, are listed in the accompanying *Description of Control Objectives, Controls, Tests, and Results of Tests.* The control objectives, controls, and management responses are an integral part of the Description.

OVERVIEW OF THE WORKFORCE NOW SERVICES

Service Overview

ADP's Workforce Now Services is comprised of both hosted and outsourced processing benefits, payroll, and time & attendance service offerings. Clients can select which service offering they want to contract for as part of the Workforce Now Services.

The following summarizes the key aspects of the Workforce Now Services:

Benefits Service

The Workforce Now Services Benefits Service offering enables an organization to efficiently manage health and welfare benefits. The Workforce Now Application provides a full-featured Human Resource Management System (HRMS) that includes benefits administration, employee and manager self-service, leave management, performance management, and recruitment management functionality. Furthermore, if opted for, it can provide connectivity to a client's internal systems, benefit providers, and other services providers.

There are two service models for Benefits Service that clients can contract for using the Workforce Now Application. The first includes the Comprehensive Benefits whereby clients contract with ADP to provide HR and benefits administration services. The services included within the Comprehensive Benefits offering are benefit and payroll connections to third party carriers, open enrollment services, and carrier billing/invoice reconciliation and payment. The second service is offered via Software as a Service whereby the Benefits clients use the Workforce Now Application to administer their benefits programs and do not contract with ADP for any outsourced Benefits Administration Services. This service also includes benefits and payroll connections to third party carriers.

<u>Implementation</u>

ADP's Comprehensive Benefits Implementation group sets up and configures a client's benefit and related payroll options. The Workforce Now Application downloads and transmits enrollment information to benefits providers and third party administrators and transmits deduction information to the client's payroll system. An array of outsourcing services are also available through the Comprehensive Benefits group including Enrollment Services, a Benefits Call Center accessible by employees and HR staff, Billing/Invoice reconciliation and payment, Life Insurance Administration, Eligibility Audits, Fulfillment, Leave Management, Qualified Medical Child Support Order (QMSCO) Administration, COBRA/HIPAA Administration, and Flexible Spending Account (FSA) Administration. Specific business processes and related controls for Life Insurance Administration, Eligibility Audits, Fulfillment, Leave Management, Qualified Medical Child Support Order Administration, COBRA/HIPAA Administration, and FSA Administration are not in the scope of this report.

Time & Attendance Services

The Time & Attendance Services offering is comprised of two solutions for which ADP Workforce Now Services clients can contract based upon their needs.

<u>Essential Time</u>

The Essential Time Service is a central calculation engine for compiling time and attendance data, and applying company-specific pay rules. It also provides labor management tools that support management/supervisor timecard review and approval, and provides management analysis and reporting capabilities.

The Essential Time processing environment is multi-tier in design; the tiers enable separation of functional components to maximize reliability, performance, scalability, availability, serviceability, and security. The Essential Time Service architecture is comprised of multiple shared server farms (PODs) with redundant servers configured for the different tiers. The servers support web, reporting, data-collection, application functions, and the clustered database servers facilitate continuous client availability. ADP assigns clients to a shared server farm in one of the data centers, hosted at ADP's GETS US Hosting and Data Center Facilities, based on the client's size, and required production environment specifications. Logical security controls are deployed within the shared server farm to secure client information.

A hosted Essential Time Service includes the following tiers:

- Web, reporting, and data-collection servers are used to record, collect, and report employee time
- Application servers that run the processing engines responsible for the application's business logic and facilitate employee records' management
- Database servers that store client data

<u>Enhanced Time</u>

The Enhanced Time Service is comprised of a multi-tier technology architecture design; the tiers enable separation of functional components to maximize reliability, performance, scalability, availability, serviceability, and security. Every client has a dedicated application instance supporting their Enhanced Time Service environment.

The key components supporting the technology architecture include the following:

- Application servers that support the collection of time accounting data as employees enter it as well as core business logic, including acquiring punches, applying pay code edits, and time approvals. In addition, the application servers run report engines to support the client's reporting requirements.
- Web servers/instances that contain all static content and listen for browser requests related to timesheet access, supervisor access for editing timesheets, and running reports. The web servers pass the browser request to the application servers for processing.

- Integration services that run on application servers through the ADP TLM Interface (Import/Export module) utility facilitate importing data into or extracting data from the Enhanced Time application.
- Background processing services that run on application servers that total data acquired from punches, schedule changes, pay code edits, and imported data.
- Database servers that store client data.

The Enhanced Time Service may also be supported by additional "optional" technology components that clients can contract separately from ADP (outside the scope of this Description), such as:

- Polling servers with Data Collection Manager (DCM) or the ADP TLM Interface (HandPunch Module) - transfers information from the data collection devices that are located at the client site to the Enhanced Time Service. Data is transmitted via a dedicated Frame Relay circuit, directly over the Internet or via Virtual Private Network (VPN).
- Data collection devices (e.g., such as Ethernet clocks or biometric devices) used by employees to swipe badges, enter badge numbers or insert their hands to register in and out punches.
- Payroll Module – The Payroll Module within the ADP TLM Interface integrates the Enhanced Time Service with ADP's Payroll systems. The Payroll Module outputs hours and temporary department and rate information so it can be imported into an ADP Payroll system. The TLM Interface Replication Module copies the pay files from the Enhanced Time Service to a specified ADP network folder for ADP's hosted HR and payroll systems for pick up and import into the payroll system. The path of the network folder is specified during implementation.

Payroll Service

The Payroll Service offering is comprised of:

- Receipt/input of employee current period hours and/or current period earnings.
- Master file maintenance (input related to new hires, updates to existing employees' data, or changes to the company's master data).
- Payroll transaction processing based on client-specified schedules.
- Production of output, including check and voucher pay statements, payroll reports, and output files, such as money movement, general ledger and data files.

The ADP payroll locations supporting clients are comprised of:

- Service Payroll Centers (collectively referred to in this report as Regions) – Regions perform the primary activities for Payroll Services clients, including printing client payrolls, ADPChecks, and distribution of payroll-related documents and files. The Regions also perform the gross-to-net calculations. Region activities are processed on the mainframe platform hosted at ADP's Global Enterprise Technology & Solutions (GETS) US hosting and data center facility in Georgia.
- Satellite locations are responsible for selling ES products to clients, implementing clients on the various ADP platforms, and providing ongoing client support.

IT Applications and Supporting Infrastructure

The table below identifies the applications supporting the ADP Workforce Now Services (which includes clients on Workforce Now V18.0 or greater), the supporting operating systems and database platforms, and the applicable client group (collectively referred to as "in-scope applications"):

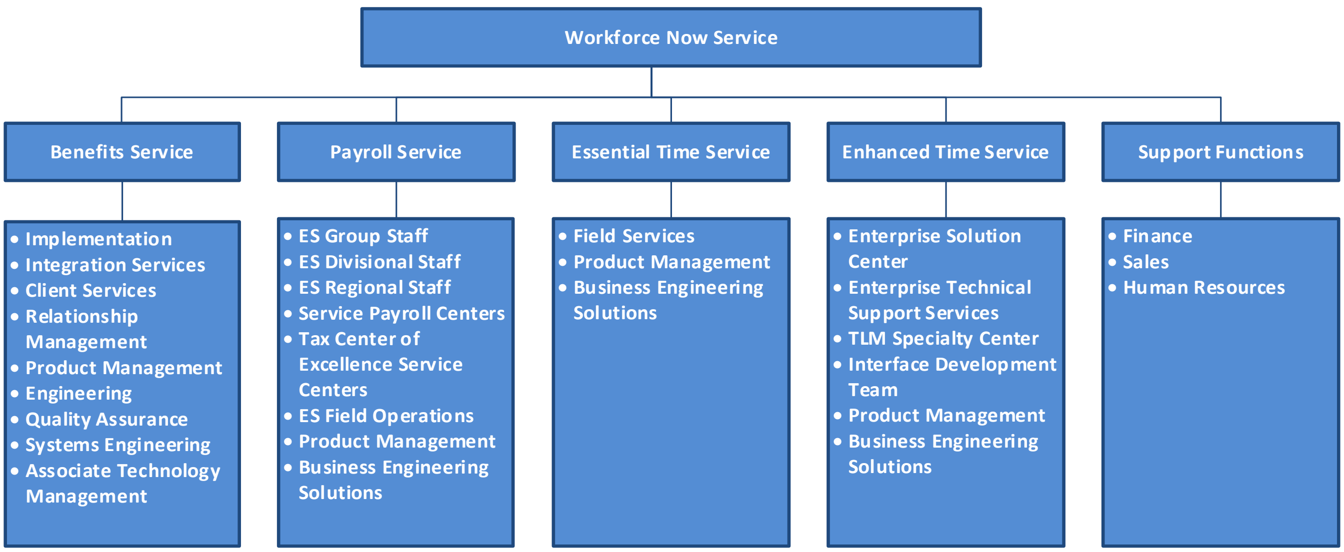
Application Name	Operating System Technology	Database Technology	Description
iReports	Linux AIX	Oracle	Hosted web-based output system that gives Payroll Service clients the ability to view PDF copies of their payroll output reports that are produced by the Payroll Application.
Enhanced Time Application	Windows	Oracle	Web-based time and labor application licensed from third party vendor (Kronos) is offered to clients who contract for the Enhanced Time Service.
MOTIF Account Request Tool	Windows	SQL	Authentication tool customized by ADP and used internally for logical security control enforcement.
Payroll Application	Mainframe	IBM DB2	Hosted back-end application to the Workforce Now Application and iReports that stores client employee master data, and processes and calculates client payrolls. The Payroll Application consists of various core modules, databases, and programs referenced throughout this description such as: Client Control Information (CCI), Datapool, Payroll Tracking Control System (PTCS), KeyFast, MQSeries, AutoLink, Calc Update Interface (CUI) database, Batch Edit Rule database, Employee Master database (EMP), Management Reporting System (MR 2000), and Statutory (STAT) File database.

Application Name	Operating System Technology	Database Technology	Description
Workforce Now Application	Windows zLinux	Oracle	Hosted human capital management application that integrates the following key modules: • Human Resource Management - allows clients to manage human resource tasks and employee information (e.g., name, address, salary) in a central database that integrates with the other Workforce Now modules. Workforce Now has built in HRMS tables that serves as the system of record for HR and employment data and enables clients to access employee information and system-generated reports in real-time. • Payroll - Allows Payroll Service clients to enter their payroll data and transmit information to the Payroll Application • Time & Attendance – Provides time and attendance functionality that enables clients to streamline payroll preparation, simplify employee scheduling, improve wage and hour compliance, and manage absence and vacation tracking. Clients can contract for Essential Time or Enhanced Time Services in this module. • Benefits - Provides flexible benefit management options to fit clients' benefit plan structures and provides a broad selection of choices from core benefits administration to a comprehensive suite of benefits administration offerings. The module, offered to Benefits Service clients, includes everything from plan set up, eligibility and enrollment, employee communication, spending accounts and COBRA, to additional benefit services.

Key Organizational Support Structure

ADP's Workforce Now Services System Key Support Structure:

The organizational structure supporting ADP's Workforce Now Services System is comprised of ADP functional teams across multiple business units. The following describes the key functional support groups aligned to the Workforce Now Services System.



<u>Benefits Service</u>

The following is a description of the key Benefits Service functional and support areas:

- <u>Implementation</u>: The Implementation team receives incoming sales orders and confirms the feasibility of product features and client needs. They are responsible for supporting the configuring software and hardware, customizing reports, and providing training to clients.

- <u>Connection Services</u>: Monitors files from the Workforce Now Application and third party systems (e.g., insurance carriers, third party administrators, client systems). If necessary, will attempt to retransmit files based upon a schedule which were not sent successfully.

- <u>Finance</u>: The Finance team provides accounts receivable and expenditure oversight, determines the appropriate business unit to apply expenses and/or revenue, provides reporting on all financial matters, and assists in determining competitive pricing structures for product lines and services offered.

- Client Services: Client Services is primarily comprised of two separate groups – the Service Team, and the Client Services team:
    - The Service Team is responsible for providing human resource and benefits administration services to Comprehensive Benefits clients located in Alpharetta, GA, Charlotte, NC; El Paso, TX; Clackamas, OR; Augusta, GA; Elk Grove, IL; and Atlanta, GA while the Client Service team is responsible for providing services to SaaS clients. The Service Team shares client services support responsibilities for ADP Comprehensive Benefits clients with ADP associates located in Manila, Philippines. The services provided by the Service Team include: benefits call center, enrollment services, billing/invoice reconciliation, benefits administration, eligibility audits, fulfillment, COBRA administration, HIPAA administration, and FSA administration. The Open Enrollment Team is responsible for Open Enrollment. The Open Enrollment Specialist receives and updates the plans and rates for clients on an annual basis and processes the participant elections. The Benefits Solution Specialists are responsible for contacting clients about their enrollment period, receiving open enrollment data and configuring the system for the new plans and rates.
    - The Client Services team is responsible for providing services to SaaS Benefits clients and is also comprised of four direct teams within: Service Center, Account Management, Open Enrollment, and Client Relationship. Once a client implementation is complete, these teams are responsible for developing and maintaining client relationships and for providing ongoing support for SaaS Benefits clients. The Client Services teams are located in Elk Grove, IL; El Paso, TX; Clackamas, OR; Owings Mills, MD; Atlanta, GA; Alpharetta, GA, and other locations.

- Relationship Management: The Relationship Management team is responsible for managing all aspects of the client relationship and overall experience and works closely with each of the previously-mentioned Client Services teams to accomplish their responsibilities.

- Product Management: The Product Management team is an extension of Marketing. The team monitors the market from many aspects including obtaining information from clients, Sales, Engineering, and Business Engineering Solutions as well as from training and competitive/market sources. Product Management is ultimately responsible for identifying and scheduling of required product enhancements. Product Management also provides the future vision and product strategy as it relates to the external marketplace and as well as internally with other ADP SaaS and Comprehensive Benefits product suites. The Product Management group is located Alpharetta, GA, and Parsippany, NJ.

The following teams, although not specifically documented in the organizational chart above, reside within the Comprehensive Benefits and SaaS groups and are responsible for various activities supporting the Benefits Services System:

- Engineering: Engineering is responsible for implementing the product roadmap and resulting development specifications for new Workforce Now Application functionality and enhancements. Application development begins with the design of a user interface design prototype that models the design specification developed by the Product Strategy team. After the prototype is tested, modified and accepted, software engineers write the code necessary to implement the design specifications developed by the Product Strategy and User Interface teams.

- Quality Assurance: The QA Team is responsible for developing and executing Workforce Now Application test plans that provide assurance that the application is free of significant operating deficiencies, and minimize the possibility that the introduction of an application change will impair a user's ability to operate the Workforce Now Application properly, or cause the functionality in the application not to perform as designed. After concluding the test phase of application development, the QA Team coordinates with the Systems Engineering team to schedule application releases (deployment) to users. In addition to performing all pre-release testing, the QA Team performs on-going problem resolution tasks to minimize the interruptions introduced to Workforce Now Application users by occasional application issues commonly referred to as "bugs." These "bugs" are quickly identified, recorded, and resolved by members of the QA Team.

- Systems Engineering: The Systems Engineering team is responsible for deploying the application releases and for ensuring the application's continuous operations. The Systems Engineering team coordinates with the QA and Engineering teams to release developed and tested applications to users typically over a weekend. The Systems Engineering team implements the new release and tests for reliability and user availability. The GETS US organization monitors system performance and availability of the servers at ADP's GETS US organization data center facilities. The controls performed by GETS US organization supporting these processes are covered in ADP's GETS US Organization SOC 1 Report.

- Associate Technology Management (ATM): ATM is responsible for the security administration of the network at ADP's GETS US organization data center facilities as well as at regional ADP business unit locations. ATM is also responsible for supporting/managing logical and remote access to ADP's WAN, ESNet. The controls performed by the ATM group that support all ADP business units are not in scope of this report and are covered in ADP's GETS US Organization SOC 1 Report.

Time & Attendance Service – Essential Time

Field Services

Field Services is primarily comprised of three separate groups:

- *Client Services (TLM Service Center)*: This group is responsible for providing client support and taking corrective action when necessary to provide timely and accurate processing. It provides limited retraining to clients who experience difficulties operating or accessing the software. When clients contact this group with issues, if the TLM Service Center representatives cannot resolve the issue, they escalate it to the Technical Support Services group.
- *Technical (Support) Services*: The Technical Support Services group provides second-level support for client issues, potential product defects, and enhancements. It is the liaison between the Regional Implementation, TLM Service Center, and the Hosting Operations groups as well as between the Hosting Operations group and third party vendors.

The Implementation Field Services group is located in offices throughout the country and is responsible for collecting information required to setup new clients on Essential Time and for configuring new client environments. Implementation receives incoming sales orders and assesses and confirms the feasibility of product features and client needs.

Other MAS TLM Groups

Other ADP MAS TLM organizations support other Essential Time System aspects. The following TLM groups are located in ADP offices throughout the country.

- *Product Management*: Product Management monitors several market aspects including obtaining information from clients, sales, development, Business Engineering Solutions, training and competitive/market sources. Product Management is ultimately responsible for identifying and scheduling required product enhancements. Product Management also provides the future vision and product strategy relating to the external marketplace and internally as related to other ADP product suites.
- *Development and Training*: The Development and Training group defines internal resource training and expertise building training tracks and lesson plans. It provides instructive coursework from beginner level to advanced user for both end-users and in-house TLM Service Center and Implementation associates. The group produces training and reference documentation for all products and functionalities.
- *Field Enablement (previously Business Engineering Solutions):* The Field Enablement group is responsible for the design, management, and execution of field test and pilot programs for new products and their subsequent rollout to field associates. Field Enablement also provides direction and implements changes to the field as MAS senior management deems appropriate.

Time & Attendance Service – Enhanced Time

The following is a description of the key functional and support areas for Enhanced Time:

Field Support: Overall management of field support services, which include the Center of Excellence, Client Account and Operations, as well as Project Management.

TLM (Time and Labor Management) Center of Excellence: This team is responsible for ensuring the consistent delivery of quality account service and project management.

Regional Services Centers (Eastern, Southeastern, Midwest, West): These teams are responsible for application support services.

Client Services: Provides assistance and limited retraining to clients experiencing difficulties using or accessing the software. They determine if issues are related to potential application defects, the result of a user error, or potential system configuration issues. This team is also responsible for managing the deployment of application updates (i.e., hotfixes and/or service packs).

Implementation Services: Responsible for new client implementations, as well as overseeing the deployment of the system in the production environment. They act as a liaison between clients, the GETS US organization, and other business units to coordinate the configuration and set up of the new client's Enhanced Time Services System. They are also responsible for defining the scope of the project and for drafting a Statement of Work (SOW), as well as providing a comprehensive project plan for setting and tracking milestones.

Project Services: This team is responsible for coordinating and managing add-on services (e.g., existing configuration changes to address new business needs) for clients in production.

Shared Services: This team is responsible for coordinating and managing upgrades (e.g., moving clients from one version of Enhanced Time to address business needs) for clients in production.

Client Account Executive: The CAE is responsible for overseeing the client experience, including coordinating the resolution of complex issues that span multiple ADP services. The CAE will be able to offer Strategic business planning, Partnership to solve clients' critical business issues, Successful service delivery across solutions, and Proactive work to maintain client satisfaction.

Client Care/Operations: Highly specialized TLM support consultants that provide clients with a personalized experience assisting users with onsite support and helping clients be more efficient and effective with ADP's product suite.

Project Managers: Internal operation support of ADP strategic initiatives.

HCM (Human Capital Management) Technical Services Group: Complements the Solution Center by providing product technical support to internal and external clients. This group serves as a technical escalation point for the Solution Center team and assists consultants in resolving the most challenging product issues that arise.

Human Resources: Maintains policies and procedures for HR activities, and screens potential hires to ensure the appropriate skill and proficiency in the new-hire base to minimize turnover while retaining critical knowledge.

National Account Services (NAS) Technical Services Group

The MAS Enhanced Time System is also supported by the National Account Services (NAS) Technical Services Group. The NAS Technical Services Group is responsible for supporting and maintaining the Super User Account Request tool (discussed further in section 'Logical Security'). This group also maintains a separate Enhanced Time test environment which can be utilized by both the MAS and NAS Enhanced Time organizations to test application functionality.

<u>Payroll Services</u>

The organizational structure supporting Payroll Services is comprised of ES Group Staff, ES Divisional Staff, ES Regional Staff, Service Payroll Centers, Tax Center of Excellence Service Centers, and ES Field Operations.

<u>ES Group Staff</u> – The ES Group Staff is responsible for activities associated with supporting data processing systems. The ES Group includes the following groups:

- Finance
- Human Resources Shared Services (HRSS)
- Sales
- Client Services
- Field Services
- Major Account Services
- National Account Services
- Small Business Services

<u>ES Divisional Staff</u> – The ES Divisional Staff supports the Service Centers. The Divisional staff is responsible for:

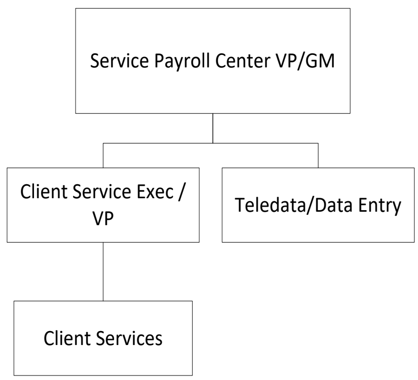
- Coordinating the activities for the Service Centers
- Promoting product and operating efficiency
- Providing technical, sales, financial, and human resources development support to the Service Centers

<u>ES Regional Staff</u> – The ES Regional Staff is located in the Service Centers and is responsible for:

- Selling products to clients

- Converting clients to ADP’s systems
- Supporting the hosting of hardware and software that is used to support transmission of client payrolls
- Supporting the hosting of hardware and software that is used to support printing of client payrolls
- Supporting processing of clients’ payrolls
- Producing and distributing payroll related documents and files
- Providing on–going support and service to clients

Service Payroll Centers (Service Center) – Each Service Center is similarly organized. Staffing varies based on the Service Center’s type (Service Payroll Center or Satellite location) and client base. In most Service Centers, the functions are part of the Regional organization.



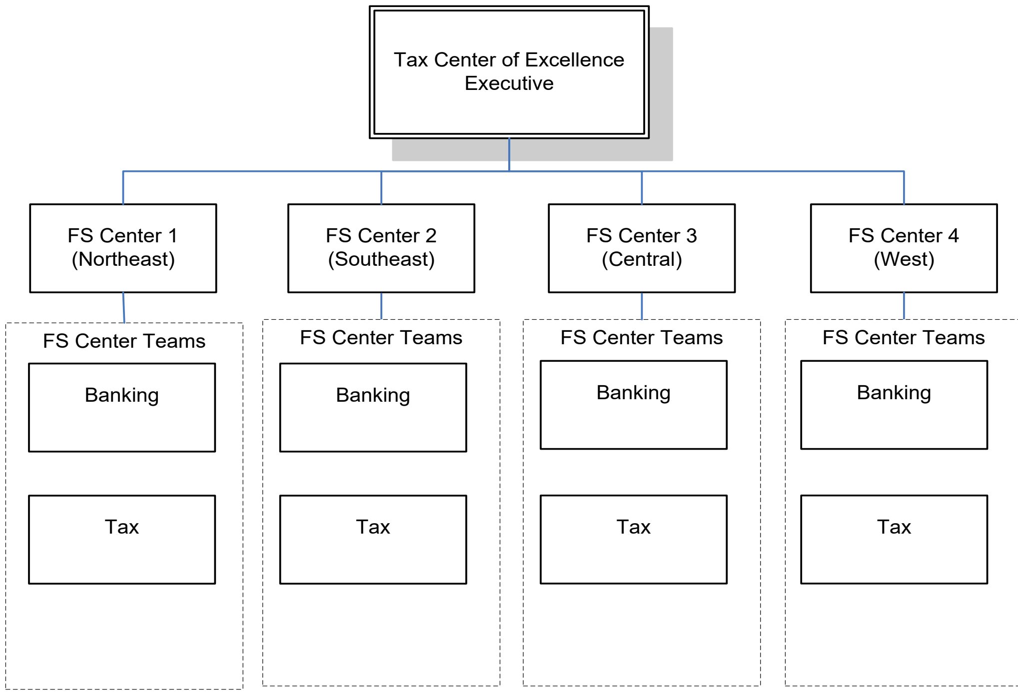
The Service Centers functional groups include:

- *Client Services*: responsible for taking corrective action, when necessary, to provide timely and accurate payroll processing. After the Implementation Specialists successfully set up clients on the Payroll Application, Client Support Specialists (CSSs), also referred to as Solution Center Consultants, are assigned to the client, allowing clients to contact CSSs directly with Payroll Application questions.
- *Teledata/Data Entry*: responsible for entering and verifying payroll information received via telephone, fax, or worksheets into the “Key–Fast” system that is used for online payroll data entry and data validation. Only some Service Centers support processing of worksheet payroll data.

Tax Center of Excellence Service Centers – For each of the Service Centers, the Payroll Application produces money movement files (if contracted by clients), such as direct deposit files, that are transmitted to individual banks and Full Service Direct Deposit (FSDD) and ADPCheck files that are transmitted to ADP’s Compliance and Payment Solutions (CAPS) system. ADP’s Banking, Check Control, and Tax Control responsibilities are consolidated into four Financial Service Centers. The Financial Service Centers are also responsible for addressing issues related to accruing and impounding tax liabilities as incurred for clients using ADP’s Payroll Tax System. The relevant functional groups within each Financial Service Center include the following departments listed in the chart below:

- Banking: responsible for a variety of functions related to payroll direct deposits and check processing.

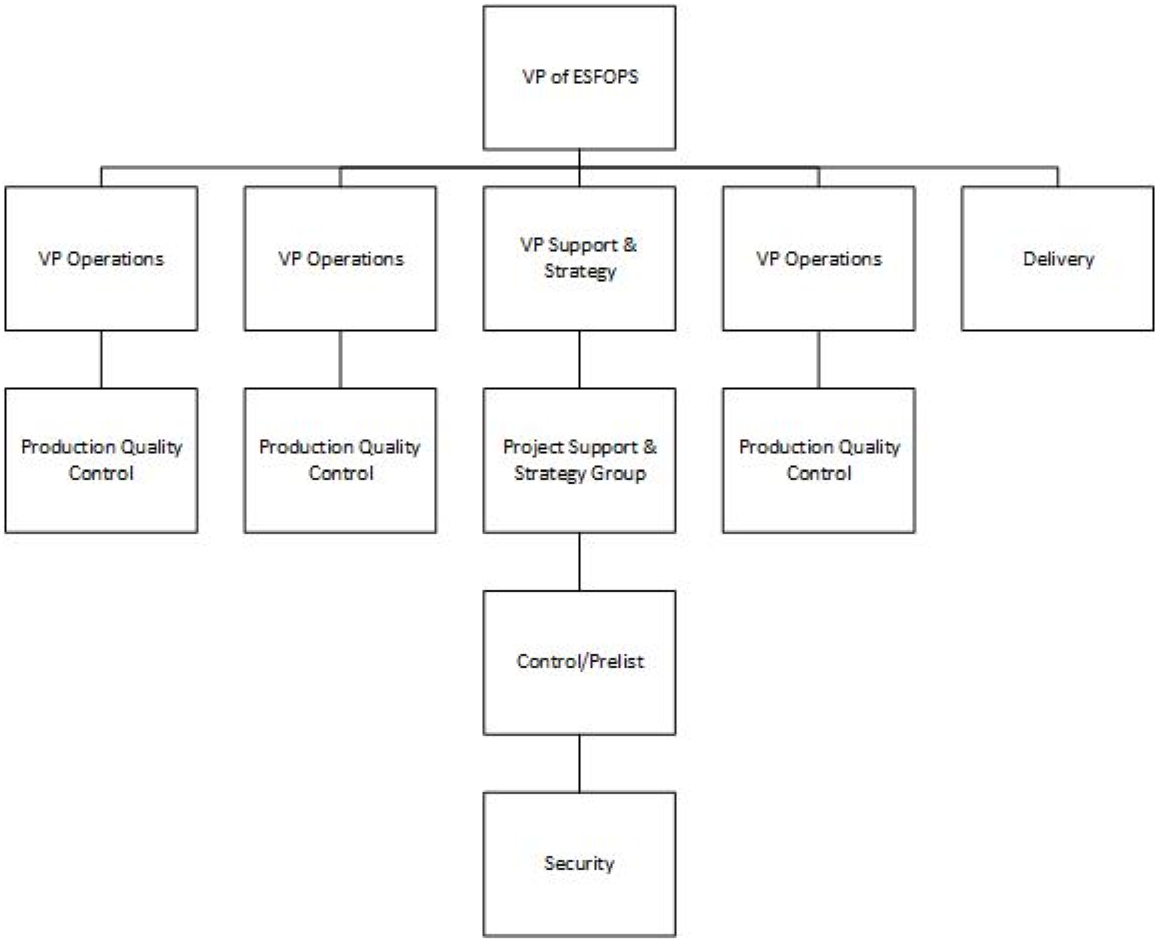
- Tax: responsible for the production of tax documents and for maintaining specific tax related client information.



ES Field Operations (ESFOPS) – the relevant functional groups within ESFOPS include:

- *Payroll Production/Quality Control/Operations:* responsible for day–to–day regional payroll production operations, including printing and stuffing paper output. The Service Centers use consistent hardware, software, and operating procedures to process payrolls and are also responsible for assembling the payroll processing output (i.e., printed reports and pay documents) as well as for packaging it for delivery to the client.
- *Prelist/Editing:* responsible for processing client input according to specifications and taking corrective action if a client input error should occur. Prelist/Editing reviews payroll processing control information for accuracy and completeness. The Regional Prelist/Editing teams also assist ATM, part of the End User Computing and End User Support, monitor transmissions from Enhanced Payroll Communication (EPC) servers. The End User Computing and End User Support group is part of the GETS US organization.
- *Control/Management Reporting:* responsible for establishing and maintaining the Management Report Master File that is used to support customized payroll reporting. The Control/Management Reporting group completes worksheets that specify client-requested reports. Information can be provided on printed reports or magnetic tape. The frequency of these reports varies depending on clients' requirements. They are also responsible for the setup and maintenance of digitized client images including clients' authorized payroll signatures and logos, and the set up and close out of clients' quarterly ledger files and quarterly reports.

- *Delivery:* responsible for the pickup and delivery of payroll packages and monitoring these activities.



Other Payroll Supporting Groups

Payroll Development – Payroll Development is responsible for the development and maintenance of the Payroll Application.

Integrated Acceptance Test – Integrated Acceptance Test (iAT) is responsible for testing Payroll Application changes in an environment that is similar to the production environment.

Release Management – Release Management is responsible for project managing, approving, and monitoring the deployment of Payroll Application changes to the production environment.
Payroll Support – Payroll support is responsible for migrating Payroll Application changes to the Payroll Application production environment.

Field Support – Field Support is responsible for providing hardware and software-related technical assistance to the Regions and Mainframe & Midrange Tech and Apps Management (M&MTAM).

Systems Engineering – Systems Engineering (SE) is responsible for developing and maintaining mainframe operating system (OS) standards and initiating OS updates for the Payroll Application production environment.

Statutory Research Shared Services – Statutory Research Shared Services is responsible for making inquiries about and obtaining information concerning requirements as well as pending and enacted legislation that may impact payroll tax issues including the taxation of employee benefits through payroll.

Deployment Engineering – Deployment Engineering is responsible for deploying application changes to the production environment of the Payroll Application's input and output systems.

Access & Identity Management (AIM) – AIM is responsible for developing the Security Management Services (SMS) product hosted at the GETS US hosting and data center facilities. SMS is a web security product that provides the basic security protocol for accessing several ADP Internet-based products, including Workforce Now, Self Service Portal, iReports, and MAS GLI and provides:

- Centralized user management
- Strong user authentication (requiring user ID/password and a digital certificate)
- Role-based user authorization
- Single sign–on features across multiple ADP Internet products

Data Service Center Financial Services Team – The Data Service Center Financial Services (DSC FS) Team is responsible for all MAS FS New Output System (NOS) balancing and error review/notification between the Payroll Application records and ADP's CAPS system records. The DSC FS team is overseen by the Financial Services Center Specialists.

Mainframe & Midrange Tech and Apps Management – M&MTAM is responsible for the remote operational support of the Payroll Application hosted at GETS US data center facilities. ADP has consolidated certain Payroll Services operations into M&MTAM. The M&MTAM organization consists of two groups:

- M&MTAM – Payroll Command Center (CC): The Command Center is located in Illinois with a second Command Center located in Pune, India and both locations support production processing. The Command Centers' primary responsibility is supporting the Payroll Application console operations. The Command Center staff is responsible for job execution, job monitoring, system monitoring, and workload balancing.
- M&MTAM – Technical Services: This group's primary responsibilities include supporting the Payroll Application job scheduling, application change management support, management of mainframe logical access privileges, and problem management. The M&MTAM controls over job scheduling and problem management are covered within the ADP GETS US Organization SOC 1 Report.

Changes to the Control Environment

The Pay eXpert application stopped supporting clients as an input system effective prior to April 1, 2019 and as a result have been removed from the scope of this report. Additionally, the Workforce Now V2.0 client group is no longer a component of this service as no clients were utilizing the Workforce Now V2.0 application during the reporting period. As a result of this change, the report control objectives and controls have been consolidated and restructured to better represent the services provided only to Workforce Now V18.0 application or greater clients. Refer to *Prior Period Control Mapping* in Section V of this report for the mapping of the prior period controls to the updated controls presented in this report, which has been provided for informational purposes only.

The Mainframe backup and IT job scheduling controls performed by the Mainframe & Midrange Tech and Apps Management (M&MTAM) group as part of the GETS US Organization are no longer included in the scope of this report. These controls are now covered by ADP's GETS US Organization SOC 1 report.

There have been no other changes to the control environment that would be considered significant to a user entity or their auditors.

SCOPE OF THE REPORT

This description was prepared in accordance with the criteria set forth for a SOC 1® Type 2 Report in the ADP Management Assertion and the guidance for a description of a service organization's system set forth in the AICPA Attestation Standards AT-C section 320 as clarified and recodified by Statement on Standards for Attestation Engagements (SSAE) No. 18 *Attestation Standards: Clarification and Recodification*.

This report covers ADP's Workforce Now Services that comprises payroll hosting, outsourcing, or both, time and attendance, benefits administration transaction processing, and its supporting technology infrastructure supporting clients using Workforce Now V18.0 or greater (collectively referred to as the 'Workforce Now Services System').

The scope of the report covers the business processes that ADP has determined are significant to its clients from a financial reporting perspective and the applicable information technology processes specific to supporting the Workforce Now Services System. New client implementations and unique client situations are outside the scope of this Description.

The Workforce Now Services System interfaces with other ADP applications and services (e.g., Payroll Tax Filing, Print Services, WGPS, and Retirement Services). In addition, clients may contract with ADP for additional HR support services via ADP Comprehensive Services. This service allows clients to transfer administrative responsibility for a range of selected HR processes to ADP. These are optional systems and services offered by ADP. This report is not intended to encompass the control aspects of other ADP services or platforms that may interface with the Workforce Now or Payroll Application. This Description and corresponding services do not cover the Canada Workforce Now Services System (specific to Canada-based clients) which is covered under a separate SOC 1 report.

TRANSACTION PROCESSING

Overview of Key Transaction Processing

The Workforce Now Application collects employee data from several different time-collection mechanisms. Clients' employees can use time clocks, biometrics, telephone interactive voice response (IVR), and the Workforce Now Application to input time-worked data.

The Workforce Now Application processes and calculates employee time and attendance data based on work and pay rules that are configured according to client specifications. Client users with the Supervisor and Administrator/Practitioner profiles can use the Workforce Now Application to:

- Import employee demographic information, accrual balances, and labor-level entry data from their HR or payroll system into the Workforce Now Application using predefined templates
- Review and approve employee timecards
- Initiate time and attendance data processing, review the results of the calculations, and address any errors and/or warnings
- Generate standard reports detailing employee accruals, user configurations, timecard exceptions, individual schedules, and employee timecard details
- Generate export files containing calculated and approved employee data at the end of every pay period to transmit to their HR or payroll system

Clients who subscribe to the Workforce Now Enhanced Time Services are supported by the Enhanced Time Application that is used to manage and process time and attendance of ADP's clients' employees. Clients are responsible for initiating processing and for the input and export of data into the application.

The Enhanced Time Application can collect employee data from various data collection devices (e.g., time clocks, biometric devices, phone, and mobile devices). These data collection devices do not form part of the System and are outside the scope of this Description.

Client employees authenticate into the Enhanced Time Application using a valid user ID and password directly via the Workforce Now Application and perform various manual and automated tasks, such as:

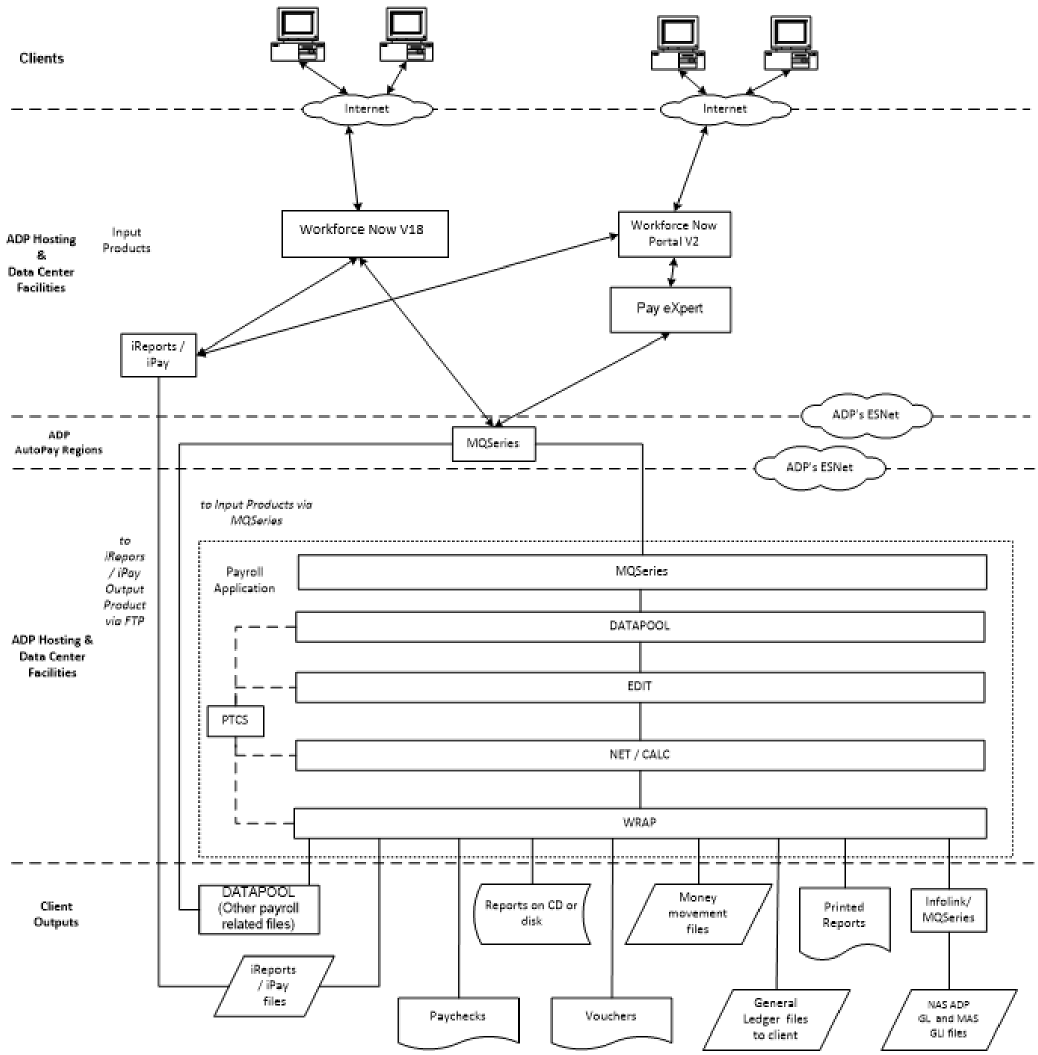
- Enter time
- Import employee demographic information, accrual balances and labor level data from their HR or payroll system to the Enhanced Time application using the ADP TLM Interface
- Review and approve timecards
- Initiate time and attendance data processing, review the results of the calculations, and address any errors and/or warnings
- Generate export files that will be transmitted to HR or payroll systems

The Enhanced Time Application calculates employee time and attendance data based on work and pay rules that are configured according to client specifications during the implementation process. Changes to client configurations can be performed by the client or by ADP upon client request. However, clients are responsible for reviewing the changes made to their environment for accuracy and completeness.

Clients can use the Enhanced Time Application to produce a variety of standard and client generated reports and output files, including:

- Reports such as detailing employee accruals, system configuration, detail quick navigation views, import, individual schedule, and timecard
- Files containing calculated and approved employee data that is exported from the Enhanced Time Application at the end of every pay period in a format required by the client's HR or payroll system. These files are transmitted to the client's HR or payroll system as follows:
    - *For any HR and Payroll system* – Clients download the files using the ADP TLM Interface and manually transmit the files from their PC to their HR or payroll system
    - *For clients that use the ADP hosted Payroll system* – The Payroll Module within the ADP TLM Interface integrates the Enhanced Time Application with their ADP hosted payroll system.

Payroll transaction processing encompasses three major payroll components: Payroll Input, Payroll Processing, and Payroll Output. Input consists of payroll data related to an employee's current period hours and/or earnings and Masterfile maintenance that is collected from the client directly into the Workforce Now Application. ADP processes payroll transactions using the client-provided input and generates a variety of standard and optional output reports (e.g., payroll registers, payroll summary), data files (e.g., money movement, direct deposit, general ledger files including files for NAS ADP GL and MAS GLI, and iReports files). Output reports and files are distributed to clients when produced. The following is a high-level overview of the payroll transaction flow:



Flow of Transactions

ADP's Workforce Now Services encompasses the following components and is supported by the Workforce Now Application:

- Data Input – Workforce Now
- Data Processing – Workforce Now
- Data Processing – Benefits - Carrier Billing/Invoice Reconciliation and Payment
- Data Processing – Benefits - Client Maintenance and Open Enrollment Services
- Data Processing – Payroll Deductions and Tax Withholdings Specifications
- Data Processing – Payroll
- Data Output – Workforce Now
- Data Output – Payroll (Money Movement/Direct Deposit Files)

Data Input – Workforce Now

Benefits Data is input into the Workforce Now Application from a variety of sources, including:

- Files loaded automatically via the Import tool (applicable to both Comprehensive Benefits and SaaS clients)
- Employee Service Center (ESC) representatives (Comprehensive Benefits clients) or ADP Client Service representatives (SaaS clients) via the Client Support Tool
- Client employees, managers, or HR administrators manually keying information into the Workforce Now Application via the web (applicable to both Comprehensive Benefits and SaaS clients)

Benefits Import of Client Files

Periodically clients transmit data files to ADP for import. These import files are generally used to establish new employee records, change existing employee records, and/or terminate employee records. Import files contain client-specific data fields used by the Workforce Now Application such as demographic and employee-indicative data (name, address, gender, marital status, earnings, etc.) and data required by the application to determine benefits eligibility (division, location, class, etc.).

Data files are imported into the Workforce Now Application using an Import tool. The Import tool produces a standard set of error and warning messages when errors occur during the file-import process. Client-specific procedures for both SaaS and Comprehensive Benefits clients determine how these errors and warnings will be corrected.

Benefits Data Entry

The Workforce Now Application is accessed via a secured "https" website and requires a user ID and password for access to input or update data. The applications also use 256-bit Secure Socket Layer ("SSL") encryption to provide data transmission security between the applications and clients. In particular, the SSL security protocol uses RSA public-key cryptography to provide data encryption and server authentication. Client employees, managers, or HR administrators and Comprehensive Benefits associates log into the Workforce Now Application using a unique user ID and password. Functional access profiles (roles with associated access privileges) are available to be assigned to individuals to enforce segregation of duties. Role design and assignment is the responsibility of the client, and typically include an employee role, a manager role, and a client administrator role.

Four standard application profiles are available to client users:

- *Employee Profile* - to enter and change personal data, to enter and change dependent data, to enroll in benefits, and to enter certain life events (qualified status changes such as the addition of a child, marriage, death, etc.).

- *Practitioner Profile* - Administrative users of the Workforce Now Application can add, change, delete company-level information, process payroll, and run reports. Practitioners also can assign, modify, and delete User Profiles assigned to employees.
- *Manager Profile* - The Manager profile has the rights of an Employee profile but may also be permitted to view certain data (e.g., leave information) for designated employees and to review or approve certain requests.
- *Time and Attendance Supervisor Profile:* The Time and Attendance Supervisor Profile has the rights of an Employee Profile but can also edit timecards and schedules of designated employees or groups of employees, and perform other managerial functions such as approving time-off requests, processing exceptions, run reports, review accruals, and review employee information.

The Workforce Now Application enforces input controls and validation checks to ensure the complete and accurate input of client data. These controls include data entry validation controls, mandatory fields, drop-down boxes and pre-populated fields that cannot be modified via data entry. As a result of these controls and validation checks, error messages appear on the user's screen to investigate and resolve. The Events tab on the Workforce Now application records the transaction data entered by employees and Employee Service Center (ESC) associates.

The transmission of files between clients and the Workforce Now Application takes place via the FileShare sub-application. Authenticated users can securely transmit, send, and receive files to other Benefits Application users via this FileShare sub-application. The data transmissions at the application level are secured via 256-bit Secure Sockets Layer (SSL) encryption.

Essential Time - Collection Mechanisms

Data is input into the Workforce Now Application from a variety of time-collection mechanisms. The scope of the SOC report addresses data transmissions of time and labor management data to the Workforce Now Application, but it does not include controls surrounding the time-collection mechanisms that the clients use. User entity control considerations related to the time-collection mechanisms are listed in the accompanying *Complementary User Entity Controls*.

<u>Time Clocks</u>

Client locations use three types of time clocks (CMI, Kronos, and RSI) that are microprocessors and read barcode badges, magnetic stripe, or radio frequency (proximity readers). A time punch initiates the start and end of shift segments and is stored on the time clock memory and the stored punches are periodically forwarded to the Workforce Now Application at scheduled intervals. The data transmission to the Workforce Now Application is initiated by data-collection software that runs on infrastructure hosted at the clients' premises.

Biometric Devices

When clients use the RSI time clock biometric device, their employees swipe their badges and insert their hands or fingers into the biometric reader that stores a template of their hand sizes and shapes of their fingerprint patterns to punch in and out and authenticates each client's biometric data. This authentication method also prevents employees from punching in or out for each other.

Telephone Using IVR

Employees call the ADP phone server and provide their user ID and PIN to punch in and out or to do labor allocation to different cost centers.

Web-based

Clients access the Workforce Now Application directly using a unique user ID and Password. Clients access the application to submit their time using one of the following methods:

- *In/Out Times*: Employees enter In/Out times into their Timecard Manager to record time
- *Total Hours*: Employees input their total hours in their Timecard Manager to record time
- *Web Clocking Function*: Employees access the web-based application to access time clock functions such as Clock In, Clock Out, or Lunch Out

Managers and supervisors use the Workforce Now Application to review and approve timecards. Every Workforce Now Application user is associated with a profile that determines the time entry, time card editing, and report generation functions that the user can perform in the application.

The Workforce Now Application is configured with the following profiles:

- *Employee Profile* - Users with this profile can enter and change personal and dependent data, enroll in benefits, and enter certain life events (qualified status changes such as the addition of a child, marriage, death, etc.)
- *Practitioner Profile*- Administrative users of the Workforce Now Application can add, change, delete company-level information, process payroll, and run reports. Practitioners also can assign, modify, and delete User Profiles assigned to employees
- *Manager Profile* - The Manager Profile has the Employee Profile rights but may also be granted the ability to view certain data (e.g., leave information) for designated employees and to review/approve certain requests
- *Time and Attendance Profile* - Users with this profile can view, update, and approve employee time and attendance information and run specific reports

The Workforce Now Application integrates security functions that limit users to specific application functions and data views based on their assigned profile. The Workforce Now Application is configured with various audit trails of user IDs, time of access, and functions performed for certain sensitive areas. Clients can request audit reports to review changes made by user accounts including accounts assigned to ADP associates.

Essential Time Data Import Interface

Clients can use the Import Interface function to import data such as employee demographic information, accrual balances, and labor level data to the Workforce Now Application. Clients import data into the Workforce Now Application using text files exported from their payroll system. The Import Interface parameters are configured during the Workforce Now Application implementation and these parameters are specific to each client based on their requirements. Errors identified during the file import process are logged in an error log and are available for review by users with the Administrator/Practitioner profile. ADP associates that are part of the Implementation and TLM Service Center groups can also use the Import Interface to initially populate the client's database and to do mass updates to a client's database.

Data Validation

The Workforce Now Application is configured with data validation controls that validate data input. These data validation controls include edit checks, mandatory fields, drop-down boxes, and pre-populated fields that cannot be modified during data entry. Errors identified by the data validation controls are displayed on the screen for client review and resolution.

Data Transfer

Depending on the input mechanism, employee time and labor data are transferred to the Workforce Now Application using the following methods:

- *For clients that use time clocks* – A server with third party data-collection software and is configured with a custom Time and Attendance Application interface used to transfer information from the data-collection devices (clocks) to the Workforce Now Application.
- *For clients that use biometric devices* – A server with third party data collection software and is configured with a custom Time and Attendance Application interface used to transfer information from the biometric devices into the Workforce Now Application.
- *For clients that use IVR system*s – IVR servers provide clients with phone access to the Workforce Now Application phone system and enable time punch information to be added to the Workforce Now Application database in real-time.
- *For clients that use web-based Workforce Now Application* – The web-based Workforce Now Application transmits data to ADP over a secure TLS connection.

Enhanced Time Data Input

The Enhanced Time application supports both automated and manual entry of client time and labor data. Clients are responsible for data input to the Enhanced Time application regardless of the manner in which the data is entered. Time and labor data can be entered automatically through Extensible Markup Language (XML) transactions from various client managed data collection devices. Data can also be entered manually by:

- Direct application entry - Users log into the Enhanced Time application using a unique user ID and password and submit their hours using one of the following four options:
    - *Time Stamp:* Employees click on the time stamp button that captures the date and time from the web server and records that information on the employee's timesheet within the Enhanced Time application.
    - *Time Stamp with a Start/Stop Timesheet*: Employees use the time stamp button to enter the time arrived at work, the time left work, and any breaks taken during the day.
    - *Start Stop Timesheet*: Employee accesses their timesheet directly and enters the time they arrived at and left work.
    - *Project Hours Timesheet:* Employee enters their hours into a specific timesheet that is connected directly to a specified project that has been set up in the Enhanced Time application.
- Data import - Users log in to the Enhanced Time application using a user ID and password and use the ADP TLM Interface to import data, such as employee demographic information, accrual balances, and labor level data that is included in text files from their payroll system to the Enhanced Time application. The ADP TLM Interface parameters are configured upon implementation and are client specific.

During manual and automated XML data file import, the Enhanced Time application applies to edit checks to validate the completeness and accuracy of data as it is being imported. Data imported that does not pass the edit checks are recorded as errors in an application log file and is made available for clients to review and resolve. The Enhanced Time application also includes edit checks that are applied during manual data input through direct application entry. These edit checks include data format checks, mandatory fields, drop-down boxes and pre-populated fields that cannot be modified. If the edits do not pass, error messages appear on the Enhanced Time application screen to notify the user.

Regardless of whether the data was entered through direct application entry or data file import, data that passes the input edit checks is automatically updated and recorded in the Enhanced Time application.

The Enhanced Time application also generates activity logs capturing user input including user IDs, time of edit, and functions performed. The activity logs are available for clients to review at any time.

Payroll Input

Datapool

Datapool, a component of the Payroll Application, is the central repository for data received from any of the input systems. Data is held in Datapool until it is ready for processing. Datapool imports and retains information to be processed by the Payroll Application until polled by the PTCS. Once polled, the data is submitted to the next processing phase of the Payroll Application.

The Payroll Application receives client data input from two primary input methods:

- Automated Input (primary method) – For the scope of this report, the Workforce Now Input system is the primary method for clients to input their payroll data.
- Manual Input (secondary method – a small percentage of clients) – Clients communicate payroll data to ADP over the phone or send completed system-generated standard forms that contain payroll data via fax or courier. Once received ADP Data Entry (Teledata) operators manually enter the payroll information into the Payroll Application for processing.

Automated Input

Clients use the input system to enter and transmit their payroll transactions which are then automatically transmitted to ADP's Payroll Application for processing. This enables clients to enter and validate transactions and provides them more control over entering payroll information. When clients use the input system, the transactions are transmitted to the Payroll Application for processing through one of the following communication systems: ADP's EPC or AutoLink, or the MQSeries file-transfer system. These communication systems run on ADP's local area network (LAN) and periodically communicate with the mainframe's Datapool component through automatic interfaces. Built-in security features (e.g., encryption, user IDs, and passwords) enable clients to maintain the confidentiality of sensitive employee information. The input system also promotes efficient data entry by using edit checks that are applied when data is input. The edit checks also improve the accuracy of payroll data input prior to it being transmitted to the Payroll Application for processing.

The input system allow the client to enter payroll data on an ongoing basis, as information becomes available, enabling data-entry flexibility. The data is accumulated within the input systems, validated by the client, and held until the client elects to submit it for processing. Upon client submission, the data is automatically transmitted by the communication systems to the Payroll Application for processing. The data can be recalled by the client from the input System and edited at any time in the input system prior to transmission. The communication systems receive the data throughout the day and periodically transfers it into Datapool where it is held until processed.

Manual Input

Payroll Services clients can also submit payroll transactions directly to ADP Teledata operators by phone. Some Regions are able to receive client payroll information by fax.

Daily, Teledata operators review online call and fax lists. The call list contains the clients whose payroll input must be obtained that day. A Teledata operator calls the client contact at a pre-arranged time and obtains the payroll information needed for input. In some Regions, clients can call the Teledata operators directly. The caller must provide information that identifies them as an authorized Teledata client. The Teledata operator keys the payroll information into the Key-Fast system (a component of the Payroll Application), which performs a preliminary data verification known as “editing” that includes validations against various control databases. Page totals are verified with the client to verify that data is keyed accurately. Input received from Key-Fast is transferred to Datapool where it is held until processed.

Data Processing – Workforce Now

The Workforce Now Application track HR, leave, and recruitment information and calculate benefits eligibility and benefit deductions based on the plan information that has been configured according to client specifications. Clients are responsible for assisting ADP in maintaining the data for benefits administration processing, reviewing the results of the calculations, and comparing results to the source documents and data. The Workforce Now Application calculates eligibility and deductions based on the plan parameters that have been configured according to client specifications during initial or annual enrollment implementation, as well as the participant demographic data and elections. Clients are responsible for reviewing the results of the calculations, comparing results to the source documents and data, and addressing any errors and/or warnings.

Clients can also elect to have the Workforce Now Application connect to third party vendors. Three types of errors can occur in the Workforce Now Application when processing data for connections to third party vendors:

- Data Errors: When a connection runs, both a data file and a data error file are produced. The data file is securely delivered to the appropriate party (vendor, client, etc.). The data error file is delivered to a tab within the Workforce Now Application. The Comprehensive Benefits group reviews the data file and addresses and resolves any errors.
- System Errors: If a system error occurs while a connection is producing or delivering the file, an email is sent to a mailbox that is monitored by members of the Connection Services group. The system error is also recorded in the Connection Manager. If a job fails after attempting a manual restart, the Connection Services group creates a ticket to track the problem to resolution.
- Third party Data Errors: Most carriers will also produce error files; these error files are sent from the carrier to the Comprehensive Benefits group. A Comprehensive Benefits Analyst will review and resolve the errors received from the carrier. In some cases, the Comprehensive Benefits group may contact the client for assistance in resolving these data errors.

The Workforce Now Application translates the data that was entered into a readable format resembling an electronic time card. This employee time card data can be reviewed, edited, and approved by both the employee and the supervisor using the Workforce Now Application.

Client administrators/practitioners initiate the processing of data using the Workforce Now Application. The Workforce Now Application calculates employee time and attendance data, based on work and pay rules, such as rounding rules, shift guarantees, and exception flags (e.g., indicating missing punches, long shifts) that are configured according to client specifications.

The Workforce Now Application is configured to generate three types of payroll-related exceptions during processing. Messages and warnings are notifications to Supervisors and Administrators/Practitioners about a potential payroll problem related to the number of hours an employee charges. These exceptions do not, however, prevent the payroll from being processed. Errors are payroll issues, such as a missed punch, that prevent the payroll from being processed and require resolution by the client. The Workforce Now Application restricts clients from processing the current period and moving to the next pay period without completing payroll, time, and event management steps (e.g., pending events, payroll related exceptions, time pair exceptions) and resolving any errors identified in the steps.

Enhanced Time Processing

Once data has successfully been entered and recorded, the Enhanced Time application translates the data into a readable format resembling an electronic timecard. This data can be reviewed, edited, and approved by both the employee and the supervisor using the web-browser enabled application.

The application automatically calculates employee time and attendance data entered, incorporating work and pay rules that are configured in the Enhanced Time application. These rules include but are not limited to rounding rules, shift guarantees, and exception flags (e.g., red box indicating missing punches, long shifts) that have been configured according to client specifications. Clients are responsible for processing pay data, reviewing the calculation results, and addressing any errors and/or warnings.

The GETS US organization is responsible for monitoring the production processing environment supporting the Enhanced Time application. Site Scope, an infrastructure monitoring tool, is used to alert support staff of client environment issues. The GETS US organization uses the Service Desk system to document client production issues. Depending on the nature of the issue, the GETS US organization will either resolve the issue or dispatch a case to the Solution Center, Technical Services Group, and/or the Implementation group for resolution.

Outages are documented in the Service Desk system for major and unplanned outages (an outage that affects multiple client environments). The GETS US organization will contact the Solution Center, Technical Services Group, and/or the Implementation group and provides status updates periodically. The Solution Center is responsible for contacting and providing the clients with updates. The infrastructure monitoring controls are covered in ADP's GETS US Organization SOC 1 Report.

Data Processing – Benefits - Carrier Billing/Invoice Reconciliation and Payment

Comprehensive Benefits customers can choose to contract for the ADP Comprehensive Benefits Invoicing Services that consist of carrier invoice billing (for historical customers that contract under payment services). Invoices are produced in the Workforce Now Application using the invoice module. The invoices are finalized monthly, based on client and carrier schedules, and can be modified and customized based on client-administrative procedures. The procedures are developed from requirements defined during the initial client agreement and implementation.

Each month, participant information is extracted from the Workforce Now Application and provided to the client. This information includes the plan rate, active enrollment, and all changes to participant enrollments. The Workforce Now Application invoice module produces three reports; a Summary Consolidated Bill Report, a report listing all participants enrolled during the month (List Bill), and an Adjustment Report. All of these reports are used by the client to determine the amount owed to the carrier. Invoices are run and completed on a timeline established by the client.

Clients that contract for the invoicing service can be classified as having invoices in two categories. One client may have invoices in both of the below categories:

- <u>List Bill Carriers</u>: These clients use the carrier bill as the bill of record and pay the carrier based upon the carrier's statements. The Benefits Administrator assigned to the client will obtain a copy of the carrier's invoice for the month either as a paper copy of the invoice through the mail, or they can download an electronic copy of the invoice from the carrier's secure site. The Benefits Administrator performs a reconciliation by using the Workforce Now Application enrollment and adjustments within, to balance to the carrier bill. Variances are reported to the carrier on a Discrepancy Report by the service center's Benefit Representatives or Service Support Specialist and tracked internally in the Savvion BPM Tool. Clients can elect to receive a copy of the Discrepancy Report, and review and correct errors when requested either during implementation or throughout the client lifecycle. Credits or debits are based on the carrier records and appear on a future bill.
- <u>Self-Bill Carriers</u>: These clients contract with ADP and their carriers to have the Workforce Now Application be their bill of record and pay the carrier based upon the Workforce Now Application data. Summaries, adjustments, and list bills are processed, and monthly invoice information is sent to the client. The benefits administrator performs reconciliations at least annually by using the Workforce Now Application enrollment and change data to balance the application data to the carrier bill or the carrier's census report. Any variances are reported to the carrier on a Discrepancy Report and tracked internally in the Savvion BPM Tool. Carriers report credits or debits to the benefits administrator who manually adds the information to the next month's bill as an adjustment. The self-bill reconciliation may only be performed if the self-bill carrier either creates invoices or maintains participant-specific census data.

ADP is responsible for working with the carriers on the clients' behalf and ensuring errors listed in the Discrepancy Reports sent from ADP are resolved. Clients with List Bill and Self-Bill carriers pay each carrier on the invoice themselves. There are a limited number of clients that contract ADP Comprehensive Benefits to pay the invoices on their behalf. Once the invoices and necessary reconciliations are completed, the benefits administrator can create a consolidated monthly bill for the client that includes payment amounts by Carrier/Plan. The consolidated monthly bill workbook is applicable to clients who have List and/or Self-Bill carriers. The Consolidated Bill workbook includes a summary sheet and a separate tab for each carrier. List Bill carriers will include the client bill as a separate tab, with participant-specific details as provided by the carrier. Self-Bill carriers will have a summary by category for the premiums due, with no participant-specific details.

If the client with List Bill or Self-Bill carriers have selected ADP to pay the invoice, the Benefits Administrator forwards this to the "WFNBA IA Finance" queue for processing. Finance then processes the payment request using the Chase Access Next Gen application accessed through ADP Treasury. Access to the Chase Access Next Gen application is limited to ADP Finance Department associates and is accessed with a user ID, password, and token. The Chase Access Next Gen application is configured to segregate personnel who can initiate and release payments. The Finance Department processes an Electronic Funds Transfer ("EFT") from a bank account designated by the client to an ADP bank account for the total monthly premium amount (total payment amount) due to all carriers. The Finance Department schedules ACH transactions for the premium amount to each respective benefit provider. Records of EFT and ACH transactions are maintained in ADP Treasury records. An electronic version of the Consolidated Bill serves as supporting documentation for each funds transfer.

Data Processing – Benefits - Client Maintenance and Open Enrollment Services

Comprehensive Benefits Clients

Open Enrollment ("OE") is the annual period when Comprehensive Benefits clients and the clients' participants are given the option of adding, deleting, or modifying their benefit plans. It allows clients and their participants the opportunity to make changes to their current benefit elections without experiencing a qualifying event (e.g., the birth of a dependent, marriage).

A Benefits Solution Specialist ("BSS") sets up a conference call with clients to review the OE process with them (PowerPoint presentation reviewed detailing the steps in the OE process and process performers roles and responsibilities) at which time another call is scheduled to discuss and gather information on any upcoming benefit changes (this may require multiple calls to collect all of the information needed). After the calls, the completed Open Enrollment Questionnaire is sent to the client detailing all changes discussed for their review. A formalized Planning Recap can be sent in place of the questionnaire detailing changes discussed during the calls as well. Any additional rate information needed to complete the system configurations will be emailed to the Annual Enrollment Specialist ("AES") or updated in the rate tool by the client. This client correspondence and client-specific detail is retained in the Annual Enrollment Organization Nucleus ("AEON") tool (open enrollment profile prior to November 2016). Once all changes have been confirmed the AES can begin the system configurations. The AEON tool is updated to capture the delivery method and dates based on the information gathered during the questionnaire phase.

A Benefit Plan Summary is produced after the client's data has been updated in the Workforce Now Application. The Implementation staff, the AES, the Relationship Manager or Client Lead and the client performs a Quality Assurance audit of all changes made to plan data on the Benefit Plan Summary. Once the correct plans, rates, and eligibility are configured in the Workforce Now Application, the OE period begins and participants can make their elections via the internet or through the Employee Service Center ("ESC"). During the AE window, the Service Support Specialist will review a test confirmation statement with the client to validate the information that will be generated on the confirmation statements distributed to employees. A payroll test file is also created to review deductions are calculated correctly based on enrollment selections. These documents and details are updated and retained within the AEON tool. After the enrollment period closes, ADP's QA team runs reports to verify that participants entered valid elections. If there are errors, clients work with the Service Support Specialist and Open Enrollment Specialist until they are resolved.

The confirmation statements for each participant are then produced from the Workforce Now Application and a proof of the merged confirmation statements are reviewed and approved by the client. Once reviewed and approved, the fulfillment center prints and mails the statements to the participants. The printing and mailing of confirmation statements by ADP for Comprehensive Benefits clients is an optional service and outside the scope of this Description.

Flexible Spending Account (FSA) Clients (Off-cycle)

Clients that renew their medical, dental, or vision plans during the normal OE process, while renewing their FSA plans outside of the normal AE process are considered 'off-cycle' clients.

FSA plan limits are governed by the IRS and the limits are communicated to clients annually, via a client alert, once they have been released by the IRS. The client alert is stored on the 'support.adp.com' website. The BSS will coordinate a meeting with the client to discuss the new FSA limits and whether the client intends to change carriers. FSA limits in client OE profiles are updated in the Workforce Now Application o, according to IRS guidelines, by Open Enrollment Specialists. Upon acknowledgement of the FSA limits, if the client discloses there is no change in carriers, the client's OE profile is updated in the system with the new FSA limits. If the client discloses a change in carriers, a new record in the client's OE profile is made reflecting the new carrier and new FSA limits. Once these changes are made, the client is notified by the AES of confirmation of what was set up and configured in the Workforce Now Application.

SaaS clients

SaaS clients do not contract with ADP for Open Enrollment services and are responsible for processing their benefits plans and participant elections.

Data Processing - Payroll Deductions and Tax Withholdings Specifications

The Payroll development team currently leverages the Agile methodology to develop and complete Payroll STAT File Maintenance changes. The specifics of this Software Development Life Cycle (SDLC) method are described in the following sections.

The Payroll Application tax-withholding rate modules are maintained in the STAT database. The STAT File database feeds the statutory and quarter/year-end modules and is used during payroll processing for tax rate information based on client company code and employee number.

The Payroll Statutory Kanban team maintains the STAT File database. Statutory Research Shared Services personnel make ongoing inquiries about, and obtain information concerning, requirements and pending and enacted legislation that can impact the following payroll tax issues, some of which, but not all, are housed in the STAT File database: tax withholding calculations, quarter and year-end forms, fringe benefits, magnetic media/electronic-filing specifications, new-product statutory requirement, wage garnishments, new hire reporting, state unemployment wages, and taxability rules.

Statutory Research Shared Services monitors statutory changes for payroll-related taxes for both U.S. and Canadian taxing authorities at the following levels: federal, state, local (city) and county, Canadian provinces and territories, and U.S. territories and commonwealths. In conducting statutory research, the Statutory Research Shared Services group uses contacts, and maintains evidence of each contact for tracking purposes, at relevant government agencies, various online and hard-copy publications, relevant Internet web sites, Internal Revenue Code and Regulations, payroll trade and other relevant association newsletters, attendance at industry and government conferences, and participation in service bureau consortiums.

Upon identification of a statutory change, the Statutory Research Shared Services Group creates a Feature tracking item in the Rally software. The Feature includes details obtained from the Work in Progress (WIP) item used for monitoring and indicates that an actual statutory change was issued. The Statutory Project Manager then creates a “Development” Feature tracking item in the Rally Software, which is assigned to a Business Analyst on the Payroll Statutory Kanban team. The Business Analyst is responsible for prioritizing, analyzing, and scheduling the statutory item, based upon the effective date of the statutory change. Identifying the Payroll Application impacts (e.g., STAT File, quarter, client, region), and creating “User Stories” in the Rally Software to be used for further research and development of the proposed change, is also the responsibility of the business analyst.

Each user story has a developer, tester, and documentation specialist assigned. Elaboration sessions are held to review story content and apply revisions as needed. The assigned business analyst, developer, tester, and documentation specialist participate in elaboration. After elaboration is complete, development occurs, followed by testing and certification. Certification and acceptance of the statutory change by the Payroll Statutory Kanban team tester signifies that the STAT File database updates are ready for deployment. Daily meetings are held by the Payroll Statutory Kanban team's Scrum Master to discuss the status of each feature and user story. The Rally software Kanban Board, a point-in-time view, is used to track the status.

The Statutory Project Manager holds a weekly tracking meeting to discuss the status of time-sensitive open statutory changes not yet released to the Regions. The Tracking Report, a point-in-time report, lists open tracking Features and the WIP report that lists potential or work-in-progress statutory items monitored by the Statutory Research Shared Services Group, are reviewed during the tracking meeting.

Statutory changes are implemented based on the details provided in the feature and User Stories. For changes that do not require code modifications, the STAT File database updates are entered directly in the STAT File database. For changes requiring coding modifications, these follow the standard change management process described in the *General Computer Controls* section of this Description.

Logical access to the STAT File database is limited to authorized personnel who login using their mainframe user ID and password. The process and controls for STAT File database access follows the Logical Security process described in the *General Computer Controls* section of this Description.

Data Processing - Payroll

Processing is divided into two phases: EDIT and NET/CALC. ADP uses the Payroll Application's PTCS to track, control, and monitor the results of each processing phase. PTCS controls the processing of data from Datapool through NET/CALC processing. Using online screens, individual Regions can define processing parameters based on their individual requirements, including the length of time data can accumulate before being transferred to the next processing phase. PTCS also provides online inquiry to track the status of the individual payrolls that are being processed by the Payroll Application. PTCS also provides online control totals and daily production statistics that are used to track and monitor Payroll Application processing activities.

EDIT Processing

EDIT is a Payroll Application program, managed by PTCS, that automatically collects and processes payroll data received from Datapool.

During EDIT processing, the program automatically compares the payroll data received from Datapool with the EMP to verify information such as employee numbers. Four error levels are used to evaluate the comparison: 1) Syntactical; 2) Relational I; 3) Relational II; and 4) Relational III. Syntactical checks verify syntax for propriety. These relational levels provide more detailed edit checking based on error complexity. The rules are stored in the Batch Edit Rule Database and changes follow the ADP change management process. The EDIT program then flags payroll data as: Ready for Edit, Ready for NET/CALC, Error, and Ready for Reprocessing. The Editing Group reviews payroll data flagged as 'Error' and if they cannot correct the error, the Client Services group is notified. The Client Services Group then contacts the client to resolve the error. The Editing Group may contact clients directly to resolve errors.

Once EDIT errors are corrected, the program communicates the payroll data status to PTCS as 'Ready for NET/CALC' and the next processing phase, NET/CALC, starts.

The EDIT processing phase produces one output from the CUI database file. This file maintains payroll information on a company level and is used to support the NET/CALC process and remains on the Payroll Application for a defined amount of time as specified by the individual region. The CUI information is retained so the region can rerun a payroll if necessary.

NET/CALC Processing

PTCS moves client payrolls flagged as Ready for NET/CALC processing from the CUI database file into NET/CALC. Once moved, the NET/CALC processing phase calculates the current payroll and updates the EMP based on client-defined payroll schedules. Payrolls requiring immediate processing are referred to as "Hot" payrolls and can be flagged by ADP's PTCS personnel to prioritize their processing.

The NET/CALC processing phase uses client options that reside in the CCI database to determine how variable routines such as calculating gross earnings, providing credit for vacation, holiday and sick time, taking voluntary deductions and other such matters are to be handled. Clients are responsible for providing the data used to configure their options in CCI upon implementation and for communicating updates to those options to ADP in a timely manner.

If a client submits changes for company or EMP items, the changes replace the previous EMP entries. The NET/CALC process takes the input data for each employee, refers to the EMP record for items such as the employee's earnings rate, tax status, and authorized deductions, and calculates the gross earnings, voluntary deductions, and net pay. The STAT File houses tax rate and formula information. Using the Payroll Application's Statutory database (STAT File) NET/CALC calculates taxes and year-to-date balances for gross earnings, federal, state and local income tax, social security deductions and goal amounts. The NET/CALC process reformats the Payroll Application data into a readable format that is ready for additional processing during the WRAP processing phase.

Monitoring of Processing Activities

The M&MTAM Technical Support and the Command Center staff use automated tools to continuously monitor the status of the scheduled jobs (e.g., transmissions, NET/CALC and EDIT jobs) and to alert the staff about job failures. This process is covered as part of the ADP GETS US Organization SOC 1 Report.

Data Output – Workforce Now

Workforce Now Application Reports

Majority of the financial reports that are provided to clients as part of the Workforce Now Application are either customized or are parameter-driven reports generated directly from the Workforce Now Application. In all cases, the completeness and accuracy of these reports is the responsibility of the client. These reports include employee benefits, reconciliation, plan description, and comparison reports. The Workforce Now Application will automatically generate error messages to notify users if there are problems related to generating these reports.

Output Data Files

The Workforce Now Application also produces output files either directly to the client, a third party vendor, or to another internal ADP system. The completeness and accuracy of these output data files is tested during client implementation, further modifications require client testing and would follow the relevant logical access and program change controls described below. The following is a brief description of the relevant data file outputs:

- Carrier Interface Files: This file contains all of the updated employee demographic, benefit, and dependent information processed during the current cycle. The carrier reporting process creates and sends a file directly to the carrier.
- Payroll File: This file is produced every pay cycle, the payroll file contains benefit deductions and any stop transactions that are sent for discontinued benefits. The results of the payroll file run are posted in the Workforce Now Application and it is the client's responsibility to upload the file to their payroll system if they are not automatically sent to one of ADP's Payroll Services.
- FSA (Flexible Spending Accounts) Interface File: This file has information on each employee (such as their name and address) and their FSA election (Health Care Account and/or Dependent Care Account). Flexible Spending Accounts information is sent either to ADP's Flexible Spending Accounts services, the client, or the client's FSA Administrator depending on the client agreement.
- COBRA (Consolidated Omnibus Budget Reconciliation Act) Interface File: This file contains information on employees and, if applicable, their dependents with COBRA qualifying events. ADP's COBRA services or the client's vendor process this file depending on the client agreement.

The connection files are transmitted to ADP internal systems and third party systems based on parameters that are set within the scheduler. The Connection Services group is responsible for scheduling automated transmissions and monitoring the transmission status to verify the completion of the file transfer. The data files can only be accessed by authorized associates that request and receive approval.

Essential Time Reports

Clients can use the Workforce Now Application to produce a variety of standard reports including employee accruals, user configurations, timecard exceptions, individual schedules, and employee time card details. Client users that have Supervisor and Administrator/Practitioner profiles have the access needed to generate the standard reports upon demand. The Workforce Now Application is configured to display error and warning messages related to the status of report generation requests.

Essential Time Output Files

At the end of each pay period, clients can use the Workforce Now Application to export calculated and approved employee data. During the pay data export process, the application displays export status error and warning messages to the user. The error and warning messages are recorded in an application error log for review. Clients can use the export files to upload pay data to their HR or payroll system for tax and benefits deductions and payment processing.

Enhanced Time Output

At the end of every payroll processing cycle, clients can export the calculated and approved employee data from the Enhanced Time application into output files. Clients can transmit these output files to their HR and payroll systems for appropriate tax and benefits deductions and payment processing as follows:

- *For any HR and Payroll system* - Clients download the files using the ADP TLM Interface and manually transmit the files to their HR or payroll system.
- *For clients that use the ADP Hosted Payroll system* - During implementation, clients can specify the ADP network path to copy pay files generated from the ADP TLM Interface. The client downloads the file created to their local hard drive to allow them to import the file into their payroll application for processing.

System Reports

Clients can use the Enhanced Time application to produce a variety of reports. The following table presents the list of the standard financial reports provided to clients:

Report Name(s)	Description	Source and Preparation
Pay Data Export File	Files containing calculated and approved employee data that is exported from the Enhanced Time System at the end of every pay period in the format that is required by the client's HR or payroll system.	System client-initiated
Timecard Audit Trail Report	Standard report that displays audit information related to specific timecard editor actions including the date/time of the action, who performed the action and what information changed.	System client-initiated

The user's ability to view and generate any of these reports is based on access privileges, assigned in the employee's role that is determined by the client administrator.

Comprehensive Payroll Output

With Comprehensive Payroll, ADP handles the everyday payroll administration and compliance tasks from the client, including entering payroll data into the Workforce Now Application on behalf of the client.

Clients can make requests to Comprehensive Payroll service which are documented in a ticket. These features include:

- Stop Pay Requests – request for payroll stops can be made by clients using ADPCheck and TotalPay option.
- Pay Reversals – request for ACH transfer to be reversed for direct deposit transactions by clients using ADPCheck and TotalPay option.
- Payroll Amendments – request for amendments to fillings will be verified by the Comprehensive Payroll team for accuracy and will not move forward until the client has approved the changes. The payroll is flagged as an amendment in the Workforce Now Application.

Once any of these requests are processed the Comprehensive Payroll Associate sends a confirmation to the client contact indicating the changes have been made.

W-2 Preview

At the end of the second month of each quarter a W-2/1099 Authorization Release Case Template will be sent to each client asking for wage information updates. Upon receipt of information, Comprehensive Payroll associate will enter the information into the Workforce Now Application to release W-2 forms to clients. Once the form is released a confirmation email is sent to client contact informing them the W-2 release was processed. The W-2 forms are then printed and mailed to the client in compliance with specified IRS deadlines.

Payroll WRAP Processing

Upon completion of the NET/CALC process, the WRAP process is kicked off to produce multiple outputs. The primary Payroll Application outputs are categorized into one of the following: Pay Statements, Reports (printed and electronic), and Data Files (e.g., files for other ADP systems, Money Movement/Direct Deposit Files).

Payroll Pay Statements

Payroll Application outputs, categorized as pay statements, that are physically printed and distributed to clients are:

- *Checks (including ADPChecks)*: Printed with the net paid amount preceded with asterisks. The earnings statement provides a comprehensive record showing the elements of gross pay (e.g., hours and rate), payroll taxes and deductions and year-to-date totals. Company check control totals are provided to verify the number of checks issued, the first and last check number used, and the total dollar amount of the checks printed.
- *Vouchers*: Similar to checks in both information content and control procedures. Vouchers are produced for employees who elect direct-deposit. “Non-Negotiable” and “This Is Not A Check” are clearly indicated on the voucher.
- *Non-Negotiable Laser Check*: A voucher-like notification provided to employers who pay their employees in cash. The document provides the employees a net-pay amount and a comprehensive earnings statement.

Design characteristics in ADP’s payroll checks and stubs provide security protection against color copy and scanner duplication systems. The checks include an intricate encoding pattern within high-resolution borders that become distorted when duplicated. In addition, the background of the checks uses a multi-tone shade over a cascading building block design (prismatic printing) that is difficult to accurately reproduce and the shading accentuates the word “VOID” when the check is copied. On the reverse side of the check, a unique printing pattern of multi-width lines embedded with encoding marks has been added to protect the document from scanner duplication. In addition, ADP’s check design uses a number of sophisticated features that includes:

- Thermochromic ink that provides a heat-sensitive ADP logo and ADP watermark to verify the authenticity
- A unique control number on pre-numbered check stock that uses special ink to improve tracking

Checks are produced on laser printers with a Graphics Handling Option. If a paper jam occurs during check printing, most printers reject damaged checks and continue to print where the jam occurred and the printer notes where the error occurred. Operators visually scan the jam point for proper sequencing, possible duplication, or additional damage. Rejected checks are subsequently moved to a holding area. The printer reprints the checks that the operator removed from the jam point. Other printers automatically insert a pink sheet of paper at the point where the paper jam occurred. The operator removes the damaged checks from the printer paper path and the printer automatically reprints the checks that the operator removed and marks the point of duplication with a pink sheet. Some Regions use Quality Assurance (QA) to inspect the laser-printed paper sheets both preceding and following the inserted pink sheet of paper to identify any duplicate checks.

For clients that have requested to have checks and vouchers stuffed in envelopes, the operators use envelope-stuffing machines. Checks that are not stuffed inside envelopes are wrapped in rubber bands and forwarded to the Quality Control group.

The envelope-stuffing machines provide a total count of the number of envelopes stuffed and detect checks that are duplicates or out-of-sequence. Each check and voucher page has an encoded page number. Some Regions incorporate additional parity checks to verify odd and even sequences. Two sequential odd or even checks indicate a potential error. Operators review identified error messages and resolve identified issues promptly.

If checks are damaged during the printing or stuffing process, the operators deface or destroy the checks in a controlled manner. Operators maintain a record of damaged checks that is forwarded to QA and/or banking personnel to alert them of potential duplicate or missing checks.

Quality Control personnel review payroll reports checks and vouchers for defects as they package them for delivery. Quality Control personnel are restricted from having access to modify the pay statements within the Payroll Application and Operations Center System. If QA personnel discover a problem with a printed payroll (e.g., wrinkling, tears, or smudges), a rerun, or reprint, may be scheduled.

Payroll Reports

In each region, the CSSs are responsible for setting up and maintaining clients' reporting requirements and schedules in MR 2000. MR 2000 enables report customization and generation. Reports can be printed or made available electronically in PDF format through ADP's iReports system, depending on client requirements. The following table presents a listing of the standard reports available to clients to support their financial reporting requirements:

Report/File Name(s)	Description	Source and Preparation
AutoPay Master Control (AMC)	Report of employee's master records consisting of employee personal data, scheduled deductions, Year-to-Date (YTD) accumulations, tax status data, and key data for current payroll.	Automated from the Payroll Application through WRAP batch processing
Payroll Register	Reports current payroll-cycle data by employee including hours, earnings, statutory and voluntary deductions. Shows totals by department and company levels.	Automated from the Payroll Application through WRAP batch processing
Unused Deduction Report	Reports employee-level deductions that were not applied in the payroll because of insufficient earnings.	Automated from the Payroll Application through WRAP batch processing
Payroll Audit Report	Reports key payroll statistics such as: list of employee changes processed by ADP, control totals, and unusual payment entries.	Automated from the Payroll Application through WRAP batch processing
Payroll Summary	Reports hours and earnings by department or cost level, taxable wages by category, and deductions.	Automated from the Payroll Application through WRAP batch processing
Labor Distribution Report	Provides the same data as the Payroll Register but is summarized at a sub-employee level (e.g., by job).	Automated from the Payroll Application through WRAP batch processing
Statistical Summary Report	Reports summarized payments to taxing jurisdictions and money impounded from clients' bank accounts to fulfill tax and money-movement obligations for the payroll being reported.	Automated from the Payroll Application through WRAP batch processing

Delivery of Printed Reports

Printed pay statements and reports are packaged in a sealed bag and delivered to clients by insured third party couriers or by common mail/delivery carriers according to the clients' delivery requirements.

ADP regions use the Operations Center tracking tool for delivery tracking and validation purposes. The tracking tool provides printed output and media distribution process visibility using a web-based software package, as well as uses multi-vendor interfaces and delivery-management tools to support the service delivery environment. Clients are responsible for notifying ADP of any issues with the delivery of printed reports.

Delivery of Electronic Reports and Pay Statements (e.g., iReports files)

The data used to create printed output, such as pay statements, is converted to a PDF format that is transmitted to the iReports system through FTP over ADP's ESNet. Clients can access the electronic reports in iReports by providing a user ID, password, and/or digital certificate. The iReports system uses SSL technology with 256-bit encryption to provide for the security of the transmitted data.

Payroll Data Files

Upon successful completion of a payroll run, the Payroll Application automatically produces a series of payroll data files that are either used by other ADP systems or transmitted back to the input system for client access and viewing. The primary data files consist of:

- Other Payroll Related Files – These output files consist of electronic payroll registers, year-to-date, AMC, and any other custom client reports that are transmitted from the Payroll Application to the input system for clients to view, download, and/or print.
- NAS ADP GL and MAS GLI Files – These output files contain payroll data in a pre-formatted general ledger file that is transmitted to ADP's NAS ADP GL or the MAS GLI products using MQSeries middleware.

Data Output - Payroll (Money Movement/Direct Deposit Files)

Money Movement/Direct Deposit Files

The Payroll Application produces money movement and direct deposit files and transmits them, for clients that have elected Full Service Direct Deposit (FSDD) or a regular Direct Deposit option as follows:

- Transmission to Financial Institutions or Bank Service Processors: Regular direct deposit information is transmitted directly to individual banks via an Automated Clearing Houses (ACH) transfer.
- Transmission to ADP's CAPS service: FSDD and ADPCheck information is transmitted to ADP's CAPS system and is then processed by the ADP Payroll & Tax Center. ADPChecks are printed in the Regions. ADPCheck data is sent to CAPS for positive pay reconciliation purposes. After processing, CAPS transmits FSDD ACH files to partner banks.

Transmission to Financial Institutions or Bank Service Processors

Upon completion of payroll processing, the direct deposit payment information is written to a separate file and stored for transmission to the appropriate recipient for clients who use the regular Direct Deposit service. Regular direct deposit information is transmitted primarily to banks using ADP's Electronic Transmission System (ETS) system that is supported and maintained by CAPS. For ADP clients that elect Regular Direct Deposit, client management is responsible completing their agreements and authorizations with their individual banks and for providing the required banking information to ADP.

The Banking Services Group receives daily reports indicating which payrolls have run and which are awaiting transmission to a specific bank. Banking Services use the Payroll Application's ACH Load Control Recap screen that lists the banks that are to receive transmissions and the total monetary amount of each transmission.

Banks can receive or retrieve direct deposit files. The Banking Services Group uses ETS transaction screens to review the status of bank transmissions and contacts daily. The review is done via phone or Voice Response Unit (VRU) for each bank identified online by ETS, as required, to support direct deposit transmissions.

Some banks receive transmissions from ADP and send transmissions at a certain time during the day. If this is the case, the direct deposit file transmission is also automatic. Other banks prefer to log into ADP's ETS system and collect their direct deposit files. Files can be transmitted from ADP to banks via FTP using a VPN and Triple Data Encryption Algorithm (3DES) encryption, over a dedicated circuit or via a dial-up connection, depending on the particular bank's requirements. Many banks communicate with ADP's ETS system using the "Connect Enterprise" system, using an electronic region ID and a login record for authentication purposes before establishing a session. After the transmission, ETS indicates that a file transmission was completed successfully.

The Financial Service Centers' Banking group confirms by telephone, VRU, or fax, (depending on arrangements made with the bank) whether the bank's total number of payments and the total monetary amount of the debits and credits received agree with ADP's totals, and records that the transmission was confirmed in ETS. Unsuccessful transmissions are re-transmitted until correct.

Transmission to ADP's CAPS

Clients electing FSDD services must complete an authorization form (e.g., the "Client Account Agreement") that is reviewed and approved by ADP and authorizes the payroll data files to be transmitted from the Payroll Application to ADP's CAPS service offering.

ADP's CAPS Service Center reviews and approves these forms. ADP creates the National Automated Clearing House Association (NACHA) master file information and upon bank approval of the NACHA transmissions, clients and their employees may wait for a specified period of time known as a pre-notification (pre-note) period before the direct deposit process is activated.

For clients electing FSDD, the Payroll Application automatically generates money movement files and transmits them to ADP's CAPS processing center. Banking Services personnel review transmission status several times throughout the day and compare the information available on the Payroll Application to the information available on ADP's CAPS systems to confirm transmissions were processed successfully and to identify any exceptions. Identified discrepancies are followed to resolution.

The CAPS process and controls are not in scope of this report and are covered in ADP's TotalPay Service System and TotalPay Service and PayCard System SOC 1 reports.

Payroll Data File Transmission Monitoring

The following groups monitor the status of data file transmissions to check for completion of the transmission and distribution of the output files:

- The Regional Prelist teams works with Regional LAN Services to monitor input data transmissions from the input System to the Payroll Application and data transmissions between ADP entities.
- The Micro Tech Support (MTS) group monitors the status of file transmissions between the input system and the Payroll Application based on MQSeries status notifications.
- The Corporate Systems Engineering Group monitors the status of the transmissions of the iReports files from the Payroll Application to the iReports system by reviewing FTP system logs.
- The Corporate InfoLink Group monitors the status of the transmissions of the general ledger files from the Payroll Application to the NAS ADP GL and MAS GLI systems based on MQSeries status notifications.
- The Banking Group monitors the status of money movement transmissions and direct deposit files from the Payroll Application to the clients' banks or ADP's CAPS system.

These groups document identified issues in problem management systems and take action to resolve identified issues promptly.

GENERAL COMPUTER CONTROLS

General computer controls establish the control environment in which computer application systems are developed and operated. Therefore, the general computer control environment has an impact on the effectiveness of controls in application systems. The following describes the general computer controls related to the System.

- Information Security
- Logical Security
- Application Development and Change Management
- Problem Management

Information Security

Information security encompasses those controls that prevent and detect unauthorized access to information resources. This includes physical access to facilities as well as logical access to information systems. The primary goal of information security is to restrict access to application programs, online transactions, and other computing resources to authorized users.

All Information Security Policies are on the ADP Intranet, and provide overall guidance for data security administration, use of third–party software, virus protection, and internal/external user security. These guidelines provide a minimum–security baseline and apply to all ADP business units.

Logical Security

Network Access

ADP's GETS US organization is responsible for the overall security administration and architecture of the ADP's trusted network infrastructure (ESNet and LANs). These controls are covered in ADP's GETS US Organization SOC 1 Report. Certain network logical access controls are standardized and apply to all Employer Services business units. Common ESNet logical access controls including Active Directory access authorization, access revocation and reviews, and administrator access are included in ADP's GETS US Organization SOC 1 Report.

Enhanced Time Application Layer – Security Management Services (SMS) Access Administration

Each client electing to use the Security Management Services (SMS) tool (which provides access to Enhanced Time via the ADP Portal) has an assigned SMS Security Master that is set up during implementation. Security Masters are responsible for managing and configuring access security options for client personnel, ensuring only authorized employees have access to view and modify client data.

To manage and configure client user security options for SMS access, Client Security Masters are provided with access to the SMS tool. SMS provides single sign-on capability for user authentication or can be configured for separate configuration and authentication. Within SMS, both the Client Security Master and Client Security Administrator roles are designated by the client. The Client Security Master can assign security roles to other lower-level security administrators within their company, including Client Security Administrator, Client User Master, and Client User. The Client Security Master and Client Security Administrator profiles can be granted the ability to modify authentication options for client users to gain Portal access to various ADP products. All four of these profiles are configured to administer individual user accounts including issuing personal registration codes. Client administrators authenticate to SMS using a combination of password authentication and required cookies (ARCOT tokens) that are installed on the user's machine. All SMS client users must authenticate using a unique user ID and a password that requires features including forced password changes, password complexity, and password history.

Client employees are identified by a combination of a registration code provided by ADP to the client and personally identifiable information (the required information is configured by the client's security master or client's security administrator within SMS). Registration codes can be company-specific codes or they can be Personal Identification (PIC) codes which are individually generated by the client security profiles and sent to employees for registration and authentication with the employee portal. Upon new client employee registration, employees are required to activate their account via Identity Verification options configured by the Client Security Master/Admin in SMS. Additionally, users are required to establish a unique password upon registration.

Upon successful login to SMS, client employees can view or update information based on the ADP products that the client has purchased or contracted. To gain access to the application, the employee's information must have been successfully loaded via HRIS, a payroll indicative file or real-time transaction. Employees who are not set up with a user account in Enhanced Time cannot access the application.

Enhanced Time Application Layer – Security Management Services (SMS) Access Administration – ADP Personnel

Additionally, ADP personnel can request access to Enhanced Time via SMS in a support role. For provisioning of access, only an authorized Service Center administrator can create SMS access for ADP associates. For ADP associates, user accounts can only be created in SMS upon receipt of an authorized request submitted through a CRM ticket. Once the account is created, roles are assigned to the account that grants access to view client data and to directly access the Enhanced Time application. The assigned roles determine each user's level of access to the tools and associated environments. The ability to assign Enhanced Time SMS roles is limited to authorized users based on job responsibilities.

For terminations, a request is sent to the GETS US organization to revoke the user's SMS access. Depending upon the circumstances, the associate's SMS user account is revoked immediately or on their effective termination date. Terminated users can no longer access the Enhanced Time application client environments via SMS once access has been removed.

Enhanced Time Application Layer – Security Administration - ADP Access to Client Environments via the MOTIF Account Request Tool

Authorized ADP associates requiring access to the Enhanced Time Application client environments for maintenance and support purposes can request temporary access via the MOTIF Account Request Tool.

A defined process is in place to add and delete ADP support-user access to Enhanced Time client environments. To access the Enhanced Time application client environments, ADP support personnel must have a valid AD user ID and password. The GETS US organization is responsible for managing the AD user IDs requested by designated TLM department contacts using the Access Control List (ACL) dashboard. The ACL dashboard is an internally-developed application running on servers hosted and managed by the GETS US organization.

For new hires to gain access or to remove access for terminating personnel, the designated TLM contacts must submit a request through the ACL dashboard to the GETS US organization.

A limited number of ADP personnel are granted ACL dashboard access to submit requests to add/delete AD user accounts. When a request has been submitted through the ACL dashboard, it is assigned to the GETS US organization for processing. If granted access, the user's credentials are sent to the new user in a separate email.

The MOTIF Account Request Tool is used to manage the accounts of ADP associates that have access to client environments. This custom program was developed by the Technical Services Group and runs on management servers hosted at ADP's GETS US organization data center facilities. The MOTIF Account Request Tool reserves a configurable number of licenses to the Enhanced Time application per client environment for use by ADP personnel. The accounts of ADP associates are assigned to the Enhanced Time Super User Account Admin profile which has full access to application functions and data. The Technical Services Group is granted administrative-level privileges to support the management of the MOTIF Account Request Tool.

ADP associates go through a two-step process to access the Enhanced Time application via the MOTIF Account Request Tool:

- Login to a hosted management server using a unique AD user ID and password to access the MOTIF Account Request Tool.
- Select the client environment that they need to access and request a login that temporarily assigns one of the reserved licenses to the user ID using a temporary password. Their AD user ID is used for the application login and provides the ability to identify the user.

- On a nightly basis, all temporary accounts are deactivated through a configuration setting in the MOTIF tool.

A limited number of supervisors in the TLM group have individual account access to a Super User account to client environments. Access is only used in the event that the MOTIF Account Request Tool is not functioning correctly due to a configuration on the client environment.

The MOTIF Account Request Tool provides a dashboard functionality that allows managers to have visibility into the temporary access requests made by their employees. On a monthly basis, a TLM administrator sends an email to the managers to initiate the review and requests the managers to review the temporary access requests within the tool and document their approval or rejection. If a manager does not respond by the date requested the MOTIF Account Request Tool is configured to disable the access until the manager provides the requested approval.

If a manager does not respond or responds negatively (rejects the access request), TLM management conducts a review of the activity performed by the individual in the specific client for which the access request was made to determine whether any unauthorized activity occurred.

Each month Technical Services Group management selects a sample of three clients that appear on the Super User Account List and generates an ADP Timecard Audit Trail report for each of the three clients. If edits were made by an ADP user account, the report lists the date, time, and type of edit(s) reflected in the client's timecard data and which ADP user account made the edit(s). Technical Services Group management inspects the modifications to client data for appropriateness and follows up on any suspicious activity.

Client access to the Enhanced Time Application is authenticated through the Workforce Now Application.

Terminations

For terminations, an ACL request is sent to the GETS US organization to revoke that user's AD access. Depending upon the circumstances, the associate's AD user ID account is revoked immediately or on their effective termination date. Terminated users can no longer access Enhanced Time application client environments once access has been removed.

Enhanced Time Application Security

Enhanced Time application security is the responsibility of each client's named security administrator. This includes ADP associates who have been granted direct access to a client's Enhanced Time application instance.

Every Enhanced Time application user is associated with a specific role and security group(s). A user's assigned role and defined security group(s) determines the application functions a user can perform.

- Enhanced Time Employee Professional: user can enter time worked by directly authenticating to the application. Clients can assign access permissions to the employee profile that relate to time entry, timecard editing, and report generation.
- Enhanced Time Manager: user can edit the timecards for a designated group of people and can perform other managerial functions in the application. Clients can also configure the Enhanced Time manager role to also restrict or allow time entry, editing timecards, generating reports and workflow notifications, modifying system settings, and accessing system information and log reports.

Direct Database Access

Authorized ADP associates requiring direct database access to Enhanced Time client data for maintenance and support purposes can access the client database via the following methods:

- Enterprise Integration Manager (EIM) – EIM is a tool used to facilitate the transmission of data to and from the Enhanced Time application.
- Various Database Utilities (e.g. SQL Plus, SQL Developer, Oracle Enterprise Manager) – Access via database utility is used for client support personnel requiring direct access to client data for support responsibilities

Payroll Application – Mainframe Access

Once authenticated at the network-level, logical access to the Payroll Application is controlled through IBM's Customer Information Control System (CICS) using Resource Access Control Facility (RACF) as the external security manager. CICS, a mainframe application, provides an interface between terminal users and application programs. The RACF credentials, with the addition of RACF groups, dictate what level of access Payroll users are given, based on their role and responsibilities.

RACF password controls have been implemented that establish a mandatory password change upon initial login and after a specific number of days, minimum password length, and password history. User IDs are deactivated after a specific number of invalid login attempts. User accounts that have not been used within a specific time period are automatically deactivated.

Payroll Application – Security Administration (application, operating system, database)

Information security's primary goal is to help control access to application programs, client data and transactions, and other computing resources as well as restricting access to authorized users. The following groups are responsible for the Payroll Application production environment security administration:

- Authorized members of the Infrastructure & Operations Mainframe Security and ATM groups have system administrator privileges for the Payroll Application production environment, LAN environments, and remote access (SecurID) for technical support purposes.

- ATM is responsible for the administration of the Active Directory user accounts that are used to authenticate to ADP's network and the Payroll Application using terminal emulation. ATM is also responsible for the administration of remote access accounts to the network (SecurID – two-factor authentication). Remote access controls are not in the scope of this report and are covered in ADP's GETS US Organization SOC 1 Report.
- The M&MTAM Technical Services group is responsible for the administration of the Payroll Application user accounts (z/OS [RACF] and application [CICS] accounts).

Management has implemented a formal process to grant logical access privileges based on the user's job responsibilities. Logical access requests are formally approved by management or Human Resources. RACF and CICS access requests are documented in a centralized Service Desk Problem Management System.

Management sends access requests to the M&MTAM Technical Services group who reviews the forms for completeness and assigns a unique RACF user ID and password to the user as well as a CICS user ID and password to access the mainframe production environment. The M&MTAM Technical Services Group then communicates the user IDs and initial passwords to the requester by email or phone. Users are forced to change their mainframe RACF passwords upon initial login.

The Mainframe Security Group executes a mainframe job on a bi-weekly basis to identify terminated employees with an active RACF user ID and revoke access to the Payroll Application. A report of automated script activity is produced and reviewed by the Mainframe Security Group who follows up on accounts marked for either deletion or investigation.

An audit trail of Payroll Application operator and device activity is available to be generated from the mainframe. The audit trail provides a record of mainframe device access, configuration changes, and user actions and is used to research any questionable activity.

The Mainframe Security Group executes a mainframe job on a bi-weekly basis to identify terminated employees with an active RACF user ID and revoke access to the Payroll system. A report of automated script activity is produced and reviewed by the Mainframe Security Group who follows up on accounts marked for either deletion or investigation.

The M&MTAM Technical Services group is responsible for performing an annual review of access to the Payroll Application. The M&MTAM Technical Services group provides a list of users to the various groups for review. Each group reviews the users in their department and submits a case requesting additions and deletions to M&MTAM Technical Services group for processing.

ADP's GETS US Organization is responsible for supporting the OS and database administration at the infrastructure level. In addition, database access for application support purposes is also granted to authorized personnel, use of application database accounts is managed by the individual application support teams for the Payroll environment.

Direct access to the production databases is restricted to authorized users and system accounts. Administrative access for end-users is restricted to the DBAs as part of the Distributed Database Services (DDS) group (as part of the GETS US organization) or part of the business units or in certain cases business users who have been granted access for a valid business need.

iReports and Workforce Now Application – Security Administration

ADP associates are granted update access to the iReports output system and the Workforce Now Application for trouble shooting purposes through ADP's Universal Access tool which enables authorized ADP support personnel to log into a client environment using a valid user name and password.

The client is responsible for administering their employees' access to the iReports output system or Workforce Now Application.

A valid user ID and password are required to authenticate to the iReports output system and the Workforce Now Application. Password controls include expiration after a specific number of days, required minimum password length, and password history tracking.

ADP has established a process for granting and revoking access for new hires, temporary employees (temps), transfers, and terminating associates' access to the iReports output system and the Workforce Now Application. To request access, an employee's manager submits a Service Desk ticket detailing the access needed that is submitted to ADP's Regional LAN Support Team. The request from the manager is considered an approval and when received the request is reviewed by the Regional LAN Support Team who creates/grants the appropriate access based on the request. To revoke access, a Service Desk ticket is created and submitted to ADP's Regional LAN Support Team. Upon notification of the termination date, or on the termination date if notified ahead of time, the Regional LAN Support Team removes access.

Application Development and Change Management

Enhanced Time Application Development and Change Management

Kronos is responsible for developing and updating the core software that the Enhanced Time application is based on. Kronos periodically provides application service packs and version upgrades and documents the nature of the change and installation procedures in its Release Notes document. Kronos version releases are produced approximately every twelve to eighteen months. The last release was v8.0, which was released in November, 2015; however, not all clients have been upgraded to v8.0 and may be on an earlier, supported version (i.e., version 6). The information below describes the service pack and upgrade process for those clients that are not on the most current version.

The ADP Time and Labor Management (TLM) groups review software releases (service packs and version upgrades) and decide if they should be applied to production on an as-needed basis to increase functionality or to correct a software issue. ADP follows formal change management procedures to implement changes to the Enhanced Time application production environment. Change requests can be submitted by clients or by Solution Center associates. The change requests must be approved by the client prior to implementation. ADP uses Siebel as the problem and change management system and the GETS US organization uses the Service Desk system to document changes. Service packs applied to a client environment are recorded in a Siebel case by TLM. If the change being applied is a version upgrade, it is documented in a Client Upgrade Offering document. The Client Upgrade Offering document and/or the Siebel case contain key change management information that includes:

- The reason for the program change
- The client's business requirements, the associated risk, and any special instructions the client has that are specific to their environment
- The individuals responsible for the preparation and testing of the change
- Related managerial and/or client approvals
- Test plans and results
- Client User Acceptance Testing (UAT) sign-off (when applicable)

Client management is responsible for reviewing and approving software change requests and providing user acceptance test results and sign-offs in a timely manner when applicable.

Implementation management assigns responsibility for managing the deployment of version upgrades to a Project Manager who monitors that key milestones are met and assigns resources from Implementation and/or ADP's GETS US organization.

Authorized members of the Implementation group submit application version upgrade requests by email to the GETS US organization. Requests to apply application service packs are submitted by the Technical Services Group or the Solution Center to the GETS US organization using the Global Case Management (GCM) system, a tool used to escalate client problems and/or changes to the production environment. ADP's GETS US organization applies the change first in a non-production environment Depending on the type of change (version upgrade/service pack), they involve the Technical Services Group associates and/or the client to test system changes in this environment.

ADP's GETS US organization uses Service Desk to document the status of the change and management/client approvals for deploying the change. Changes are deployed in production by ADP's GETS US organization; however, TSS is granted administrative privileges for emergency and troubleshooting purposes. ADP's GETS US organization applies approved application changes (service packs/version upgrades) to the production environment during predefined maintenance windows and notifies the appropriate TLM group when the requested changes are completed. The Solution Center and/or TSS validate the application change (service pack) once it is migrated to the production environment and resolves identified issues in a timely manner. If the change applied was a version upgrade the client contacts the Project Manager by email and verifies the change is operating as intended. If the change negatively impacts the client environment, the ADP groups noted above are responsible for investigating the issue and taking corrective action to resolve the issue.

Enhanced Time Application Configuration Change Management

Client management (and not ADP) is responsible for testing the deployment of configuration changes and comparing the updated configuration settings against the communicated requirements.

ADP TLM Interface Change Management

The ADP TLM Interface utility is used to facilitate the transfer of data to the Enhanced Time application. Changes to the utility follow a different process than upgrades, service packs, and configuration changes. An ADP TLM Interface Development SDLC has been established to govern changes and is characterized as a spiral lifecycle model in which multiple small cross-functional teams from the Business Analysis, Development, and Quality Assurance groups work together to iterate through the full design, development, and unit test cycles of release features. The general ADP TLM Interface release process is used for releases, including more abbreviated maintenance releases (service packs). The release process comprises the following phases:

- *Business Requirements* - Product Management gathers data to request enhancements for the next ADP TLM Interface release and captures this information within the Rally system. The respective IT/business product owners meet at the beginning of a release cycle to prioritize and assign the requirements to a sprint cycle. During the meeting, the Interface Business requirements are authorized by the respective IT/business product owners.
- *Development* - Based on the business requirements, the Interface Development Team builds the release in a development environment. Tortoise SVN is used to control ADP TLM Interface source code.
- *Testing and Test Plan* - The QA department is responsible for functional, integration and regression, and user acceptance testing for all releases. The QA department creates the Test Plan document that defines test cases for new and existing features. The Test Plan is approved by the ADP TLM Development Manager, the Lead Developer, and the QA Lead.
- *Deployment to Production* - Requests for release deployment to production go through a project team which includes Product Management, Business Engineering Services (BES), and GETS. The request is put on a list of projects and the project team meets at least once a month to prioritize the project list. Once it is decided to move forward with the release, TSS submits a case to GETS. The deployment occurs during the standard maintenance window and is documented in the case. The latest version of the TLM Interface release is deployed to production based upon the client's request or to address a client issue.

MOTIF Account Request Tool Change Management

The MOTIF Account Request Tool is used to grant access to ADP associates to support client environments as an ADP-developed access request tool. Changes to the MOTIF Account Request tool follow a formal change management process that includes authorization, testing and approval prior to deployment into the production environment. The ability to develop changes and promote changes to production is appropriately restricted to authorized personnel. The MOTIF Account Request tool is configured to require a second-level approval on all changes prior to promotion to the production environment. Changes to the MOTIF tool source code generates an automated email notification to the MOTIF Development Operations team for review. Due to the sensitive nature of the changes applied to the MOTIF Account Request tool, changes are also monitored. On a daily basis, a scheduled job compares the fingerprint of the Development File branch to that of the Production File branch to detect any changes to the Production File branch that occurred outside of the defined MOTIF change management process. A daily email notification is sent to members of the MOTIF Development Operations team with the results of this script. If a difference is identified between development and production, an investigation is performed to address the difference and the resolution is documented.

Payroll Application – Application Development and Change Management

The Payroll development team currently uses the Agile methodology to develop and complete Payroll Application changes. The specifics of this method are in the following sections below related to Application Development and Change Management.

The Payroll Development Group is responsible for maintaining and developing changes supporting the Payroll Application. The changes (i.e., major releases and minor changes, which include patches, break fixes, emergency changes, standard report changes, and minor configuration changes) follow a formal systems development and maintenance process and supporting control activities. 'Projects' are application changes that are packaged in releases. There are formal procedures established to request, develop, and test changes in the test environment. Changes are certified, then deployed and implemented in the production environment.

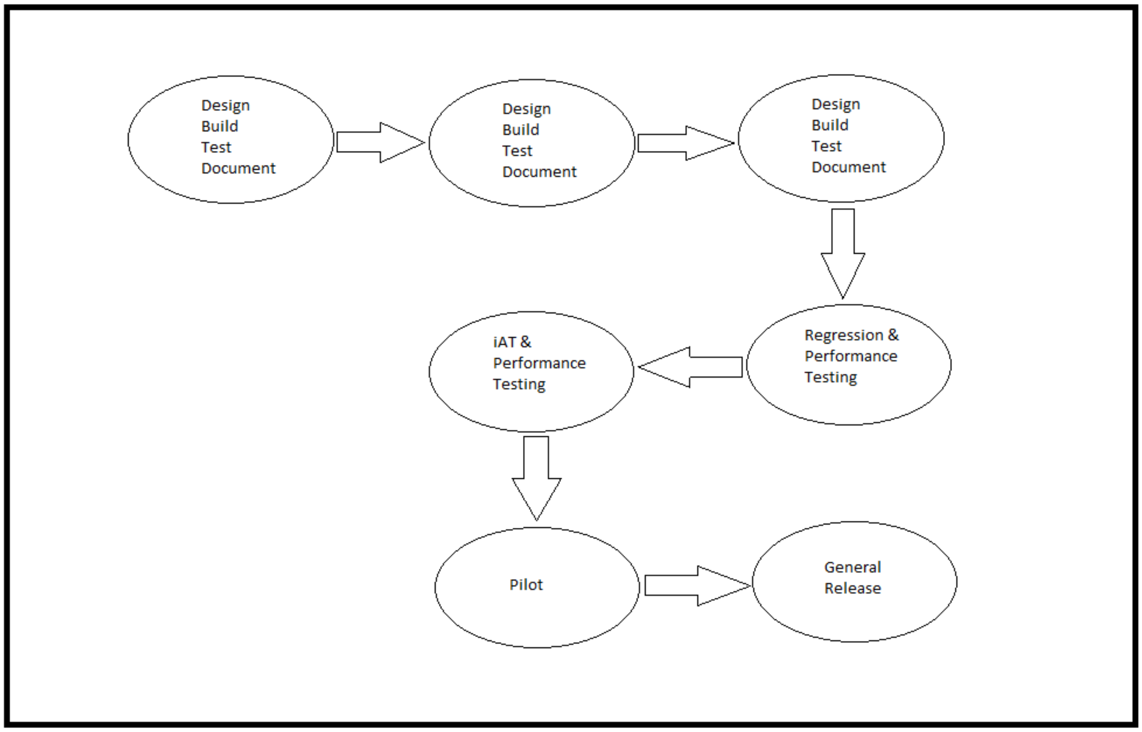
<u>Change Request Management</u>

Requests for program changes go through formalized reviews and approvals which are documented in tickets. Management of Release Management and Payroll Development collaborate to review and authorize program change requests.

<u>Software Development, Testing, and Implementation Procedures</u>

Payroll Development, Testing, and Implementation processes follow an Agile (value-driven) methodology.

Payroll application development uses Agile Scrum and Kanban frameworks as shown in the following diagram:



Changes are developed, modified, and tested in a test environment that is separate from the production environment. The test environments reside on separate mainframe logical partitions (LPAR's) that have been configured to support the Payroll Application change management process including development, testing, and baseline (i.e., approved code master repository).

A Product Owner, Scrum Master, and Scrum Development Team are assigned to each major project and are responsible for planning, developing, and maintaining project tasks. Each Scrum Development Team uses Rally software to document tasks associated with the project, due dates for each task, and issues associated with the tasks and their status. The Product Owner and Scrum Master monitor the tasks and identify if tasks are completed on or before agreed-upon project milestones. Scrum Masters hold daily "standup meetings" to assess the project status, potential blockages, and deadlines.

The Payroll team deploys major releases on a monthly basis and follows the Agile Scrum Process. Minor changes, such as patches and statutory changes, follow the Agile Kanban Process (e.g., testing in the iAT is not required). There is a decrease in the number and extent of releases during the year-end freeze period, when the Payroll Application operations process a higher number of client transactions and statutory changes, thus minimizing the implementation of non-critical system modifications during these busy periods. Calculation accuracy and completeness changes occur during the year-end freeze period but system releases are delayed until the end of the freeze period.

Payroll Development implements Agile Scrum and/or Kanban as a management framework for incremental product development using one or more cross-functional, self-organizing teams of about seven people each. It provides a structure of roles, meetings, rules, and artifacts. Teams follow best practices defined by ADP management and are responsible for creating and adapting processes within this framework. Scrum uses fixed-length iterations, called Sprints, which are typically three weeks long. Scrum teams attempt to build a potentially shippable (properly tested) product increment in each sprint.

<u>Agile Roles</u>

Product Owner

- Single person responsible for maximizing the return on investment (ROI) of the development effort
- Responsible for product vision
- Constantly re-prioritizes the Product Backlog, adjusting any long term expectations such as release plans
- Final arbiter of requirements questions
- Accepts or rejects each product increment
- Approves the product and determines whether to ship
- Decides whether to continue development
- Considers stakeholder interests

Scrum Master

- Facilitates the Scrum process
- Helps resolve impediments
- Creates an environment conducive to team self-organization
- Captures empirical data to adjust forecasts
- Shields the team from external interference and distractions
- Enforces timeboxes
- Keeps Scrum artifacts visible
- Promotes improved engineering practices

Scrum Development Team

- Cross-functional (e.g., business analysts, architects, developers, testers, domain experts, documentation specialists)
- Negotiates commitments with the Product Owner, one Sprint at a time
- Has autonomy regarding how to reach commitments
- Intensely collaborative
- Contains 7 ± 2 members

Agile Ceremonies

Sprint Planning Meeting
At the beginning of each Sprint, the Product Owner and Scrum Development Team hold a Sprint Planning Meeting to negotiate which Product Backlog Items they will attempt to convert to working product during the Sprint. The Product Owner is responsible for declaring which items are the most important to the business (Minimum Viable Product – MVP). The Scrum Development Team is responsible for selecting the amount of work to implement without accruing technical debt.

Daily Scrum and Sprint Execution
Every day, the Product Owner, Scrum Master, and Scrum Development Team members spend a total of 15 to 30 minutes reporting to each other. During each meeting, Scrum Development Team members summarize the previous days' work and the current days' work, as well as what impediments exist. During Sprint execution, the Scrum Development Team defines, develops, and reviews system requirements to produce an MVP. Business User Stories, written by the Product Owner, contain requirements. Scrum Development Team members write technical User Stories, which also support the MVP. The structure for the hardware, software, and data supporting the requirements is determined and developed. The Scrum Development Team plans for system implementation, testing, documentation, and training. The Scrum Development Team designs, codes, tests, and documents programs and conversion programs. The team uses automated, repeatable tests to help ensure code integrity throughout the sprint iterations. The ChangeMan Version Control System is used to control and monitor source code. The Scrum Development Team maintains current Sprint metrics. Organizational impediments are impediments that are issues beyond the Scrum Development Team's control. ADP Management resolves organizational impediments at the appropriate management level.

Sprint Review Meeting
At the end of the sprint, the Scrum Development Team holds a review meeting to demonstrate a working product increment to the Product Owner and stakeholders. The meeting features a live demonstration. It is the opportunity to inspect and adapt the product as it emerges, and iteratively refine the understanding of the requirements.

Sprint Retrospective Meeting
After a Sprint ends, the Scrum Development Team attends a retrospective meeting to reflect on its own process. They inspect their behavior and take action to adapt it for future Sprints. The goal is to gain a common understanding of multiple perspectives and to develop actions that will take the team and the organization to maturity.

Backlog Refinement Meeting
Most Product Backlog Items (PBI's) initially need refinement because they are too large. During this meeting, the team estimates the amount of effort they would expend to complete items in the Product Backlog and provide other technical information to help the Product Owner prioritize them.

Documentation (performed in parallel with Scrum and Kanban)

While the Scrum Development Team is completing tasks, the ES Information Development Services team member develops documentation to accompany the release. The documentation includes highlights of the release, new feature information, descriptions of product changes, new or revised procedures or processes, help updates, and installation instructions.

Documentation developed by the Information Development Services Group is available to the Regions via an internal documentation website. Documentation updates are posted to the website for Pilot and General Release phases when code is released.

The Payroll Support Group issues Information Board bulletins that provide additional information about updates or changes released previously and Program Problem Notifications that alert the Regions and M&MTAM Technical Services of problems they may encounter and temporary solutions for these problems.

Release Hardening, iAT, Pilot, General Release:

Release Hardening Phase
After the Product Owner has accepted the User Stories as meeting acceptance criteria for the Minimum Viable Product, the Release is ready and approved for Hardening. During Hardening, the Release code is frozen and no new functionality is developed. A customized System Test Plan is created and documentation is reviewed and finalized. Minimum Viable Product testing verifies that the change accurately produces the desired results. Continuous Integration Testing verifies full system, end-to-end and input-to-output functionality. Regression testing captures information about a test payroll-processing environment before and after installing the release to ensure existing functionality is uncompromised. Performance testing occurs in an environment that mirrors a region’s production environment. This is to record the installation time and to benchmark system performance before and after the release installation, and activation of new features. Payroll development uses Benchmarking information for capacity planning purposes.

iAT Phase
iAT testing replicates the testing that was originally performed by the payroll development testers but uses a more robust regional-level test base. Performance testing is performed again at this phase. Tasks include installing the entire release for the first time, complete end-to-end testing including input-to-output functionality, and standard payroll certification for both the U.S. and Canada.

The iAT Group performs a final review of the installation procedures and release documents that the Information Development Services Group prepared and conducts a turnover meeting with the Release Management Group.

Pilot Phase
As part of the Pilot Phase, the Payroll Application releases/changes are installed and run on one or more Region LPARs to monitor performance. The M&MTAM Technical Services Group has an Implementation Guide

documenting the installation process. Offsite IT personnel from ADP Release Management and Payroll Application development groups provide technical support to the pilot region. Feedback from the pilot region LPARs drives modifications to programs, documentation, or training procedures.

General Release Phase

Upon successful completion of the iAT and/or Pilot phases, the Release Management Group sends a written communication authorizing deployment to ADP's production environment. Upon receipt of the deployment authorization, the Payroll Application development testers and Payroll Support group make the program changes available to the production environment using an internally-developed Release Patch Distribution System (RPDS) that sends via FTP the release code to the production environment over ADP's ESNet. Once the release code has been made available to the production environment, the Payroll Application Delivery, Service and Support group releases a written communication stating that the release is available for deployment to the production environment. Upon receipt of this communication, authorized members of Software Configuration Management team move certified code to the baseline environment, the approved code master repository. The M&MTAM Technical Services and System Engineering staff use the Control M Scheduling System to schedule the migration of the application code into the production environment. M&MTAM Technical Services works with the M&MTAM Command Center to perform backups prior to installation. The final step of each application release is to send out an information message confirming a successful installation. The message is sent to the applicable Corporate, Regional IT, and M&MTAM Command Center personnel. The Release Management Group monitors the installation process on the Payroll Application LPARs to support timely and complete installation of releases or changes. This process helps ensure that responsibilities are segregated between the development group and M&MTAM personnel, who are responsible for migrating changes into the production environment.

Authorized IDS personnel post the release documentation developed by the Information Development Services Group to the internal documentation website. The Corporate Field Support Group provides technical support during complex product/system enhancements and rollouts.

Minor Payroll Application changes, such as patches, emergency changes, break fixes, standard report changes, and statutory (STAT File) releases, are packaged into smaller releases that must also go through a Pilot phase. The Payroll Application development tester moves Patch and STAT File Release updates to the baseline environment indicating that testing is complete. Only a limited number of authorized personnel, primarily members of the Payroll Application Delivery, Service and Support or the Payroll Support group, can make Patch and STAT File releases available to the Payroll Application production environment via the RPDS system. Similar to the process for major changes, ADP staff use the Control M Scheduling System to schedule the application code for installation to the production environment.

iReports and Workforce Now Application – Application Change Management

Changes to the iReports output system and the Workforce Now Application consist of major releases, break fixes, minor enhancements, configuration changes, report changes, or emergency changes. Changes are governed by the respective product owner and/or business unit management responsible for the system.

Requests for changes occur from internal sources or from external clients and are reviewed by each product owner and business unit management and prioritized according to client demand and internal objectives. Once reviewed, change authorizations are provided by the product owner and/or business unit management through email or during change review meetings and documented through meeting minutes. Authorized changes are then assigned a project manager and a development team to make any required coding changes.

Segregated development and test environments from the production environment exist for the iReports output system and the Workforce Now Application. Upon completion of development, testing of changes commences and is performed by the iAT group. These groups are responsible for creating test plans, executing the testing, and reviewing the test results following a similar process as described above. If the results are satisfactory, iAT will email the respective project manager, product owner, and/or business unit management for the system certifying that the change is ready for production. The project manager then reviews and approves the changes for release to production by submitting a change order to the Release Management & GETS Product Support.

Authorized members of Release Management & GETS Product Support to deploy the program code to the production environment during predefined maintenance windows. Patches and hot fixes are packaged together and released as needed.

Payroll Application – Operating System and Database Change Management

The Corporate Mainframe System Technology Group located in ADP's Corporate Headquarters in New Jersey is responsible for updates to the host Operating System (IBM's z/OS). The Corporate Computing Services (CCS) group holds CCS/Regional change control status meetings regularly.

<u>Policy and Methodology</u>

All IBM z/OS changes follow formal change management procedures. The Corporate Mainframe System Technology group manages four categories of OS and database changes:

- OS Release Change
- Product Version/Release Change or New Product Installation
- Parameter Changes or Minor Product Maintenance
- Automation Changes

The Corporate Mainframe System Technology group creates and maintains formal project plans for OS Release Changes. Documentation, if required, is also distributed to the appropriate technical organizations. The documentation may include knowledgebase records or links to ADP or vendor documentation.

The Corporate Mainframe System Technology Group prioritizes the vendor software update notifications and usually groups them into quarterly releases. OS and database change requests are reviewed during the daily and weekly Change Advisory Board (CAB) meetings and require approval before they can be deployed.

Testing

Information Technology personnel test new operating system releases and modifications. Whenever possible, mainframe operating system changes are tested in a non-production and Pilot environment prior to being deployed to the production environment. OS Release Changes require testing in the iAT environment and two pilots prior to general release. Product Version/Release Changes or New Product Installations require iAT testing and a minimum of one pilot prior to general release, and Parameter Changes require iAT testing.

Deploying the Updates

A standard naming convention that indicates the version number is used for the executable code. Access to system software source code is limited via RACF to authorized personnel, primarily members of the Corporate Mainframe System Technology Group. Using file transfer over ADP's ESNet, the Corporate Mainframe System Technology Team remotely releases host operating system updates to the Payroll Application production environment and installs the updates. With each release, the Corporate Mainframe System Technology Group reviews system logs to determine whether the installation of the OS changes to the Regions' LPARs was successful and investigates identified any problems until resolution. The final post-implementation step, which is optional, may be completed by the M&MTAM Command Center who verifies that the change was successful and updates the Service Desk ticket accordingly.

Problem Management

Benefits Services Specific

Problem management falls into two categories:

- Employee-specific issues (problems with eligibility, enrollment, and employee data)
- System or application issues that may be escalated to QA

Comprehensive Benefits Clients Employee-Specific Issues

When support is required, employees contact the ADP Comprehensive Benefits Employee Service Center (ESC) via telephone or email. Support is generally required for benefits eligibility and enrollment issues and requires follow up with additional parties such as carriers, other administrators (COBRA, FSA, etc.), and client Human Resources personnel. ESC personnel are responsible for documenting these issues and their resolution in the problem management system. Additionally, documentation of the issue resolution and a reference to the problem management case number is recorded in the employee notes section. ESC personnel are responsible for escalating issues internally through a Team Lead or Manager. Employee-specific issues that are captured in the problem management system can be exported, classified, and reported to clients via periodic status reports. Telephone call handling statistics can be captured from the Inter-Tel call system and are reported to clients against the Service Level Agreements that are specified in the client procedures document, if requested.

Comprehensive Benefits Clients System or Application Issues

Participants and/or internal client personnel can contact the ESC for system or application issues. Contact reasons can include system unavailability, inability to log in, inability to save data, or an anomaly in the performance of a system module such as reporting or invoicing. If the issue cannot be resolved by the Comprehensive Benefits group, it is informally escalated to QA for further research. The tracking and resolution of these issues is documented in the CRM system.

Third Party Data Errors

Most third party administrators provide an error report to ADP if an error in Comprehensive Benefits client-participant information is detected after a completed transmission. Comprehensive Benefits personnel are responsible for reviewing emails with error reports and resolving the issues and Comprehensive benefits clients are responsible for assisting ADP in resolving errors received from a third party provider.

SaaS Clients

After the implementation process is complete, the client is transitioned to the Client Services group for support. Client Services is comprised of Inbound and Resolution Support Analysts. The Inbound Support Analyst team is available to answer phone calls from the toll-free Client Service phone number and responds to emails that are sent to the Client Services email box. Client interactions (e.g., phone calls and emails) are documented in the Case Record Management (CRM) system. The CRM system record is the repository for the notes and actions taken to resolve the issue(s). For any call resulting in further action, a case is created and dispatched to the appropriate Case Queue.

Benefits associates also monitor case queues and are responsible for handling outbound client calls, including complex and time-consuming issues. These issues can include payroll-connection and carrier connection related items. All interactions with the client are documented in the CRM system.

On a daily basis, Client Service management receives a report of open cases that are due that day or that have missed a commitment date. The cases are reviewed with the associates and commitment dates are adjusted as needed. Each week, management receives a report that lists outstanding CRM system records and includes the "last activity date" for each record. This report is shared with associates to assist them to review and update their cases. This process helps ensure that cases are being resolved in a timely manner.

When clients identify an issue and they need system support, they contact the Client Services group by phone or email. Only client contacts that are identified in the CRM system as authorized contacts can ask the Client Services group to make changes to benefits-related data. When the Client Services group modifies data, upon client request, the Client Service associate records the request in the CRM system and tests the change on a selection of client employees. Client Services verifies that the information is correct for a selection of client employees and notifies the client that the change has been deployed. Clients are responsible for QA testing the requested changes to verify that they were made accurately and completely.

Essential Time Specific

Upon completion of the Essential Time implementation, clients are transitioned to the TLM Service Center group for support. The TLM Service Center group is a virtual organization and the call centers are located in Parsippany, NJ; Elk Grove, IL; El Paso, TX; Augusta, GA; La Palma, CA; Manila, Philippines; and Pune, India. These locations, regardless of location, respond to Essential Time client inquiries.

When clients identify an issue with the application and need support, they contact the TLM Service Center group via phone or email. The Technical Support Analyst authenticates the caller by confirming that s/he is listed as an authorized client contact. Members of the TLM Service Center group are responsible for documenting all phone and email interactions with clients in Siebel. Each interaction is assigned a priority level and assigned to a member of the TLM Service Center based on client, skill set, and the identified issue.

TLM Service Center personnel respond to inbound calls based on the product features being asked about and outbound calls are made to the client depending on the severity and complexity of the issue. TLM Service Center representatives record the information and steps taken to correct issues and use descriptive labels for traceability and reporting. TLM Service Center Management monitors the status of cases and resolution by generating open cases and case aging reports from the Tableau system, which pulls data directly from Siebel.

Issues that cannot be resolved by the first-tier TLM Service Center group are escalated to the Technical Support Services group for resolution. The Technical Support Services group tracks escalated issues in the Serena Business Manager system and notifies the TLM Service Center group when they are resolved.

If the issue cannot be resolved by the Technical Support Services group, it is escalated to the GETS US organization via Service Desk. The GETS US organization tracks escalated issues in the Service Desk Problem

Management system. The GETS US organization notifies the TLM Service Center/Technical Support Services groups when the issue has been resolved.

Enhanced Time Specific

When clients identify an issue with the application and they need support, they contact the Solution Center through phone or email who then utilizes the e-Access ticketing tool to track client issues. Cases are given a priority level and are assigned to a member of the Solution Center based on prior client interaction, necessary skill set, and nature of the issue. If the Solution Center deems the issue to be hardware related, it is escalated to the GETS US organization using the Global Case Management (GCM) tool. The GETS US organization opens a ticket in the Service Desk system and updates it to track the status of the issue. The GETS US organization notifies the Solution Center and/or TSS when the issue has been resolved so that the corresponding case can be closed.

Urgent cases are monitored real-time via an urgent case dashboard. On a daily basis, Solution Center managers receive an automated email of open cases. Solution Center Managers filter the listing based on the open cases assigned to them, and review the open cases to determine whether open issues are resolved appropriately. Periodically, Solution Center managers update the notes in the ticket to keep the status of the open case.

SUBSERVICE ORGANIZATIONS

ADP GETS US Organization

Overview of Subservice Provider Relationship

The Workforce Now application and supporting technology infrastructure are hosted and managed by ADP's GETS US organization. The GETS US organization is responsible for various support functions, including operating system change management, network problem and incident management, network administration, operating system and database administration, data transmission support and system monitoring, physical security, environmental safeguards, and data backups. The processes and controls within these functions are delivered as a common set of services to all ADP business units and are not included in the scope of this report. These common services are covered in ADP's GETS US Organization SOC 1 Report.

The table below outlines the control process areas applicable to the Workforce Now application that are covered in the scope of this report (Workforce Now SOC 1 Report) and those that are covered in the scope of ADP's GETS US Organization SOC 1 Report:

Process Name	ADP's GETS US Organization SOC 1 Report	Workforce Now Services SOC 1 Report
Application Development and Change Management		✓
Operating System (OS), Hardware, and Infrastructure Change Management		
a. Mainframe OS - Payroll Application		✓
b. Other OS –iReports, Workforce Now Application, Enhanced Time	✓	
c. Hardware and Infrastructure Change Management	✓	
Network Monitoring and Incident Management	✓	
Logical Security		
a. iReports, Workforce Now Application, Enhanced Time, and Payroll Application layers and Mainframe OS		✓
b. Windows, AIX, zLinux OS	✓	
c. Network Administration	✓	
d. OS and Database Administration[1]	✓	✓

Process Name	ADP's GETS US Organization SOC 1 Report	Workforce Now Services SOC 1 Report
Physical Access	✓	
Environmental Safeguards	✓	
Computer Operations and Data Backup	✓	
Problem Management		✓
Data Input		✓
Data Processing		✓
Data Output		✓

[1] ADP's GETS US organization is responsible for supporting the OS and Database Administration at the infrastructure level. In addition, database access for the Workforce Now Application and Payroll Application support purposes is managed by application-side personnel.

Complementary Subservice Organization Controls

ADP's GETS US organization is subject to the same oversight and governance as outlined in the "*Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Control Activities, and Information and Communication*" section previously described. Additionally, various business unit personnel supporting the services within this Description interact with GETS US organization personnel on a regular basis. The GETS US organization has implemented the following key control activities to support the associated control objectives as they related to the scope of this Description:

Control Process Area	Sub-Service Organization Controls
Operating System Software, Hardware, and Infrastructure Change Management	Controls to address the implementation of and changes to operating system software, hardware, and infrastructure to confirm changes are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.
Network Monitoring	Controls to address ADP's network monitoring and security mechanisms for protection from external threats and interruptions.
Logical Security	Controls to address logical access to programs, data, and computer resources to confirm it is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.
Physical Security	Controls to address physical access to computer and other resources to confirm it is restricted to authorized and appropriate personnel.

Control Process Area	Sub-Service Organization Controls
Environmental Safeguards	Controls to confirm operational procedures are in place within the hosting and data center facilities over physical assets to prevent processing errors and/or unexpected interruptions and support the complete, accurate, and timely processing and reporting of transactions and balances.
Data Backups	Controls to address regular data and applications backups and availability for restoration in the event of processing errors or unexpected processing interruptions.
Operational Monitoring and Incident Management	Controls to address operational problems identification and resolution in a timely manner.

These controls are covered in ADP's GETS US Organization SOC 1 Report.

COMPLEMENTARY USER ENTITY CONTROLS

ADP controls were designed with the assumption that certain controls would be implemented by user entities (clients). It is not feasible for control objectives relating to transaction processing to be achieved completely by ADP's management or the user entities acting alone. It is necessary for user entities to implement controls to achieve some of the control objectives identified in this report (as applicable).

The User Entity Control Considerations presented below are controls that user entities should have placed in operation to achieve the control objectives in this report and should not be regarded as a comprehensive list of controls that should be used by user entities. The applicability and implementation of these controls may vary by user entity based on the nature of the services and applications being used by ADP's user entities. Other controls may be required by user entities and should therefore be evaluated by the user entity. User entity auditors should consider whether user entities have implemented these controls (as applicable) when understanding and evaluating the internal controls at the respective user entity.

Control Objective #1: Data Input – Workforce Now

Client management is responsible for:

- *Benefits*
  - Verifying that data sent to ADP is complete and accurate
  - Verifying that data entered is recorded in the Workforce Now Application completely and accurately
  - Correcting identified errors in the input data files and resending the updated file to ADP in a timely manner
  - Validating that data sent to ADP is received in a timely manner
  - Reviewing any error reports that are provided by ADP
  - Entering complete and accurate data using the application GUI and time-collection mechanisms
  - Access controls to the time-collection mechanisms that their employees use to track their time
  - Addressing any input errors identified by the system and re-submitting data input in a timely manner
- *Essential Time*
  - Entering complete and accurate data into the Enhanced Time Application using the application GUI and/or other import mechanisms
  - Addressing any input errors and re-submitting the updated inputs in a timely manner
- *Enhanced Time*
  - Validating the completeness and accuracy of employee and timecard information entered into the Enhanced Time Application through the various time and labor management data collection devices (e.g., time clocks, biometric devices, phone, mobile devices, IVR)

- Reviewing and resolving Enhanced Time Application error messages and/or error log files reported and/or displayed
  - Reviewing (as deemed necessary) transactions logs and other audit logs produced by the Enhanced Time Application for appropriateness, and notifying ADP of any unusual activity performed by ADP and client associates
- *Payroll*
  - Reviewing that custom settings (e.g., approval workflows, company profiles, time-off policy) used in the processing of payroll are configured based on the client's environment
  - Notifying ADP of changes in the authorized contacts list
  - Validating the accuracy of initial data entry when using the input System
  - Reviewing error messages that result from transmitting data, addressing errors and resending data in a timely manner
  - The accuracy/completeness and authorization of worksheets and faxes that are sent to ADP
  - Setting up a second authentication method (such as the use of a passphrase) for phone or fax payrolls
  - Setting up a receipt confirmation method (such as callback or fax) for phone or fax payrolls
  - Reviewing Correction Notices received from ADP
  - Reviewing the Master Control form, containing the listing of each employee's master record, produced by the Payroll Application after initial account set-up, to confirm that employee-level and company-level information was initially recorded completely and accurately

Control Objective #2: Data Processing – Workforce Now

Client management is responsible for:

- *Benefits*
  - Reviewing the results of the benefit eligibility and benefit deductions calculations, and comparing results to the source documents and data
  - Approving the business rules and benefits eligibility rules that are configured in the Workforce Now Application
  - Providing information to resolve errors and correcting, if necessary, processing errors identified
  - Addressing any output errors and re-generating reports/exports in a timely manner
  - Reviewing the completeness and accuracy of the reports that are produced by the Workforce Now Application
  - Assisting ADP in resolving errors received from a third party provider
- *Essential Time*
  - Initiating processing in a timely manner
  - Reviewing and resolving any warnings, messages, and errors
  - Requesting assistance from ADP to resolve issues as required

- *Enhanced Time*
    - Reviewing and resolving any processing warnings, messages, and errors reported or displayed by the Enhanced Time Application
    - Requesting, and when applicable, authorizing, assistance from ADP to resolve issues
    - The authorization and appropriateness of configuration settings and business rules established and maintained in the Enterprise Enhanced Time Application (e.g., pay rules, time card approval configurations, shift guarantees)
    - Reviewing (as deemed necessary) transaction logs and other audit logs produced by the Enhanced Time Application for appropriateness, and notifying ADP of any unusual activity performed by ADP and client associates

Control Objective #3: Data Processing - Benefits - Carrier Billing/Invoice Reconciliation and Payment

Client management is responsible for:
- Reviewing and approving the terms of the invoicing
- Investigating and resolving invoicing problems or identified issues
- Reconciling the amount debited from their account against the Workforce Now Application and Carrier invoice amounts (Comprehensive Benefits clients only)
- If not done by ADP, timely and accurate payment of carrier invoices

Control Objective #4: Data Processing - Benefits - Client Maintenance and Open Enrollment

Client management is responsible for:
- Providing all benefit plan change information and validating that the information gathered by the AES is accurate
- Requesting, reviewing, and approving the Benefit Plan Summary and payroll test file (including FSA only clients)
- Reviewing and approving the test confirmation statement template
- Reviewing and approving the business rules and benefits eligibility configurations in the Workforce Now Application

Control Objective #5: Data Processing - Payroll Deductions and Tax Withholding Specifications

Client management is responsible for:
- The completeness and accuracy of client-specified deductions
- Submitting client-specified deduction changes to ADP in a timely manner
- Verifying that deduction and tax withholding information is accurate before providing payroll processing approval if the client uses Quick View

- Reviewing the Master Control and Personnel Change reports that are distributed upon payroll processing to determine whether deduction and tax withholding information is complete and accurate and notifying ADP if an error is identified or a change needed

Control Objective #6: Data Processing - Payroll

Client management is responsible for:

- Setting up the payroll processing submission schedule each year
- Verifying receipt of submission confirmation
- Reviewing system reports when known client-specific situations exist, verifying that the issue was resolved, and any changes to data were appropriate

Control Objective #7: Data Output – Workforce Now

Client management is responsible for:

- *Benefits Service*
  - Validating the completeness and accuracy of customized reports and data file outputs during the implementation process
  - Notifying ADP of required changes to output reports or data files
  - Testing and approving changes to output reports and data files
  - Restricting employee access rights to data outputs and report generation
  - Notifying ADP of any errors identified in data outputs
- *Essential Time Service*
  - Initiating the output generation and reviewing the output reports to determine the information contained within the reports is complete and accurate
  - Addressing any output errors and re-generating reports/exports in a timely manner
- *Enhanced Time Service*
  - Initiating and authorizing the output generation
  - Restricting employee access rights to data outputs and report generation
  - Reviewing the completeness and accuracy of the output files and reports that are produced
  - Reviewing error messages and logs that result from generating output files and/or reports and transmitting output files and reports
- *Payroll Service*
  - Notifying ADP of changes required to their payroll output
  - Printing and secure check distribution, if done in–house by client
  - Defining the processing schedule and communicating required changes to ADP in a timely manner
  - Acknowledging the receipt of payroll output
  - Reviewing the payroll output reports and notifying ADP of any discrepancies
  - Notifying ADP of any issues with delivery of printed reports

Control Objective #8: Data Output – Payroll (Money Movement/Direct Deposit Files)

Client management is responsible for:

- Banking service, to ADP (completing their agreement and authorization with the individual banks and providing the necessary banking information to ADP if the client elects Regular Direct Deposit)
- Confirming accuracy and completeness of direct deposit funds disbursement information provided to ADP

Control Objective #9: Application Development and Change Management

Client management is responsible for:

- Approving, validating, and confirming with ADP all plan configuration changes made in the Workforce Now Application
- Approving, validating, and confirming with ADP all carrier changes made in the Workforce Now Application
- Performing final user acceptance testing, including open enrollment testing, and providing testing approvals, as well as communicating issues and/or problems related to the Workforce Now Application
- Providing user acceptance test results and sign-offs in a timely manner when requested by ADP
- Testing configuration change deployments and comparing the updated configuration settings against the communicated client requirements
- Maintaining a list of authorized ADP client contacts

Control Objective #11: Logical Security

Client management is responsible for:

- Determining that only authorized client personnel are granted logical access to the iReports output system and the Workforce Now Application
- Granting and revoking access to the iReports output system and the Workforce Now Application
- Periodically reviewing assigned employee access to the iReports output system and the Workforce Now Application for appropriateness
- Reviewing the Audit Trail log within the Workforce Now Application (highlighting any updates made to payroll data), to identify any unauthorized activity and notifying ADP of any discrepancies
- Immediately notifying ADP of actual or suspected information security breaches, including compromised user accounts
- Periodically reviewing all users and their assigned access rights, including application users and users assigned with administrator privileges in SMS
- Administering and informing ADP of any changes regarding the individual(s) who will be provided security master access within the SMS tool
- Selecting the required security options within SMS to enable employee user account administration and authentication. The following options are available:

- Organizational registration code – provided to an organization to use during registration
    - Personal registration code – uniquely associated with a participant and used during registration
- Enforcing the use of unique SMS Identity Verification Options in combination with the selected SMS registration code to verify users upon authentication
- Periodically changing the organization registration code if selected as the SMS security option
- Securely communicating and managing registration codes to users for initial logon to ADP portals and applications
- Implementing policies and procedures to administer and update identity verification options (registration codes and personal identifiers)

Control Objective #12: Problem Management

Client management is responsible for:

- Responding to ADP requests for information and/or resolution of reported problems and incidents in a timely manner
- Notifying ADP of problems or issues encountered
- Reporting processing problems in a timely manner
- Maintaining a list of authorized client contacts with ADP

SECTION FOUR

DESCRIPTION OF CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULTS OF TESTS

TESTING PERFORMED AND RESULTS OF TESTS OF ENTITY-LEVEL CONTROLS

In planning the nature, timing and extent of its tests of the controls specified by ADP in this Description, Ernst & Young considered the aspects of ADP's control environment, control activities, risk assessment, information, and communication and monitoring activities and performed such procedures over these components of internal control as it considered necessary in the circumstances.

PROCEDURES FOR ASSESSING COMPLETENESS AND ACCURACY OF INFORMATION PRODUCED BY THE ENTITY (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by ADP and provided to user entities (if relevant and defined as part of the output control objectives), IPE used by ADP management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures was performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) agree data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

TRANSACTION PROCESSING CONTROL OBJECTIVES AND CONTROLS

Data Input – Workforce Now

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.01	Clients have the ability to import data to the Workforce Now Application using the Import Tool. Any errors that occur during the data import process are recorded in a log and made available for review by client users with the Administrator/Practitioner role.	For a sample benefits data import via the Import Tool, observed an import of a data file to determine whether errors identified during the import process were recorded in a log and made available for review.	No deviations noted
		Observed the completion of the Import Interface for Essential Time data to determine whether the import loaded completely and errors identified during data import were logged.	No deviations noted
		Observed a QA Engineer access the Workforce Now Application as the Administrator/Practitioner role to determine whether the error log was available for review.	No deviations noted

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.02	The Workforce Now Application uses input controls to enforce the complete and accurate input of data: • Data entry validation controls, such as format checks • Mandatory fields • Drop down boxes In the event that incorrect data is attempted to be entered into the system, error messages appear on the users' screen.	For a sample benefits data input within the Workforce Now Application, observed that, when incorrect data was entered, input controls (e.g., data entry validation, mandatory fields, and drop down boxes) caused error messages to appear on the users' screen, and prevented the transaction from recording within the applications.	No deviations noted
		Observed an ADP associate attempt to submit incorrect/incomplete payroll data (e.g., SSN, zip code, employee name, pay frequency) into the Workforce Now Application and inspected the related error messages generated to determine whether pre-defined data validation rules are in place to detect and identify erroneous data input and incomplete data.	No deviations noted
		Observed a QA Engineer enter Essential Time data in the Workforce Now Application to determine whether data validation controls include time entry format checks, prompts for mandatory fields, drop-down boxes for restricted selection, and pre-populated fields that cannot be edited.	No deviations noted
		Observed a QA Engineer enter incomplete Essential Time data in the Workforce Now Application to determine whether data validation control error messages are displayed on the screen.	No deviations noted

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.03	The Workforce Now Application utilizes a 256-bit Secure Socket Layer (SSL) encryption for the web browser application sessions which adds security for data entry.	Observed an ADP associate log into the Workforce Now Application on a sample day to determine whether the site uses SSL technology with encryption. For a sample file from the Workforce Now Application: • Inquired of a Principle Quality Assurance Engineer to determine whether SSL technology with encryption is used to securely transmit payroll data entered from the input system into the Payroll Application; • Inspected a data string within the file to determine whether data is not presented in clear text.	No deviations noted No deviations noted
Enhanced Time Service			
1.04	The Enhanced Time application contains edit checks to identify errors resulting from invalid and/or incomplete data that is imported manually and automatically through XML. Any errors identified are reported in a log file that is made available for clients.	For a sample employee, observed data being imported into the Enhanced Time application to determine whether errors related to incomplete and invalid data were appropriately identified. Inspected the import log file generated by the Enhanced Time application to determine whether errors identified during the data import were reported in the log file and made available for clients to review.	No deviations noted No deviations noted

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.05	The Enhanced Time application contains the following edit checks that validate the accuracy/completeness of data entered manually: • Data entry validation controls, such as time entry format checks • Mandatory fields • Drop-down boxes • Pre-populated fields that cannot be modified through data entry	For a sample employee, observed the manual entry of employee data to determine whether when invalid or incomplete data was entered manually, the edit checks caused error messages to appear on the users' screen. These edit checks included: • Data entry validation controls, such as time entry format checks • Mandatory fields • Drop-down boxes • Pre-populated fields that cannot be modified through data entry	No deviations noted
	If the edits do not pass, error messages appear on the users' screen, preventing further processing.	For a sample of input transactions, observed invalid or incomplete data being input to determine whether the edit checks caused error messages to appear on the users' screen and further processing was prevented.	No deviations noted
1.06	Once data entered passes the required edits, employee and time data is automatically updated in the Enhanced Time application.	For a sample transaction, observed an ADP associate enter data into the Enhanced Time application manually and through file import and inspected the Enhanced Time application's client master records, after successful processing, to determine whether data entered was automatically recorded accurately and completely.	No deviations noted

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	Description of Control Activity	Test of Controls	Results
Payroll Service			
1.07	Data file transmissions between the Workforce Now Application and the Payroll Application are monitored and identified issues, if any, are documented, reported, and followed up to resolution.	Observed ADP personnel monitoring data file transmission alerts on a sample day to determine whether automated monitoring tools are used to monitor for issues or exceptions with data file transmissions between the Workforce Now Application and the Payroll Application. For a sample of identified file transmission issues between the Workforce Now Application and the Payroll Application, inspected the problem resolution record (Service Desk tickets, End of Night checklists, emails) to determine whether reported issues were documented and followed up through resolution in a timely manner.	No deviations noted No deviations noted

Control Objective 1: Controls provide reasonable assurance that the benefits administration, payroll, and time & attendance data received is authorized and recorded completely and accurately.

Ref	Description of Control Activity	Test of Controls	Results
1.08	Payroll data (e.g., employee records, salary, deductions, marital status, and tax jurisdiction) entered into the Workforce Now Application is transmitted to the Payroll application successfully and automatically updates the Employee Master Database (EMP) within the Payroll Application.	Observed a production support associate enter payroll master data (employee records, salary, deductions, marital status, tax jurisdiction) into the Key-Fast system and inspected the Payroll Application to determine whether the data was successfully transmitted and automatically updated in the Employee Master Database. Inspected relevant documentation from the Workforce Now Application and the Payroll Application to determine whether master data (employee records, salary, deductions, marital status, tax jurisdiction) entered by a production support associate was successfully transmitted and automatically updated in the Employee Master Database.	No deviations noted No deviations noted
1.09	The Payroll Application EDIT processing performs a series of edit checks on payroll data files received from the input system by comparing the data files within the Employee Master Database (EMP) to verify that the information is accurate. Errors that appear on EDIT screens are investigated and resolved by the Production Support (Editing) group prior to the payroll being released for further processing.	Observed members of the Production Support (Editing) group perform EDIT processing real-time in the Payroll Application on a sample day to determine whether errors identified appear on EDIT screens. Observed members of the Production Support (Editing) group on a sample day reviewing and investigating the errors that appeared on EDIT screens to determine whether the errors were resolved prior to the payrolls being released for further processing.	No deviations noted No deviations noted

Data Processing – Workforce Now

Control Objective 2: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance data is processed accurately and in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.01	The Workforce Now Application tracks HR, leave, and recruitment information and calculates benefit eligibility and benefits deductions based on the plan information that has been configured according to client specifications.	For a sample client and participant, and his/her elected benefits, inspected the associated benefit deductions and recalculated the benefits deductions per the client and plan configuration to determine whether the Workforce Now Application tracks HR, leave, and recruitment information and calculates benefit eligibility and deductions accurately based on the plan information configured.	No deviations noted
		For a sample client and participant and his/her elected benefits, inspected the elected benefits data to determine whether the benefit eligibility decision was appropriate based on the client and plan configuration.	No deviations noted
2.02	Participant data errors may occur with processing of participant information when extracting and formatting data to be sent to third party administrators. Error reports, which include the participants that had errors in their information, are sent to the Comprehensive Benefits group. The Comprehensive Benefits group is responsible for tracking, researching, and resolving these errors.	For a sample of data errors, inspected corresponding documentation and system records to determine whether errors were tracked, researched, and resolved by the Comprehensive Benefits group.	No deviations noted

Control Objective 2: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance data is processed accurately and in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.03	The Workforce Now Application is configured to process payroll based on client defined work and pay rules (i.e., rounding, shift guarantees, exception flags).	Observed the processing of payroll for a sample of work and pay rules within the Workforce Now Application and re-performed system results to determine whether employee time and payroll is calculated based on the work and pay rules.	No deviations noted
2.04	During the processing of payroll, the Workforce Now Application is configured to notify the user regarding payroll related exceptions (e.g., messages, warnings, and errors) and prevent the processing of payroll for errors.	Observed the processing of a client payroll to determine whether users are notified of payroll related exceptions, including messages, warnings, and errors, for supervisor approvals, overtime hours, and missing time punches.	No deviations noted
		Observed the processing of a client payroll to determine whether payroll related errors prevent the processing of payroll.	No deviations noted
2.05	The Workforce Now Application restricts clients from moving to the next pay period without completing specific payroll, time, and event management steps.	Observed the processing of a client payroll to determine whether the Workforce Now Application restricts clients from generating payroll and moving to the next pay period without completing specific payroll, time, and event management steps.	No deviations noted
Enhanced Time Service			
2.06	The Enhanced Time application allows clients the functionality to configure work and pay rules such as shift guarantees, overtime rules, and exception flags.	Inspected the configuration screen of the Enhanced Time application to determine whether clients can configure work and pay rules such as shift guarantees, rounding rules, and exception flags.	No deviations noted

Control Objective 2: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance data is processed accurately and in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.07	The Enhanced Time application automatically calculates work and pay rules such as shift guarantees, rounding rules, and exception flags based on the configured inputs by clients.	For a sample of transactions input into the Enhanced Time application, observed that rounding rules, shift guarantees, and exception flags produced the expected output according to the configuration of the client work and pay rules.	No deviations noted
Comprehensive Payroll Service			
2.08	Clients using the Comprehensive Payroll service (ADPCheck, FSDD) must approve a stop pay or reversal with their Payroll specialist to initiate a refund.	For a sample of stop payments and reversals processed by the Comprehensive Payroll team, inspected the case management ticket to determine whether the stop pay or reversal was approved by the client prior to the Payroll Specialist initiating a refund.	No deviations noted
2.09	Amendments must be approved by the client before being processed.	For a sample of amendments processed by the Comprehensive Payroll team, inspected the case management ticket to determine whether the amendment was approved by the client prior to being processed.	No deviations noted
2.10	ADP provides a preview W-2 to the client for review prior to the processing deadline.	For a sample of Comprehensive Payroll clients, inspected the Workforce Now system to determine whether a preview W-2 was provided to the client for review prior to the processing deadline.	No deviations noted

Data Processing – Benefits - Carrier Billing/Invoice Reconciliation and Payment

Control Objective 3: Controls provide reasonable assurance that carrier billing, invoice reconciliation, and payments are processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.01	ADP Comprehensive Benefits maintains documented client administrative procedure manuals to provide guidance during the carrier invoicing and billing process.	Inspected the client administrative procedures to determine whether they were documented and available to Comprehensive Benefits personnel.	No deviations noted
3.02	The Workforce Now Application calculates the invoicing amounts based on client parameters and employee enrollments. For clients that have contracted for this service, Comprehensive Benefits personnel use standard invoice processing. For premium remittance clients, ADP uses checklists to process the summary consolidated billing invoices if the client uses ADP to pay the carrier invoices.	For a sample client, inspected the Workforce Now Application to determine whether invoicing amounts were calculated based on client parameters and employee enrollments. For a sample of premium remittance clients and invoices, inspected the invoice checklists to determine whether the checklists were used to process the summary consolidated billing invoices.	No deviations noted No deviations noted
3.03	A summary of consolidated invoice information is created and sent to each client on a monthly basis that provides information regarding invoices and amounts due to carriers.	For a sample of clients and dates, inspected the monthly consolidated invoice summaries and evidence of their delivery to determine whether the summaries were generated and delivered to clients as specified.	No deviations noted

Control Objective 3: Controls provide reasonable assurance that carrier billing, invoice reconciliation, and payments are processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.04	For clients that have contracted to have their bills processed according to the carrier bill and Workforce Now Application records, Comprehensive Benefits personnel reconcile carrier invoices with data stored in the Workforce Now Application on a monthly basis and the carrier invoices or census reports with the data stored in the Workforce Now Application at least annually (if applicable, i.e., if the carrier maintains employee enrollment data) to verify that the amounts are valid and accurate. If variances are identified, discrepancy reports are generated as a result of the reconciliation and are either updated on the carrier websites or sent to the carriers to update their system.	For a sample of clients and months, inspected the monthly carrier reconciliation to determine whether Comprehensive Benefits personnel reconciled carrier invoices with data stored in the Workforce Now Application and that if variances were identified, discrepancy reports were generated and either updated on the carrier website or sent to the carrier.	No deviations noted
		For a sample of clients, inspected the annual reconciliation documentation, to determine whether Comprehensive Benefits personnel reconciled carrier invoices or census reports with data stored in the Workforce Now application and that if variances were identified, discrepancy reports were sent to the carrier.	No deviations noted

Control Objective 3: Controls provide reasonable assurance that carrier billing, invoice reconciliation, and payments are processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.05	ACH transactions for the client carrier payments are approved by an authorized client contact and the VP of Finance or the Sr. Director of Finance prior to processing. Approvers cannot verify transactions that they have input into the Chase Access Next Gen application.	For a sample of clients and months, inspected the ACH transaction approval form to determine whether the transaction was approved by an authorized client contact and the VP of Finance or the Director of Finance and that the amounts approved corresponded to the required amount owed to the carrier. Observed a member of the ADP Finance Department attempt to approve their transaction in the Chase Access Next Gen application to determine whether the Approver has the ability to verify a transaction that they have input.	No deviations noted No deviations noted
3.06	Only authorized associates have access to the Chase Access Next Gen application used to transfer funds to and from client accounts.	Inspected the Chase Access Next Gen application user list and inquired of management regarding the users' job responsibilities to determine whether only authorized users had access to the accounting software. Inquired of management regarding the users' job responsibilities to determine whether access was segregated between personnel that can setup vendors, initiate payments, and release payments.	No deviations noted No deviations noted
	User IDs, passwords, and a token are required to access the Chase Access Next Gen application.	Observed a user log in to the Chase Access Next Gen application to determine whether a user ID, password, and token were required.	No deviations noted

Data Processing – Benefits - Client Maintenance and Open Enrollment Services

Control Objective 4: Controls provide reasonable assurance that open enrollment activities for Benefits Administration Services (Comprehensive Benefits) clients are processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.01	An Open Enrollment Questionnaire and/or Planning Recap documentation is used to track the Open Enrollment dates of each client during the OE period.	For a sample of clients, inspected the Open Enrollment Questionnaire and/or Planning Recap documentation to determine whether the client Open Enrollment dates were tracked.	No deviations noted
4.02	Open Enrollment is set up in the Workforce Now Application as requested by the client and completion of the following items: • Rate Sheet (if applicable) • Benefits Plan Setup Form (if applicable)	For a sample of clients, inspected the Rate Sheet (if applicable) and Benefits Plan Setup Form (if applicable) to determine whether the Open Enrollment was completed as requested with the required information to update the client's profile in the Workforce Now Application.	No deviations noted
Comprehensive Benefits Service			
4.03	A Benefit Plan Summary is produced by ADP and provided for review by ADP management and the client to validate open enrollment information was accurately and completely input into the Workforce Now Application.	For a sample of clients, inspected the Benefit Plan Summary to determine whether the report was produced and provided for review by the Implementation staff, the Benefits Solution Specialist, or the Relationship Manager.	No deviations noted

Control Objective 4: Controls provide reasonable assurance that open enrollment activities for Benefits Administration Services (Comprehensive Benefits) clients are processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.04	When the open enrollment period begins participants can make their elections and employee records in the Workforce Now Application are updated in real-time. QA reviews the data warehouse dashboard to verify that participant elections were entered and there are no errors. If there are errors, clients work with Comprehensive Benefits until they are resolved.	For a sample client, observed an election transaction during the client's open enrollment period to determine whether the transaction was automatically recorded within the Workforce Now Application. For a sample of clients, inspected the data warehouse to determine whether participant elections were entered and errors, if any, were documented and resolved.	No deviations noted No deviations noted
4.05	*FSA Plan Only* Clients electing FSA-only plans are set up in the Workforce Now Application as requested by the client. The setup is performed by the Comprehensive Benefits group based on the following documentation: • Summary of plan renewal information communicated to the client for review • Confirmation from the client with approval to proceed and update (if applicable) • Confirmation of changes made in the Workforce Now Application communicated to the client (if applicable)	Inspected the Workforce Now Application for a sample of FSA-only clients to determine whether the enrollment was set up as requested. For a sample of FSA-only clients, inspected email communication and supporting documentation to determine whether: • A summary of plan renewal information was communicated to the client for review • A confirmation email from the client with approval to proceed and update was received (if applicable) • A confirmation email of changes made in the Workforce Now Application was communicated to the client (if applicable)	No deviations noted No deviations noted

Data Processing - Payroll Deductions and Tax Withholdings Specifications

Control Objective 5: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the Payroll Application in accordance with statutory and/or client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
5.01	The Corporate Statutory Research Shared Services group monitors statutory changes impacting payroll-related taxes for both U.S. and Canadian taxing authorities.	For a sample of statutory changes, inspected the Rally ticket to determine whether statutory changes impacting payroll related taxes for both U.S. and Canadian taxing authorities were monitored, documented, and tracked through resolution by the Corporate Statutory Research Shared Services group.	No deviations noted
5.02	Upon identification of a statutory change impacting payroll-related taxes, the Statutory Research Shared Services creates and distributes an email/document detailing the change. The Stat Project Manager activates a Statutory feature in the Rally software where the Business Analysts on the Payroll Statutory Kanban team will review and analyze the impact (e.g., STAT file, quarter, client, and region) and approve.	For a sample of statutory changes, inspected the Rally ticket and relevant design and analysis documentation (STAT change request form, analysis and design documents, peer-review meeting minutes) to determine whether the Statutory Research Shared Services created and distributed documentation detailing the change and the impact of the statutory change was reviewed, analyzed, and approved by Business Analysts on the Payroll Statutory Kanban team.	No deviations noted

Control Objective 5: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the Payroll Application in accordance with statutory and/or client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
5.03	Statutory changes requiring coding modifications are coded by the appropriate development team and tested and certified for production release by the appropriate testing group. *Upon completion of testing, changes are deployed to production following the change management process outlined in Control Objective 9.*	For a sample of statutory changes that required coding modifications, inspected the testing results within the Rally ticket to determine whether the change was tested and certified for production release by the appropriate testing group.	No deviations noted
5.04	Statutory changes that do not require coding modifications are applied to the STAT File database by authorized STAT members.	Inspected the system-generated listing of user IDs with update privileges in the STAT File database and inquired of the Director Applications Development regarding the job responsibilities of the identified users to determine whether accounts were assigned to appropriate STAT members. For a sample of statutory changes applied to the database where no coding was required, inspected the STAT File database records to determine whether an authorized user applied the change.	No deviations noted No deviations noted

Control Objective 5: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the Payroll Application in accordance with statutory and/or client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
5.05	Client Support Specialists (CSSs) process client requests to add, modify, or delete client–specified deductions in the Payroll Application upon receiving approval from an authorized client contact.	For a sample of client-specified deduction requests, inspected the case management record or email correspondence and Payroll Application to determine whether the requested change was correctly updated in the Payroll Application based upon a request by an authorized client contact.	No deviations noted

Data Processing - Payroll

Control Objective 6: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored and deviations are resolved, and that payroll data is processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
6.01	Payroll processing procedures for the ADP payroll Regions have been documented and provide overall guidance to ADP personnel and are available through the ADP Intranet.	Inspected payroll processing procedures documentation for the ADP payroll Regions to determine whether the procedures were documented and provided overall payroll processing guidance to ADP personnel and are available on the ADP Intranet.	No deviations noted
6.02	Automated payroll processing jobs are executed to process client payroll based on information entered, statutory regulations, and client defined requirements.	For a sample test client in the Payroll Application production environment, executed a sample payroll run and performed the following to determine whether automated payroll processing jobs are executed to process client payroll based on information entered, statutory regulations, and client defined requirements:	No deviations noted
		Salary Employee Inspected the pay rate from the employee profile maintained in the input system for a sample of employees and inspected the agreed pay rate amount to the payroll register generated upon completion of the selected payroll run.	No deviations noted
		Inspected the relevant tax withholding settings and deduction screen maintained in the input system for a sample of employees and: • agreed the amounts for any deductions to the payroll register	No deviations noted

Control Objective 6: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored and deviations are resolved, and that payroll data is processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
		generated upon completion of the selected payroll run; and • recalculated the amounts for any tax withholdings and any 401k deductions and agreed those amounts to the payroll register generated upon completion of the selected payroll run.	
		Hourly Employee Inspected the pay rate from the employee profile maintained in the input system for a sample employee and recalculated the gross payroll based on the regular hours and overtime hours and agreed the gross payroll amount to the payroll register generated upon completion of the selected payroll run.	No deviations noted
		Inspected the relevant tax withholding settings and deduction screen maintained in the input system for the sample employee above and • Agreed the amounts for any deductions to the payroll register generated upon completion of the selected payroll run, and • Recalculated the amounts for any tax withholdings and any 401k deductions and agreed those amounts to the payroll register generated upon completion of the selected payroll run.	No deviations noted

Control Objective 6: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored and deviations are resolved, and that payroll data is processed completely and accurately.

Ref	Description of Control Activity	Test of Controls	Results
6.03	At the end of each production day, the Prelist/Editing group reviews the status of jobs processed and notifies Operations and/or Client Services to confirm job completion status and any identified issues requiring further investigation and resolution.	For a sample of days and Region LPARs, inspected the End-of-Day Checklist to determine whether the Prelist/Editing personnel reviewed the status of jobs and identified issues were documented and followed up to resolution.	No deviations noted
		Observed a member of the Prelist/Editing group inspecting status screens at the end of a sample day and clearing "inventory" screens for a sample of Regional LPARs to determine whether job completion status was reviewed and any identified issues were reviewed and confirmed.	No deviations noted

Control Objective 6: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored and deviations are resolved, and that payroll data is processed completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
6.04	Automated reconciliations are performed daily and weekly to compare the Payroll Ledger to the EMP totals for each client. The Quality Control group reviews the reconciliation report and investigates any differences to resolution.	Inspected the out-of-balance report job schedule in the Payroll Application to determine whether the reconciliation to compare the Payroll Ledger to the EMP totals for each client is scheduled to run automatically daily and weekly.	No deviations noted
		Observed a member of the Quality Control group performing a review for a sample daily and weekly reconciliation report to determine whether any differences identified between the Payroll Ledger and the EMP totals were investigated and resolved.	No deviations noted
		Observed a client reconciliation difference being generated and inspected the corresponding daily and weekly reconciliation reports to determine whether the difference was accurately presented on the reconciliation reports.	No deviations noted

Data Output – Workforce Now

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
7.01	Data transmissions files and output report files between the Workforce Now Application, clients, other ADP systems, and third party administrators take place using standard encryption methods, including Secure Socket Layer (SSL).	Inspected a sample data file and output report file made available to clients and/or other ADP systems to determine whether Secure Socket Layer (SSL) technology encryption was used during transmission. Inspected the ADP Internet-based products to determine whether a valid password and ID was required for successful authentication and whether SSL technology encryption was in place to secure transmission of payroll data.	No deviations noted No deviations noted
7.02	During the export of pay data, the Workforce Now Application displays and records in a log error and warning messages related to the status of the export file.	Observed a QA engineer export pay data for a client to determine if error and warnings messages related to the status of the export file are displayed in the Workforce Now Application. Observed the pay data export log to determine whether error and warning messages are logged and available for review.	No deviations noted No deviations noted
7.03	Client users with Manager, Participant, and Time & Attendance Supervisor profiles have access to generate reports. The applications display error and warning messages	Observed an ADP Associate login as the Manager, Participant and Time & Attendance Supervisor profiles, to determine whether users with Manager, Participant and Time & Attendance Supervisor profile have access to	No deviations noted

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
	related to the status of the reports generated.	generate reports in the Workforce Now Application, and that users with the Employee role cannot generate reports in the Workforce Now Application. Observed the process for generating reports from the Workforce Now Application to determine whether error and warning messages related to blank data and missing fields were displayed on screen during the report generation.	 No deviations noted
Enhanced Time Service			
7.04	The Enhanced Time application provides the ability for clients to restrict access to generate reports and export files based on roles and permissions in the application.	Inspected the Enhanced Time application functionality to determine whether clients can configure roles and profiles to restrict report generation access.	No deviations noted
7.05	Status messages are automatically generated on screen and subsequently recorded in an application log file to notify the client when a report or export file is generated successfully or unsuccessfully with errors.	For a sample test client, inspected the Enhanced Time application status screens to determine whether: • The resulting log files for a successfully generated report and export file were automatically generated and subsequently recorded in the application log file indicating the report and export file were generated successfully (i.e., complete). • The resulting log files for an unsuccessfully generated report and export file were automatically generated and subsequently recorded in the application log file	No deviations noted

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
		indicating the report and export file were generated unsuccessfully (i.e., incomplete).	
Payroll Service			
7.06	Client output reports (e.g., payroll register, payroll journal) and data files (e.g., MAS GLI, other payroll-related output, money movement, and direct deposit) are automatically generated from the Payroll Application upon completion of each payroll run.	For a sample test client in the Payroll Application production environment, executed a sample payroll run and inspected the following reports to determine whether the reports were automatically generated, transmitted to iReports and the payroll information (gross pay, net pay, taxes) was accurately and completely produced: • AutoPay Master Control (AMC) • Payroll Register • Unused Deduction Report • Payroll Audit Report • Payroll Summary • Labor Cost Report • Statistical Summary Report	No deviations noted
		Observed the data files being automatically generated from the Payroll Application for a sample of each of the following data files for a sample client and selected a transaction from each file and compared the payroll information (net pay amounts, control totals) from the file to amounts in the Payroll Application to determine whether the amounts were completely and accurately produced: • NAS ADP GL data file • MAS GLI data file	No deviations noted

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	Description of Control Activity	Test of Controls	Results
		• Other payroll related files • Money movement file • Direct deposit file	
7.07	Client output reports (e.g., payroll register, payroll journal) and other payroll-related data files are automatically transmitted and made available to Workforce Now clients through iReports output reports or Workforce Now Application data files.	For a sample test client in the Payroll Application production environment, executed a sample payroll run and inspected the following output reports to determine whether the reports were automatically transmitted to iReports and made available to Payroll Services clients: • Master Control (AMC) • Payroll Register • Unused Deduction Report • Payroll Audit Report • Payroll Summary • Labor Cost Report • Statistical Summary Report	No deviations noted
		For a sample test client in the Payroll Application production environment, executed a sample payroll run and inspected the payroll-related data files to determine whether the data files are automatically transmitted to the input system.	No deviations noted

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
7.08	The Corporate Systems Engineering group monitors the results of data file (e.g., iReports, MAS GLI file, and general ledger) and output report file transmissions and is alerted of any identified issues or exceptions. Issues are documented, reported, and followed up on to resolution.	Observed a member of the Corporate Systems Engineering group monitoring data file transmission alerts on a sample day to determine whether automated monitoring tools are used to monitor for issues or exceptions with data file transmissions between the Workforce Now Application and the Payroll Application.	No deviations noted
		For a sample of identified transmission issues, inspected the related problem resolution tickets to determine whether monitoring was performed and identified transmission problems were documented and followed to resolution.	No deviations noted
7.09	For client output reports printed by ADP, the Regional Payroll Production Operations group monitors the transmissions of the output print files from the Payroll Application to the ADP printers and is alerted of any identified issues or exceptions and that exceptions are followed up on to resolution.	For a sample of Region LPARs, observed a member of the Regional Payroll Production Operations group monitoring the transmissions of output print files on a sample day to determine whether issues were documented and followed up to resolution.	No deviations noted
7.10	Production Support and Quality Control personnel review printed client output reports and electronic media for defects.	For a sample of Region LPARs, observed a Production Support and Quality Control associate review client-output reports and electronic media on a sample day to determine whether printing defects were identified and resolved.	No deviations noted

Control Objective 7: Controls provide reasonable assurance that benefits administration, payroll, and time & attendance output data is transmitted completely and accurately to clients.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
7.11	Print Operations Quality Control personnel are restricted from having access to modify the output print files within the Payroll Application and Operations Center system.	Inspected the access rights screen within the Payroll Application for the Operations Quality Control personnel to determine whether the Quality Control personnel were restricted from having access within the Payroll Application to modify the output print files.	No deviations noted
		Inspected the system-generated user listing for the Print Operations RACF group and inquired of the Program Manager-Technical Services to determine whether access to client data in the Payroll Application was restricted to appropriate personnel based upon job responsibilities.	No deviations noted

Data Output - Payroll (Money Movement/Direct Deposit Files)

Control Objective 8: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the Payroll Application to the ADP Compliance and Payment Solutions (CAPS) systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.01	Money movement/direct deposit files are automatically generated from the Payroll Application upon completion of each client payroll processing run.	For a sample client and payroll run, inspected the money movement and direct deposit files to determine whether the files were automatically generated from the Payroll Application upon completion of the payroll cycle.	No deviations noted
		For a sample client and payroll run, inspected the money movement in the Payroll Application and direct deposit file to determine whether the payroll information (net pay amounts) agreed to the corresponding records contained in the Payroll Application.	No deviations noted
8.02	Direct deposit files are automatically sent to the ADP ETS system for retrieval or transmitted directly to the client bank in accordance with client specifications.	For a sample of days and Region LPARs, inspected the output file to determine whether the direct deposit file was automatically generated from the Payroll Application and transmitted to the ADP ETS system or client bank in accordance with client specifications.	No deviations noted

Control Objective 8: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the Payroll Application to the ADP Compliance and Payment Solutions (CAPS) systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.03	The Banking group confirms by telephone, VRU or fax, depending on arrangements made with the bank that the bank's total number of payments and the total monetary amount received agree to totals within the Payroll Application.	For a sample client and payroll run, observed an ADP Banking associate confirm bank totals with the client over the phone on a sample day to determine whether the bank's total number of payments and total monetary amount received agreed to the totals within the Payroll Application. For a sample of days and Region LPARs, inspected the ACH Load Control Recap screen to determine whether the Banking group confirmed the bank's total number of payments and the total monetary amount received agree with the total in the Payroll Application.	No deviations noted No deviations noted
8.04	Clients electing Full Service Direct Deposit (FSDD) of payrolls complete an authorization form (e.g., the "Client Account Agreement") that is signed by both the client ADP's Risk and Compliance Group.	For a sample of clients that elected FSDD, inspected the "Client Account Agreement" form and the Payroll Application to determine whether the form was completed and signed (approved) by the client, and the FSDD was set up per the client request.	No deviations noted
8.05	Client money movement files (e.g., FSDD and ADPCheck) are automatically transmitted to ADP's CAPS system upon completion of each payroll run.	For a sample payroll run and client, inspected the money movement file to determine whether the file was automatically generated from the Payroll Application and transmitted to ADP's CAPS system upon completion of the payroll run.	No deviations noted

Control Objective 8: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the Payroll Application to the ADP Compliance and Payment Solutions (CAPS) systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.06	Banking personnel review the transmission status and compare the information available on the Payroll Application to the information available on the CAPS system. Identified differences are followed–up in order to resolve them promptly.	For a sample of days and LPARs, inspected reconciliation documentation prepared by the ADP Banking personnel and re-performed a sample review between the Payroll Application records and ADP's CAPS system records to determine whether the review was performed accurately, and timely action was taken to resolve any out-of-balance conditions.	No deviations noted

GENERAL COMPUTER CONTROL OBJECTIVES AND CONTROLS

Application Development and Change Management

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.01	A formal and documented application development and change management policy has been developed to guide the in-scope applications' development groups.	Inspected the application development and change management policy to determine whether development requirements were documented for application development projects to guide the in-scope applications' development groups.	No deviations noted
9.02	Change requests to the in-scope applications are formally documented and authorized by appropriate ADP management.	For a sample of changes made to each of the in-scope applications, inspected the relevant change documentation to determine whether the change request was documented and authorized by appropriate ADP management.	No deviations noted

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.03	Changes to in-scope application are tested (unit, regression, functional testing and peer-reviewed) in a segregated test environment and the results are approved by ADP management prior to deployment.	For a sample of months, inspected test documentation for the major releases to the Payroll Application to determine whether testing was executed, and the test results were documented and approved by ADP management prior to deployment.	No deviations noted
		For a sample of minor changes made to the Payroll Application, inspected test documentation to determine whether testing was executed, and test results were documented and approved by ADP management prior to deployment.	No deviations noted
		Inspected the relevant Payroll Application system configurations to determine whether separate development, test and production environments were established.	No deviations noted
9.04	Changes to the in-scope applications are approved for migration to the production environment by ADP Management prior to deployment.	For a sample of changes made to each of the in-scope applications, inspected the relevant change documentation to determine whether the change was approved by the project manager prior to deployment to production.	No deviations noted

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.05	Access to deploy application version upgrades and service packs to the production environment is restricted to properly authorized personnel based on job function.	Inspected the user listing of ADP personnel with the access to deploy application version upgrades and service packs to the in-scope applications' production environments and inquired with ADP management and obtained job titles for each user to determine whether the users were authorized and appropriate based upon job responsibility.	Deviations noted For five (5) out of twenty-eight (28) users with access to deploy changes to production for Workforce Now, access was no longer required based on the user's job role and function. *Refer to the end of this Control Objective section for additional procedures performed by Ernst & Young and Management's Response.*
Payroll Application Only			
9.06	Source code is controlled and monitored using version control systems in the development environment. Only a limited number of authorized personnel have access to source code system in the development environment.	Inspected the system-generated listing of users with the ability to migrate code to the Payroll Application production environment, compared the users against the system-generated listing of developers with access to the version control system, and inquired of the Director of Mainframe Security to determine whether source code was controlled using the ChangeMan version control system and	No deviations noted

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	Description of Control Activity	Test of Controls	Results
		access to migrate code to the production environment was appropriate based on the individual's job responsibility and excluded those responsible for development functions.	
Enhanced Time Application Only			
9.07	*MOTIF Account Request Tool* Changes to the MOTIF Account Request Tool follow a formal change management process that includes authorization, testing, and approval prior to deployment into the production environment.	For a sample of changes, inspected the supporting documentation to determine whether the change was authorized, tested, and approved prior to deployment into production.	No deviations noted
9.08	*MOTIF Account Request Tool – Authorized Access* The ability to develop changes and promote changes to production is appropriately restricted to authorized personnel. *Note: While users have the ability to develop and promote changes, control 9.09 is designed to require an independent second-level review before a change can be promoted, enforcing segregation of duties.*	Inspected the user listing of ADP personnel with access to develop and promote changes to MOTIF to determine whether the users were authorized and their access was appropriate based upon job responsibility.	No deviations noted

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.09	*MOTIF Account Request Tool –Review* Program changes to the MOTIF Account Request tool require an independent second-level review prior to promotion to production.	Inspected the source code repository configuration to determine whether the tool is configured to require an independent second-level approval prior to promoting a change to production.	No deviations noted
		For a sample of changes, inspected the source code repository tool to determine the change was approved by two separate individuals prior to deployment to production.	No deviations noted
		Inspected the user listing of ADP personnel with access to change the source code repository configuration settings to determine whether they are segregated from the development team.	No deviations noted
9.10	*MOTIF Account Request Tool – Notification* An automated email notification is sent to the MOTIF Development Operations team when a change is promoted to production.	Inspected the MOTIF Account Request Tool settings to determine that the tool is configured to generate an automated email when a change is promoted to production.	No deviations noted
		For a sample change, inspected the associated email to determine whether an email is automatically generated and sent to the MOTIF Development Operations team when a change is promoted to production.	No deviations noted

Control Objective 9: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.11	*MOTIF Account Request Tool – Code Compare* A script runs daily in the Task Scheduler to compare the MOTIF Production Release File fingerprint to the Development File fingerprint. A daily automated email is generated and sent to the MOTIF team with the results of this script.	Inspected the Task Scheduler and the script to determine whether the script was scheduled to run on a daily basis and was configured to automatically send an email containing the results of the file compare.	No deviations noted

Additional Procedures Performed by Ernst & Young:

Control 9.05 – *Workforce Now Application*

For five (5) out of twenty-eight (28) users with access to deploy changes to Workforce Now that was no longer appropriate, EY reviewed available logs and validated that the users did not log into the change deployment tool during the period. Additionally, EY inspected evidence to validate that the users' accounts were disabled as of June 16, 2020 following the identification of the inappropriate access and determined that the users did not log into the change deployment tool and that there were no unauthorized changes migrated by the users after the access was considered to be inappropriate.

Management Response to Testing Deviations:

Control 9.05 – *Workforce Now Application*

Management agrees that access to deploy changes to Workforce Now for five (5) out of twenty-eight (28) users was no longer necessary. Management reviewed log files and determined that the users did not log into the change deployment tool after the access was considered to be inappropriate. Management confirmed that access for each associate no longer requiring access was disabled.

Operating Systems (OS) and Database Change Management (Payroll Application Only)

Control Objective 10: Controls provide reasonable assurance that the implementation of and changes to operating system software and data management systems and network infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	Description of Control Activity	Test of Controls	Results
10.01	ADP has established a formal Change Management Process that outlines the requirements for making operating system (OS) and database changes. The process is documented and maintained by ADP management.	Inspected the Change Management Process document to determine whether requirements for making changes to the Payroll Application operating system and database were documented.	No deviations noted
10.02	Operating system and database changes to the Payroll Application production environment are authorized, tested, and approved by the Change Approval Board (CAB) prior to deployment.	For a sample of operating system and database changes to the Payroll Application production environment, inspected change orders and testing documentation to determine whether the related change was authorized, tested, and approved by the CAB prior to deployment.	No deviations noted

Control Objective 10: Controls provide reasonable assurance that the implementation of and changes to operating system software and data management systems and network infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
10.03	Access to deploy operating system and/or database changes to the Payroll Application production environment is restricted to appropriate personnel.	Inspected the RACF user access listing to identify individuals with the ability to migrate operating system and database changes to the Payroll Application production environment, inspected job titles and inquired of the Senior Director – Technical Services to determine whether access was appropriate based on job responsibilities.	No deviations noted
		For a sample of operating system and database changes to the Payroll Application production environment, inspected the change order ticket, RACF user access listing, and inquired of the Senior Director – Technical Services to determine whether the change was deployed by authorized personnel.	No deviations noted

Logical Security

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.01	ADP associates accessing the iReports output system and Workforce Now Application are required to authenticate using a valid user ID and password that comply with the ADP's security policies and standards.	Inspected the relevant password configuration settings governing access to each of in-scope applications and the documented Information Security Standards to determine whether password settings (history, length, expiration, complexity) comply with ADP's security policies and standards.	No deviations noted
		Observed an ADP associate attempt to authenticate to the iReports output system and Workforce Now Application to determine whether a valid user ID and password was required to access the systems.	No deviations noted
11.02	Client users require a valid user ID and password for authentication to the iReports output system and the Workforce Now Application.	Inspected the log in screen for the iReports output system and the Workforce Now Application to determine whether a valid user ID and password were required for authentication to the systems.	No deviations noted
		Observed an ADP associate attempt to authenticate to a sample system to determine whether a valid user ID and password were required to access the applications.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.03	Only appropriate ADP associates have access to the administrative functionality for the iReports output system and Workforce Now Application.	For a sample of users granted administrative-level privileges the iReports output system and Workforce Now Application, inquired of ADP management regarding the job responsibilities and inspected job titles to determine whether access was restricted to authorized personnel.	No deviations noted
11.04	The Workforce Now Application provides the ability for clients to restrict user access based on roles and functions.	Inspected the Workforce Now Application security screens to determine whether the applications provide the ability for clients to manage user access based on roles and functions within both applications.	No deviations noted
11.05	User access additions and modifications to the iReports output system and Workforce Now Application require authorization from appropriate ADP management. Changes are documented and executed.	For a sample of user access additions and modifications: • Inspected the ticket to determine whether the request to grant access to the iReports output system and Workforce Now Application was documented and authorized by appropriate ADP management. • Inspected system-generated user access listings from the iReports output system and Workforce Now Application to determine whether access was granted as requested.	Deviations noted For three (3) of twenty-five (25) new users granted access to the Workforce Now Application, through the SMS tool, documentation of the request and approval could not be provided. *Refer to the end of this Control Objective section for additional procedures*

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
			performed by Ernst & Young and Management's Response.
11.06	User access deletions to the iReports output system and Workforce Now Application require authorization from appropriate ADP management. Changes are documented and executed.	Inspected a screenshot of the configured job schedule and a sample termination email notification to determine whether a nightly job is scheduled to run automatically to remove terminated Active Directory users from the iReports output system and the Workforce Now Application. For a sample of user terminations inspected system-generated user access listings from the iReports and the Workforce Now Application to determine whether access was revoked as requested.	No deviations noted No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	Description of Control Activity	Test of Controls	Results
11.07	Auditing has been enabled at the application level for the Workforce Now Application. Transactional data is logged with the user ID of the person who initiated the transaction and is available for review.	Inspected the relevant configuration settings within the Workforce Now Application to determine whether auditing was enabled and transactional data was being logged and made available for review. Observed a Technical Services Manager log into the Workforce Now Application and make changes to a sample employee's compensation rate and effective date, and inspected the Employment Actions Audit Report and modification history screen within the Workforce Now Application to determine whether the employee compensation changes and the user ID of the operator who made the change were logged and available for review.	No deviations noted No deviations noted
11.08	Only authorized individuals have update access to the production database.	For a sample in-scope application production databases, inspected the system-generated listings of users with update access, inquired of ADP Management, and inspected job titles, to determine whether access was limited to authorized individuals based on job responsibilities.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Payroll Application			
11.09	Only appropriate ADP associates have access to the administrative functionality for the Payroll Application and key mainframe datasets.	Inspected the system-generated listings of users with access to the key mainframe datasets in the Payroll Application and inquired of Corporate Mainframe Security management regarding job responsibilities to determine whether access was restricted to authorized personnel.	No deviations noted
11.10	User access additions and modifications to the Payroll Application requires authorization from appropriate ADP management. Changes are documented and executed.	For a sample of user access additions and modifications: • Inspected the ticket to determine whether the request to grant access to the Payroll Application was documented and authorized by appropriate ADP management. • Inspected system-generated user access listings from the Payroll Application to determine whether access was granted as requested.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.11	The Corporate Mainframe Security group configures the audit policy within the Payroll Application so that an audit log of operator activity is generated. The audit logs are available for review and provide a record of device access, configuration changes, and user actions.	Observed the Senior Director – Technical Services log into a sample production LPAR on a sample day and process a sample command, and inspected the corresponding audit log to determine whether the Payroll Application logged the activity.	No deviations noted
		For a sample of Region LPARs, inspected the relevant audit log settings to determine whether the Payroll Application was configured to generate the audit log of the operator's activities.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	Description of Control Activity	Test of Controls	Results
11.12	On a bi-weekly basis, a mainframe job is executed by Mainframe Security personnel to identify terminated employees with an active RACF user ID, and revoke their access to the Payroll system.	Inspected the configuration of the relevant mainframe terminations job within the Payroll Application to determine whether the script was configured to run on a bi-weekly basis and disable RACF accounts belonging to terminated users on the HR listing.	No deviations noted
		For a sample of weeks, inspected the script output from the mainframe job to determine whether the job was executed by Mainframe Security personnel, terminated employees with an active RACF user ID were identified, and access was revoked from the Payroll Application.	No deviations noted
		For a sample week, inspected a sample terminated employee identified on the mainframe termination job script output and in the Payroll Application to determine whether access was revoked following execution of the mainframe termination job.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.13	The Corporate Mainframe Security group has set up automated scripts that run periodically and automatically delete inactive RACF accounts and mark users with extended (administrative) privileges for additional investigation.	Inspected the configuration of the relevant automated script within the Payroll Application to determine whether the script was configured to run periodically (i.e., monthly) and delete inactive RACF accounts and flag users with extended (administrative) privileges.	No deviations noted
		For a sample of months and LPARs, inspected the RACF inactivity report, email sent to the ES information security team, and the RACF user listing to determine whether the automated script was run to automatically delete inactive RACF accounts and administrator accounts were flagged for investigation.	No deviations noted
		For a sample month and LPAR, inspected a sample inactive RACF account on the inactivity report and the RACF user listing to determine whether the account was deleted following execution of the automated script.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.14	ADP business partners, IT Engineering and Global Product & Technical Services review the list of business and IT users with RACF mainframe access on an annual basis. In addition, IT Management reviews the list of IT users (i.e., DBA, Storage Management, CICS, MVSSYS) on a quarterly basis. Additions and deletions are communicated to M&MTAM Technical Services for updates.	Inspected the access recertification tool and RACF application review documentation to determine whether the Business Engineering Solutions team and Operations Executives completed the annual review of RACF accounts for business users.	No deviations noted
		For a sample of quarters, inspected the confirmation emails and user listings to determine whether IT Management completed the review of RACF accounts belonging to IT users.	No deviations noted
		For a sample of changes requested during the annual and quarterly reviews, inspected updated user listings to determine whether identified changes were communicated to M&MTAM Technical Services and completed.	No deviations noted
		For a sample annual and quarterly review, inquired of the M&MTAM Manager and re-performed the review for a sample of users to determine whether the process to review access on the Payroll Application was complete and accurate.	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Enhanced Time Application			
11.15	*MOTIF Authentication* ADP associates with support job responsibilities accessing client environments are required to authenticate through a unique user ID, and a password that is compliant with the Information Security Standards, when requesting temporary access to the environment.	Observed an ADP associate accessing a sample client environment to determine whether they are required to authenticate through a unique user ID and password that is compliant with the Information Security Standards. Inspected the user listing of ADP associates that access client environments to determine whether unique user IDs are assigned.	No deviations noted No deviations noted
11.16	*MOTIF User Access Management (Active Directory Network Groups)* User account additions, modifications, and deletions require authorization from appropriate ADP management. Changes are documented and executed by an individual separate from the requestor according to policy and as requested.	For a sample of employee and contractor account additions and modifications, inspected the documented network user access notification and current system user listing to determine whether the access was requested by appropriate ADP management and the access was granted as requested by an individual separate from the requestor. For a sample of employee and contractor terminations (i.e., deletions), inspected the documented network user access notification and network user access listing to determine whether the access was revoked.	No deviations noted No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	Description of Control Activity	Test of Controls	Results
11.17	*MOTIF (Active Directory Network Groups) Password Policies* Password rules/restrictions are enforced at the network-level according to policy.	Inspected the network password configuration settings to determine whether password policies were enforced and configured in accordance with ADP security policies and standards.	No deviations noted
11.18	*MOTIF - User Access* ADP access to client environments is restricted to authorized personnel.	For a sample of ADP personnel with access to the MOTIF Account Request Tool, inspected the current access granted and inquired of TLM management to determine whether such access was authorized and appropriate based upon job responsibilities.	No deviations noted
11.19	*MOTIF – Temporary User Access* Temporary access to client environments is disabled nightly.	For a sample user with temporary access, inspected the password expiration configuration to determine the password was configured to expire nightly. For a sample temporary access request, inspected supporting documentation to determine the temporary access expired overnight.	No deviations noted No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	Description of Control Activity	Test of Controls	Results
11.20	*MOTIF Temporary Access Review* Requests for temporary access to client environments are logged and reviewed on a monthly basis. Users whose temporary access is not approved have their access revoked. For any temporary access requests that were rejected during the monthly review, or if a manager did not respond, TLM management conducts a review of the activity performed by the individual in the specific client for which the access request was made to determine whether any unauthorized activity occurred.	For a sample of months, inspected the evidence of the review of ADP associates who requested a temporary password to access client environments to determine whether the review was performed, and for any issues identified as a result of the review, TLM management reviewed access logs to determine whether any unauthorized activity occurred. Inspected the configuration setting of the stored procedure to determine whether user access is disabled if the access is not approved.	No deviations noted No deviations noted
11.21	*MOTIF Super User Account* Access to the Super User account within the MOTIF Account Request Tool is restricted to properly authorized personnel based on job function.	Inspected the list of ADP accounts with access to the Super User account within the MOTIF Account Request Tool and inquired with TLM management to determine whether access to the account(s) was restricted to authorized personnel based upon job responsibilities. Inspected the listing of ADP associates with elevated access to client environments to determine whether unique user IDs are assigned.	No deviations noted No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	***Description of Control Activity***	***Test of Controls***	***Results***
11.22	*MOTIF Administrator Access* Administrator access to the MOTIF Account Request Tool is restricted to properly authorized personnel based on job function.	Inspected the list of ADP personnel with administrator access to the MOTIF Account Request Tool and inquired with TLM management to determine whether access is restricted to authorized personnel based upon job responsibilities.	No deviations noted
11.23	*ADP Portal (SMS) Authentication* ADP associates and client administrators authenticate to the Enhanced Time application via SMS using a unique user ID and password.	Inspected a list of users with access to the Enhanced Time application portal to determine whether users were granted a unique user ID to log on to the system. Inspected the configuration in SMS to determine whether ADP associates and client administrators authenticate to the Enhanced Time application using a unique user ID and passwords.	No deviations noted No deviations noted
11.24	*ADP Portal (SMS) Password Parameters* Password parameters are automatically enforced for all users of the Enhanced Time application via the users' SMS accounts. Password parameters are configured in accordance to ADP security policies and standards.	Inspected the password configuration settings to determine whether password policies were enforced and configured in accordance with ADP security policies and standards.	No deviations noted
11.25	*ADP Portal (SMS) User Access Approvals* For ADP associates, user accounts can only be created in SMS upon receipt of an authorized request submitted through an online SMS	For a sample user with access to Enhanced Time, inspected the access permissions to determine whether the user	No deviations noted

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
	request form. User accounts must be assigned an SMS Enhanced Time role, which provides access to the application	account had to be assigned a role which allows access to client data. For a sample of new accounts that have been provisioned in SMS, inspected the SMS request to determine whether the access was appropriately authorized, set up as requested, and appropriate for the user's job responsibilities.	*10/01/19 – 03/31/20* Deviations noted For two (2) of five (5) new user accounts selected for testing, documentation was not retained to evidence whether the new user account was authorized by an appropriate individual. *04/01/19 – 09/30/19* No deviations noted *Refer to the end of this Control Objective section for additional procedures performed by Ernst & Young and Management's Response.*

Control Objective 11: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
11.26	*ADP Portal (SMS) Access Revocation* Accounts for terminated ADP associates are removed from SMS upon termination.	For a sample of users with access to Enhanced Time via the ADP Portal, inspected the associated access profile and inquired of the user's manager to determine whether access to the ADP Portal is current and did not belong to a terminated ADP associate or contractor.	No deviations noted
		For the population of terminated ADP associates, inspected the current SMS roles and client access lists to determine whether access for the terminated employee was removed.	No deviations noted
11.27	*ADP Portal (SMS) User Access Appropriateness* ADP access to Enhanced Time client environments via the ADP Portal is restricted to appropriate personnel.	For a sample of users with access to Enhanced Time via the ADP Portal, inspected the associated access profile and inquired of the user's manager to determine whether access to the ADP Portal is current and did not belong to a terminated ADP associate or contractor.	No deviations noted
		For the population of users with access to Enhanced Time via the ADP Portal, inspected the user accounts to confirm that shared or generic accounts are not in use.	No deviations noted

Additional Procedures Performed by Ernst & Young:

Control 11.05 – *Workforce Now Application*

For the three (3) out of twenty-five (25) new users granted access to the Workforce Now Application through the SMS tool, access was provisioned without request and approval documentation, EY obtained retroactive approval of access by the user's manager, to confirm access to the SMS tool (which grants access to the Workforce Now Application) was considered to be appropriate for the identified users currently at the time it was granted.

Control 11.25 – *Enhanced Time*

In response to the identification of two (2) new user deviations, Management reviewed 100% of the new user accounts for the period of October 1, 2019, to March 31, 2020, to determine whether the users' access to the Enhanced Time via the ADP Portal was authorized. Of the forty-four (44) new user accounts identified (100% of the population), it was determined that documentation was not retained to evidence whether the new user account was authorized by an appropriate individual for a total of thirty-seven (37) accounts. We obtained and inspected ADP Management's review to determine whether the users' access to Enhanced Time via the ADP Portal was authorized and no further deviations were noted. Additionally, ADP Management reaffirmed the requirement to retain documentation to evidence the authorization of new user accounts with the responsible associates.

Management Response to Testing Deviation:

Control 11.05 – *Workforce Now Application*

Management agrees that documentation of request and approval for three (3) new ADP associates granted access to Workforce Now Application through the SMS Access tool was not properly maintained. Management noted that the access for the three (3) new ADP associates was confirmed as being appropriate based on their job function and responsibilities. Also, the access granted was found to be appropriate at the time of the request. Management identified control 11.07 as a compensating control in that it serves to mitigate any potential risk with logging of changes to client data which allows clients to identify unauthorized activity and notify ADP of any discrepancies. Management has since reeducated the associates on the document retention procedures for access provisioning.

Control 11.25 – *Enhanced Time*

Management agrees that documentation was not retained to evidence whether the new user account was authorized by an appropriate individual for two (2) of five (5) new user accounts selected for testing. In response to the deviations, Management reviewed 100% of the new user accounts for the period October 1, 2019, to March 31, 2020, to determine whether the users' access to Enhanced Time via the ADP portal was authorized. Of the forty-four (44) new user accounts identified (100% of the population), documentation was not retained to evidence whether the new user account was authorized by an appropriate individual for a total of thirty-seven (37) accounts. For the remaining seven (7) accounts, appropriate documentation of authorization was identified. For all thirty-seven (37) new user accounts without documentation of authorization, Management determined that the users' manager provided authorization outside of the access request form that was not retained. Management performed an evaluation of thirty-seven (37) new user accounts and determined that their access to Enhanced Time via the ADP Portal was authorized and was appropriate at the time the accounts were created. ADP Management reaffirmed the requirement to retain documentation to evidence the authorization of new user accounts with the responsible associates.

Problem Management

Control Objective 12: Controls provide reasonable assurance that problems and client inquiries are recorded and resolved on a timely basis.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
12.01	A problem management case is automatically generated for third party data error files received for a client. The errors are reviewed and resolution notes are documented by the Benefits Representative.	For a sample third party data error file, inspected the problem management case to determine whether it was automatically generated. For a sample of third party data error files, inspected the problem management cases and resolution notes to determine whether third party data errors were documented, reviewed, and resolved by a Benefits Representative.	No deviations noted No deviations noted
12.02	Employee Service Center (ESC) associates use formal and documented client requirements to guide them in performing services for each client.	For a sample of clients, inspected the client requirements to determine whether they were documented and were available to ESC personnel.	No deviations noted
12.03	ADP associates are responsible for properly documenting incidents (system issues and client inquiries) in the problem management system, determining the priority of the issue, and resolving the issue.	For a sample of incidents, inspected the problem management case to determine whether the issue was recorded, given a priority, investigated and the resolution was documented.	No deviations noted
12.04	The TLM Service Center group documents phone and email interactions, including exceptions, problems, and errors, with clients in the Siebel problem management systems.	For a sample of Siebel cases, inspected the case details to determine whether client inquiries via phone and email, including exceptions, problems, and errors, are documented in the Siebel systems.	No deviations noted

Control Objective 12: Controls provide reasonable assurance that problems and client inquiries are recorded and resolved on a timely basis.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
12.05	Siebel cases are given a priority level and assigned to a member of the TLM Service Center group, based on prior client interaction, necessary skill set, and nature of the issue at hand for resolution.	For the same sample of Siebel cases as noted in 12.04 above, inspected the case details to determine whether cases were prioritized, assigned to members of the TLM Service Center group, and resolved.	No deviations noted
12.06	Open Service Requests (cases) and aging reports are reviewed by the Client Service Managers or TLM Service Center Management periodically and case notes are updated to provide a status of the open issue.	For a sample of open Service Requests, inspected the ticket documentation and case notes to determine whether open issues were monitored and the case notes were updated periodically to provide a status of the open Service Request. Observed the Tableau system to determine whether open case and aging reports are available to TLM Service Center Management for review and monitoring.	No deviations noted No deviations noted

Control Objective 12: Controls provide reasonable assurance that problems and client inquiries are recorded and resolved on a timely basis.

Ref	Description of Control Activity	Test of Controls	Results
12.07	If a client issue cannot be resolved by the Client Services group or the TLM Service Center group, the issue is escalated to Client Product Support (CPS) or Technical Support Services group, respectively, for additional support. The Technical Service group tracks the escalated issue in the ticket and notifies the requester when the issue is resolved. If the CPS group cannot resolve the issue, it is escalated to QA.	For a sample of client issues that were escalated to CPS and QA, inspected the CRM system records and the QA tickets to determine whether the described procedures were followed and that the issues were either resolved or in the process of being resolved. For a sample of Serena Business Manager tickets escalated from the TLM Service Center group, inspected the Serena Business Manager ticket details to determine whether the issues were resolved and the requester was notified of the resolution.	No deviations noted No deviations noted
12.08	Issues that cannot be resolved by the TLM Service Center or Technical Support Services group are escalated to the GETS US organization for resolution by creating a ticket in the Service Desk Problem Management system. The GETS US organization tracks the escalated issues in the ticket and notifies the requester when the issue is resolved.	For a sample of Service Desk tickets escalated from the TLM Service Center and Technical Support Services groups, inspected the Service Desk ticket details to determine whether the issues were resolved and the requester was notified of the resolution.	No deviations noted

Control Objective 12: Controls provide reasonable assurance that problems and client inquiries are recorded and resolved on a timely basis.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Enhanced Time Service			
12.09	Members of the Solution Center are responsible for documenting and tracking application/support issues communicated by the client through the Siebel tool.	For a sample of application/support issues communicated from clients, obtained and reviewed the supporting documentation in the Siebel tool to determine whether the issues were documented and tracked.	No deviations noted
12.10	Issues not resolved within the tiered groups of the Solution Center are escalated to IT Operations and a ticket is opened to track the status of the issue through to resolution.	For a sample of application/support issues communicated by clients and escalated for not being resolved within the tiered groups of the Solution Center, obtained and reviewed the supporting documentation to determine whether IT Operations was notified and a ticket was opened to track the issue.	No deviations noted
12.11	The Team Leads and Solution Center managers monitor the progress of urgent cases to verify that cases are responded to and worked timely.	Observed the Siebel dashboard to determine whether urgent cases are being monitored by Solution Center managers in real-time. For a sample of application/support issues, obtained and inspected associated Siebel tickets to determine whether urgent cases were responded to and worked timely.	No deviations noted No deviations noted
12.12	Open Service Requests (cases) are reviewed by the Solution Center Managers periodically and case notes are updated to provide a status of the open issue.	For a sample of open Service Requests, inspected the ticket documentation and case notes to determine whether open issues were monitored and the case notes were updated periodically to provide a status of the open Service Request.	No deviations noted

SECTION FIVE

OTHER INFORMATION PROVIDED BY ADP

ADP GLOBAL BUSINESS RESILIENCY PROGRAM

ADP has taken significant steps to mitigate the impact of business interruption resulting from a variety of potential events, including the loss of key facilities and resources. A Global Business Resiliency Policy and Program have been developed, in compliance with applicable regulations and guidelines, to establish a single, global framework that addresses how ADP manages and controls identified risks resulting from disasters and other significant business-disruptive events.

Disaster Recovery Planning

Disaster Recovery plans have been developed to address a disaster impacting the data centers and to provide immediate response and subsequent recovery from any unplanned service interruption.

Disaster Recovery plans have been developed to:

- Provide an organized and consolidated approach to managing response and recovery activities following an unplanned incident or business interruption, to avoid confusion and to reduce exposure to error
- Provide prompt and appropriate response to any unplanned incident and reduce resulting business interruption impacts
- Recover essential business operations in a timely manner, increasing ADP's ability to recover from a loss of an ADP facility

Disaster Recovery plans are designed to create a state of readiness in response to any of the following incident scenarios at ADP Data Centers:

- Incidents causing physical damage such as fire, smoke, or water
- Incidents that indirectly affect facility access such as the need to close a building because of a storm, or evacuate a building in response to a threat or a fire in a nearby facility
- Impending or unexpected regional disasters such as an earthquake, hurricane, typhoon, or flood
- External incidents that could cause a service interruption such as a loss of electrical or telecommunication services

ADP requires that Disaster Recovery plans be reviewed, revised, and tested at least annually; various components may be subject to semi-annual or quarterly reviews and revisions.

Business Continuity Planning

Business Continuity plans have been developed to maintain or restore business operations following interruption to, or failure of, critical business processes and/or systems.

Business Continuity plans are:

- Documented for the critical components of the enterprise
- Based on the results of a thorough Business Impact Analysis and Risk Threat Analysis
- Developed in conjunction with internal systems users
- Subjected to formal change control procedures
- Distributed to all individuals who would need them in case of an emergency
- Kept current and backed-up copies are stored at an offsite location

Business Continuity plans are designed to provide prompt response to, and subsequent recovery from, an unplanned business interruption such as critical service loss (e.g., computer processing, telecommunications), loss of access to a building or a facility catastrophe (e.g., fire, flood). ADP's Business Continuity plans are focused on restoring specific services to clients.

Business Continuity plan components include but are not limited to:

- Crisis Management / Emergency Response
- Incident Detection / First Alert Notification
- Plan Activation
- Recovery Strategies / Recovery Recommendations
- Recovery Procedures, Tasks and Resource Requirements
- Minimum Recovery Configurations
- Plan Administration
- Reports / Forms

ADP requires Business Continuity plans to be reviewed, revised and tested at least annually; various components may be subject to semi-annual or quarterly reviews and revisions.

GSO AND SECURITY OVERVIEW

ADP's Global Security Organization (GSO), led by a Global Chief Security Officer, is comprised of a converged global information security, operational risk, and privacy team staffed by more than 300 associates. The GSO is charged with the design, implementation, and oversight of ADP's corporate-policy based Information Security Program. Each ADP business unit has representatives responsible for maintaining and enforcing ADP's security policies and practices in their business units.

Robust Privacy Practice - ADP's Chief Privacy Officer is responsible for global Privacy Policy development and compliance oversight. ADP deploys global Privacy Policy training that outlines how ADP associates should handle sensitive client data and that fosters compliance with global privacy laws.

Best-of-Breed Technologies - ADP regularly deploys key security technologies including firewalls, Internet content monitoring, enterprise anti-virus, network-based IDS/IPS, hardened hosts, enterprise security incident event-management technology, two-factor authentication for privileged and remote access, robust role-based application access to ADP's applications and data, and network access controls.

'Built-In' vs. 'Tacked on' Security - ADP's secure development processes and quality assurance programs include a wide range of internal services and tools available to developers, quality engineers, and security experts. Penetration testing and source code reviews of core ADP products and services are executed before they are introduced to the Internet, and iteratively thereafter, and ongoing scanning occurs for publicly-known vulnerabilities.

Third Party Assurance – Third party sites and services are reviewed to ensure that ADP's vendors comply with ADP's information security policies and standards.

Continuous Monitoring - ADP has a robust assessment process, aligned with industry best practices, that reviews and regulates adherence to security baseline compliance requirements, security patching, and hardened configurations to reduce risk and exposure to known vulnerabilities, as well as, respond to emerging threats.

Secure Client Data in Motion - Using the latest encryption technologies, ADP protects sensitive client information as it traverses the Internet.

ADP Human Firewall - In accordance with country-specific laws, ADP requires new hires to pass rigorous background checks including criminal record, professional work history, education, etc. ADP provides its associates and contractors with relevant training and continually updates its security and privacy practices.

Threat Management - To manage emerging threats, ADP uses Unified Threat Management methodology that includes multiple technologies, to leverage security information and protect ADP's business and its clients. Intrusion Detection Systems and Deep Packet Inspection are used for identification and analysis of ADP's network traffic. Network based IDS devices/agents are placed throughout ADP's web-hosting infrastructure to monitor network traffic and identify possible attacks or suspicious activity. ADP also uses gateway anti-virus and data loss prevention (DLP) tools.

Data Protection - Protecting client data is an integral part of the trusted ADP-client relationship. ADP's Security Information and Event Monitoring (SIEM) platform is scalable and can feed ADP's Security Information Data Warehouse. Understanding any client-data threat is critical to ADP and it is critical that ADP understands who has access to data, who should have access, and who has accessed this data. When this data is fed into a machine-learning platform and users' data access profiles are developed, unauthorized access attempts or authorized access abuses become apparent.

ADP's DLP system integrates with a wide-range of platforms and endpoints to help identify systems, databases, and repositories with critical or sensitive information. Security alerts for systems with known Personally Identifiable Information (PII), or where sensitive corporate information resides, will be immediately addressed.

Financial Crimes Prevention - ADP's highest priority is to protect client funds and the privacy and security of our clients' data. A fraud detection technology has been added to ADP's existing Trusted Platform Security Infrastructure that is similar to the advanced detection and predictive technologies used at many banking and credit institutions. ADP primarily bases its detections on the schemes and scenarios that have been identified and detected from the information collected from ADP's partners. ADP continuously tests and applies additional indicators including predictive analysis, transaction difference thresholds, and anomaly transaction scoring to identify additional fraudulent events. ADP has built a fraud analysis team tasked with monitoring fraud detection systems and alerts; recognizing and triaging fraud indicators; and charged with the ability to take decisive action to prevent losses resulting from fraudulent events.

Infrastructure Assurance - ADP's hosting centers are protected with multi-tier firewalls configured in accordance to a well-defined access policy. Network based IDS devices/agents are placed throughout the web-hosting infrastructure to monitor network traffic and uncover possible attacks or suspicious activity. ADP uses anti-virus software throughout our infrastructure because of potential viruses, worms, etc. Anti-virus signature files are regularly updated and files passing through the hosting infrastructure are scanned, remediated, deleted, or quarantined based upon the results of the scan.

Security Intelligence - Security Intelligence, a key component of ADP's security operations, collects intelligence from internal and external sources and translates that intelligence into actionable events. The data and analytics come together in the SIDW, a high-speed data warehouse where volumes of data can be searched.

Trusted Platform Management - As risks are identified and tied to possible security incidents, ADP can measure when an identified risk actually impacts an organization. This meaningful data then drives global risk remediation efforts.

Incident & Crisis Management - Staffed with full-time security, privacy, and legal experts, The Incident & Crisis Management team is equipped and staffed to respond to changes in both cyber and physical threats and attack conditions.

PRIOR PERIOD CONTROL MAPPING

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
Control Objective 1: Benefits – Data Input		
1.01	Clients have the ability to import data to the Workforce Now Application using the Import Tool. Any errors that occur during the data import process are recorded in a log and made available for review and follow-up by the client.	Control 1.01
1.02	The Workforce Now Application uses input controls to enforce the complete and accurate input of data: • Data entry validation controls, such as format checks • Mandatory fields • Drop down boxes In the event that incorrect data is attempted to be entered into the system, error messages appear on the users' screen.	Control 1.02
1.03	The Workforce Now Application is accessed via secured "https" website and require a user ID and password for access to input or update data.	Control 7.01
1.04	The Workforce Now Application utilizes a 256-bit Secure Socket Layer (SSL) encryption for the web browser application sessions which adds security for data entry.	Control 1.03
Control Objective 2: Benefits - Data Processing		
2.01	The Workforce Now Application tracks HR, leave, and recruitment information and calculates benefit eligibility and benefits deductions based on the plan information that has been configured according to client specifications.	Control 2.01

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
2.02	Participant data errors may occur with processing of participant information when extracting and formatting data to be sent to third party administrators. Error reports, which include the participants that had errors in their information, are sent to the Comprehensive Benefits group. The Comprehensive Benefits group is responsible for tracking, researching, and resolving these errors.	Control 2.02
2.03	Connection Services staff use the EConnect utility for connection job scheduling. If a job fails after attempting a manual restart, Connection Services group is notified to resolve the issue.	Refer to the *Complementary User Entity Controls* section for *Control Objective #2: Data Processing – Workforce Now (Benefits)* for client responsibility to address any output errors and re-generating reports/exports in a timely manner.
2.04	The FTP with PGP connections use username/password authentication and provide detailed logging of activity.	Control 7.01
2.05	Data transmissions between the Workforce Now Application, clients and third party administrators take place via the EConnect tool. EConnect encrypts and sends or receives and decrypts data transmission using the following protocols: • Secure FTP • FTP with PGP	Control 7.01

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
Control Objective 3: Benefits - Data Output		
3.01	Participant data errors may occur with processing of participant information when extracting and formatting data to be sent to third party administrators. Error reports, which include the participants that had errors in their information, are sent to the Comprehensive Benefits group. The Comprehensive Benefits group is responsible for tracking, researching, and resolving these errors.	Control 2.02
3.02	Users can generate several reports using the Workforce Now Application. When the client selects a report for generation, a version of the report is created in the report output folder. Reports can be generated in several formats including pdf, spreadsheet, and text file. Users can elect to receive an automatic warning message to notify clients if there are problems with the generation of reports.	Control 7.01
3.03	Data file outputs are automatically generated completely and accurately from the Workforce Now Application and transmitted through EConnect. Changes to output files follow the standard application program change management controls.	Control 7.02 Control 7.06 Control 7.07
Control Objective 4: Benefits - Carrier Billing/Invoice Reconciliation and Payment		
4.01	ADP Comprehensive Benefits maintains documented client administrative procedure manuals to provide guidance during the carrier invoicing and billing process.	Control 3.01
4.02	The Workforce Now Application calculates the invoicing amounts based on client parameters and employee enrollments. For clients that have contracted for this service, Comprehensive Benefits personnel use standard invoice processing. For premium remittance clients, ADP uses checklists to process the summary consolidated billing invoices if the client uses ADP to pay the carrier invoices.	Control 3.02

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
4.03	A summary of consolidated invoice information is created and sent to each client on a monthly basis that provides information regarding invoices and amounts due to carriers.	Control 3.03
4.04	For clients that have contracted to have their bills processed according to the carrier bill, Comprehensive Benefits personnel reconcile carrier invoices with data stored in the Workforce Now Application on a monthly basis to verify that the amounts are valid and accurate. If variances are identified, discrepancy reports are generated as a result of the reconciliation and are either updated on the carrier websites or sent to the carriers to update their system.	Control 3.04
4.05	For clients that have contracted with ADP and their carriers to have their bills processed according to Workforce Now Application records, Comprehensive Benefits personnel reconcile the carrier invoices or census reports with the data stored in the Benefits application at least annually to verify that the amounts are valid and accurate (if applicable, i.e., if the carrier maintains employee enrollment data). If variances are identified, discrepancy reports are generated as a result of the reconciliation and are sent to the carriers to update their system upon request.	Control 3.04
4.06	ACH transactions for the client carrier payments are approved by an authorized client contact and the VP of Finance or the Sr. Director of Finance prior to processing. Approvers cannot verify transactions that they have input into the Chase Access Next Gen application.	Control 3.05
4.07	Only authorized associates have access to the Chase Access Next Gen application used to transfer funds to and from client accounts. User IDs, passwords, and a token are required to access the Chase Access Next Gen application.	Control 3.06

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
Control Objective 5: Benefits - Client Maintenance and Open Enrollment		
5.01	An Open Enrollment Questionnaire and/or Planning Recap email is used to track the Open Enrollment dates of each client during the OE period.	Control 4.01
5.02	Open Enrollment is set up in the Workforce Now Application as requested by the client and completion of the following items: • Rate Sheet (if applicable) • Benefits Plan Setup Form (if applicable)	Control 4.02
5.03	A Benefit Audit Report (BAR) or Benefit Plan Summary is produced by ADP and provided for review by ADP management and the client to validate open enrollment information was accurately and completely input into the Workforce Now Application.	Control 4.03
5.04	When the open enrollment period begins participants can make their elections and employee records in the Workforce Now Application are updated in real-time. QA runs reports to verify that participant elections were entered and there are no errors. If there are errors, clients work with the Benefits Support Specialists until they are resolved.	Control 4.04

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
5.05	*FSA Plan Only* Clients electing FSA-only plans are set up in the Workforce Now Application as requested by the client. The setup is performed by Workforce Now Solution specialists based on the following documentation: • Summary of plan renewal information communicated to the client for review • Confirmation email from the client with approval to proceed and update (if applicable) • Confirmation email of changes made in the Workforce Now Application communicated to the client (if applicable)	Control 4.05
Control Objective 6: Time and Attendance - Essential Time - Data Input		
6.01	Clients authenticate to the Workforce Now Application using approved input mechanisms (i.e., clocks, web Application, hand punch, IVR) and credentials (i.e., badge, client database ID, user ID, and password, hand scan).	Control 11.01
6.02	The Workforce Now Application is configured with three roles (i.e., Employee, Supervisor, and Client Administrator/Practitioner) that can be assigned to client employees depending on their access requirements.	Control 11.04
6.03	During the import of client data using the Import Interface, the Workforce Now Application records errors in a log that is available for review by client users with the Administrator/Practitioner role.	Control 1.01
6.04	The Workforce Now Application is configured with data validation controls (i.e., time entry format checks, mandatory fields, drop-down boxes, and pre-populated fields) that display error messages on the client's screen.	Control 1.02

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
Control Objective 7: Time and Attendance - Essential Time - Processing		
7.01	The Workforce Now Application is configured to process payroll based on client defined work and pay rules (i.e., rounding, shift guarantees, exception flags).	Control 2.03
7.02	During the processing of payroll, the Workforce Now Application is configured to notify the user regarding payroll related exceptions (e.g., messages, warnings, and errors) and prevent the processing of payroll for errors.	Control 2.04
7.03	The Workforce Now Application restricts clients from moving to the next pay period without completing specific payroll, time, and event management steps.	Control 2.05
Control Objective 8: Time and Attendance - Essential Time - Data Output		
8.01	Client users with Manager, Participant, and Time & Attendance Supervisor profiles have access to generate reports. The applications display error and warning messages related to the status of the reports generated.	Control 7.03
8.02	During the export of pay data, the Workforce Now Application displays and records in a log error and warning messages related to the status of the export file. *Note: Refer to Control 12.03 for data encryption and Control Objective 22 for problem management.*	Control 7.02
Control Objective 9: Time and Attendance - Enhanced Time - Data Input		
9.01	The Enhanced Time Application contains edit checks to identify errors resulting from invalid and/or incomplete data that is imported manually and automatically through XML. Any errors identified are reported in a log file that is made available for clients.	Control 1.04

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
9.02	The Enhanced Time Application contains the following edit checks that validate accuracy/completeness of data entered manually. • Data entry validation controls, such as time entry format checks • Mandatory fields • Drop-down boxes • Pre-populated fields that cannot be modified through data entry If the edits do not pass, error messages appear on the users' screen, preventing further processing.	Control 1.05
9.03	Once data entered passes the required edits, employee and time data is automatically updated in the Enhanced Time Application.	Control 1.06
Control Objective 10: Time and Attendance - Enhanced Time - Processing		
10.01	The Enhanced Time Application allows clients the functionality to configure work and pay rules such as shift guarantees, rounding rules, and exception flags.	Control 2.06
10.02	The Enhanced Time Application automatically calculates work and pay rules such as shift guarantees, rounding rules, and exception flags based on the configured inputs by clients.	Control 2.07
Control Objective 11: Time and Attendance - Enhanced Time - Data Output		
11.01	The Enhanced Time Application provides the ability for clients to restrict access to generate reports and export files based on roles and permissions in the application.	Control 7.04
11.02	Status messages are automatically generated on screen and subsequently recorded in an application log file to notify the client when a report or export file is generated successfully or unsuccessfully with errors.	Control 7.05

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
Control Objective 12: Payroll - Data Input		
12.01	Client users require a valid user ID and password for authentication to the Workforce Now Portal input system, Pay eXpert input system, iReports output system, and the Workforce Now Application.	Control 11.02
12.02	The Workforce Now Portal input system, Pay eXpert input system and the Workforce Now Application restrict erroneous data input and incomplete data from being entered through pre-formatted data entry screens.	Control 1.02
12.03	Secure Socket Layer (SSL) technology with encryption is used to securely transmit payroll data entered from the Workforce Now Portal input system, Pay eXpert input system and the Workforce Now Application into the Payroll Application.	Control 7.01
12.04	Data file transmissions between the Workforce Now Portal input system, Pay eXpert input system and the Workforce Now Application and the Payroll Application are monitored and identified issues, if any, are documented, reported, and followed up to resolution.	Control 1.07
12.05	Payroll data (e.g., employee records, salary, deductions, marital status, and tax jurisdiction) entered into the Workforce Now Portal input system, Pay eXpert input system and the Workforce Now Application is transmitted to the Payroll application successfully and automatically updates the Employee Master Database (EMP) within the Payroll Application.	Control 1.08
12.06	The Payroll Application EDIT processing performs a series of edit checks on payroll data files received from the Input Systems by comparing the data files within the Employee Master Database (EMP) to verify that the information is accurate. Errors that appear on EDIT screens are investigated and resolved by the Production Support (Editing) group prior to the payroll being released for further processing.	Control 1.09

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
Control Objective 13: Payroll - Deductions and Tax Withholdings Specifications		
13.01	The Corporate Statutory Research Shared Services group monitors statutory changes impacting payroll-related taxes for both U.S. and Canadian taxing authorities.	Control 5.01
13.02	Upon identification of a statutory change impacting payroll-related taxes, the Statutory Research Shared Services creates and distributes an email/document detailing the change. The Stat Project Manager activates a Statutory feature in the Rally software where the Business Analysts on the Payroll Statutory Kanban team will review and analyze the impact (e.g., STAT file, quarter, client, and region) and approve.	Control 5.02
13.03	Statutory changes requiring coding modifications are coded by the appropriate development team and tested and certified for production release by the appropriate testing group. *Upon completion of testing, changes are deployed to production following the change management process outlined in Control Objective 17.*	Control 5.03
13.04	Statutory changes that do not require coding modifications are applied to the STAT File database by authorized STAT members.	Control 5.04
13.05	Client Support Specialists (CSSs) process client requests to add, modify, or delete client–specified deductions in the Payroll Application upon receiving approval from an authorized client contact.	Control 5.05
Control Objective 14: Payroll - Processing		
14.01	Payroll processing procedures for the ADP payroll Regions have been documented and provide overall guidance to ADP personnel and are available through the ADP Intranet.	Control 6.01

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
14.02	Automated payroll processing jobs are executed to process client payroll based on information entered, statutory regulations, and client defined requirements.	Control 6.02
14.03	M&MTAM personnel monitor the status of the scheduled jobs and are alerted of any identified processing issues or exceptions. Issues/exceptions are documented, reported, and followed up on to resolution.	Control 6.03
14.04	At the end of each production day, the Prelist/Editing group reviews the status of jobs processed and notifies Operations and/or Client Services to confirm job completion status and any identified issues requiring further investigation and resolution.	Control 6.04
14.05	Automated reconciliations are performed daily and weekly to compare the Payroll Ledger to the EMP totals for each client. The Quality Control group reviews the reconciliation report and investigates any differences to resolution.	Control 6.05
Control Objective 15: Payroll – Output		
15.01	Client output reports (e.g., payroll register, payroll journal) and data files (e.g., MAS GLI, other payroll-related output, money movement, and direct deposit) are automatically generated from the Payroll Application upon completion of each payroll run.	Control 7.06
15.02	Client output reports (e.g., payroll register, payroll journal) and other payroll-related data files are automatically transmitted and made available to Workforce Now clients through iReports output reports, Pay eXpert data files or Workforce Now Application data files.	Control 7.07

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
15.03	Data files (e.g., NAS ADP GL, MAS GLI, other payroll-related output, money movement, and direct deposit) and output report files are made available to clients and other ADP systems utilizing Secure Socket Layer (SSL) technology encryption to secure the transmission of payroll data.	Control 7.01
15.04	The Corporate Systems Engineering group monitors the results of data file (e.g., iReports, MAS GLI file, and general ledger) and output report file transmissions and is alerted of any identified issues or exceptions. Issues are documented, reported, and followed up on to resolution.	Control 7.08
15.05	For client output reports printed by ADP, the Regional Payroll Production Operations group monitors the transmissions of the output print files from the Payroll Application to the ADP printers and is alerted of any identified issues or exceptions and that exceptions are followed up on to resolution.	Control 7.09
Control Objective 16: Payroll – Output (Money Movement/Direct Deposit Files)		
16.01	Money movement/direct deposit files are automatically generated from the Payroll Application upon completion of each client payroll processing run.	Control 8.01
16.02	Direct deposit files are automatically sent to the ADP ETS system for retrieval or transmitted directly to the client bank in accordance with client specifications.	Control 8.02
16.03	The Banking group confirms by telephone, VRU or fax, depending on arrangements made with the bank that the bank’s total number of payments and the total monetary amount received agree to totals within the Payroll Application.	Control 8.03
16.04	Clients electing Full Service Direct Deposit (FSDD) of payrolls complete an authorization form (e.g., the “Client Account Agreement”) that is signed by both the client ADP’s Risk and Compliance Group.	Control 8.04

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
16.05	Client money movement files (e.g., FSDD and ADPCheck) are automatically transmitted to ADP's CAPS system upon completion of each payroll run.	Control 8.05
16.06	Banking personnel review the transmission status and compare the information available on the Payroll Application to the information available on the CAPS system. Identified differences are followed–up in order to resolve them promptly.	Control 8.06
Control Objective 17: Application Development and Change Management		
17.01	A formal and documented application development and change management policy has been developed to guide the in-scope applications' development groups.	Control 9.01
17.02	Change requests to the in-scope applications are formally documented and authorized by appropriate ADP management.	Control 9.02
17.03	Changes to in-scope application are tested (unit, regression, functional testing and peer-reviewed) in a segregated test environment and the results are approved by ADP management prior to deployment.	Control 9.03
17.04	Changes to the in-scope applications are approved for migration to the production environment by ADP Management prior to deployment.	Control 9.04
17.05	Access to deploy application version upgrades and service packs to the production environment is restricted to properly authorized personnel based on job function.	Control 9.05
17.06	*Payroll Application Only* Source code is controlled and monitored using version control systems in the development environment. Only a limited number of authorized personnel have access to source code system in the development environment.	Control 9.06

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
17.08	*MOTIF Account Request Tool* Changes to the MOTIF Account Request Tool follow a formal change management process that includes authorization, testing, and approval prior to deployment into the production environment.	Control 9.07
17.09	*MOTIF Account Request Tool – Authorized Access* The ability to develop changes and promote changes to production is appropriately restricted to authorized personnel. *Note: While users have the ability to develop and promote changes, control 17.10 is designed to require an independent second-level review before a change can be promoted, enforcing segregation of duties.*	Control 9.08
17.10	*MOTIF Account Request Tool –Review* Program changes to the MOTIF Account Request tool require an independent second-level review prior to promotion to production.	Control 9.09
17.11	*MOTIF Account Request Tool – Notification* An automated email notification is sent to the MOTIF Development Operations team when a change is promoted to production.	Control 9.10
17.12	*MOTIF Account Request Tool – Code Compare* A script runs daily in the Task Scheduler to compare the MOTIF Production Release File fingerprint to the Development File fingerprint. A daily automated email is generated and sent to the MOTIF team with the results of this script.	Control 9.11
Control Objective 18: Operating Systems (OS) and Database Change Management (Payroll Application Only)		
18.01	ADP has established a formal Change Management Process that outlines the requirements for making operating system (OS) and database changes. The process is documented and maintained by ADP management.	Control 10.01

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
18.02	Operating system and database changes to the Payroll Application production environment are authorized, tested, and approved by the Change Approval Board (CAB) prior to deployment.	Control 10.02
18.03	Access to deploy operating system and/or database changes to the Payroll Application production environment is restricted to appropriate personnel.	Control 10.03
Control Objective 19: Logical Security		
19.01	ADP associates accessing the in-scope applications are required to authenticate using a valid user ID and password that comply with the ADP's security policies and standards.	Control 11.01
19.02	Only appropriate ADP associates have access to the administrative functionality for the in-scope applications and key mainframe datasets (specific to the Payroll Application).	Control 11.03 Control 11.09
19.03	The Workforce Now Application, Workforce Now Portal input, and Pay eXpert input system provide the ability for clients to restrict user access based on roles and functions.	Control 11.04
19.04	User access additions and modifications to the in-scope applications require authorization from appropriate ADP management. Changes are documented and executed.	Control 11.05 Control 11.10
19.05	User access deletions to the in-scope applications require authorization from appropriate ADP management. Changes are documented and executed.	Control 11.06

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
19.06	Auditing has been enabled at the application level for the in-scope applications. Transactional data is logged with the user ID of the person who initiated the transaction and is available for review.	Control 11.07
19.07	Only authorized individuals have update access to the production database.	Control 11.08
19.08	The Corporate Mainframe Security group configures the audit policy within the Payroll Application so that an audit log of operator activity is generated. The audit logs are available for review and provide a record of device access, configuration changes, and user actions.	Control 11.11
19.09	On a bi-weekly basis, a mainframe job is executed by Mainframe Security personnel to identify terminated employees with an active RACF user ID, and revoke their access to the Payroll system.	Control 11.12
19.10	The Corporate Mainframe Security group has set up automated scripts that run periodically and automatically delete inactive RACF accounts and mark users with extended (administrative) privileges for additional investigation.	Control 11.13
19.11	ADP business partners, IT Engineering and Global Product & Technical Services review the list of business and IT users with RACF mainframe access on an annual basis. In addition, IT Management reviews the list of IT users (i.e., DBA, Storage Management, CICS, MVSSYS) on a quarterly basis. Additions and deletions are communicated to M&MTAM Technical Services for updates.	Control 11.14

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
19.12	*MOTIF Authentication* ADP associates with support job responsibilities accessing client environments are required to authenticate through a unique user ID, and a password that is compliant with the Information Security Standards, when requesting temporary access to the environment.	Control 11.15
19.13	*MOTIF User Access Management (Active Directory Network Groups)* User account additions, modifications, and deletions require authorization from appropriate ADP management. Changes are documented and executed by an individual separate from the requestor according to policy and as requested.	Control 11.16
19.14	*MOTIF (Active Directory Network Groups) Password Policies* Password rules/restrictions are enforced at the network-level according to policy.	Control 11.17
19.15	*MOTIF - User Access* ADP access to client environments is restricted to authorized personnel.	Control 11.18
19.16	*MOTIF – Temporary User Access* Temporary access to client environments is disabled nightly.	Control 11.19
19.17	*MOTIF Temporary Access Review* Requests for temporary access to client environments are logged and reviewed on a monthly basis. Users whose temporary access is not approved have their access revoked. For any temporary access requests that were rejected during the monthly review, or if a manager did not respond, TLM management conducts a review of the activity performed by the individual in the specific client for which the access request was made to determine whether any unauthorized activity occurred.	Control 11.20

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
19.18	*MOTIF Super User Account* Access to the Super User account within the MOTIF Account Request Tool is restricted to properly authorized personnel based on job function.	Control 11.21
19.19	*MOTIF Administrator Access* Administrator access to the MOTIF Account Request Tool is restricted to properly authorized personnel based on job function.	Control 11.22
19.20	*ADP Portal (SMS) Authentication* ADP associates and client administrators authenticate to the Enhanced Time application via SMS using a unique user ID and password.	Control 11.23
19.21	*ADP Portal (SMS) Password Parameters* Password parameters are automatically enforced for all users of the Enhanced Time application via the users' SMS accounts. Password parameters are configured in accordance to ADP security policies and standards.	Control 11.24
19.22	*ADP Portal (SMS) User Access Approvals* For ADP associates, user accounts can only be created in SMS upon receipt of an authorized request submitted through an online SMS request form. User accounts must be assigned an SMS Enhanced Time role, which provides access to the application	Control 11.25
19.23	*ADP Portal (SMS) Access Revocation* Accounts for terminated ADP associates are removed from SMS upon termination.	Control 11.26
19.24	*ADP Portal (SMS) User Access Appropriateness* ADP access to Enhanced Time client environments via the ADP Portal is restricted to appropriate personnel.	Control 11.27

September 30, 2019 Report Control Reference #	September 30, 2019 Description of Control Activity	March 31, 2020 Report Control Reference #
Control Objective 20: Physical Security (Payroll Application Only)		
20.01	Access to the Print Rooms is controlled by a multi–level badge access system and is monitored by surveillance cameras.	The risk of unauthorized access to output print files within the Print Rooms is now addressed by Control 7.11.
20.02	Physical access changes to the Print Rooms (i.e., additions, modifications, and deletions) require authorization from appropriate ADP management, and are executed and documented.	
20.03	On a periodic basis (e.g., monthly or quarterly), management reviews the list of users who have physical access to the Print Rooms and confirms that the access is appropriate for the users' current job responsibilities.	
20.04	Access to the badge-access control system used to grant and revoke badges is restricted to authorized personnel.	
Control Objective 21: System Backups (Payroll Application Only)		
21.01	Backup jobs are executed according to the backup schedule and take place automatically through the Control M tool scheduling system.	Covered within the ADP GETS US SOC 1 Report
21.02	The M&MTAM Command Center group monitors the results of the backup procedures and is alerted by the application through an automatically generated ticket of any identified backup issues or exceptions. Issues, if any, are documented, reported, and followed up on to resolution.	Covered within the ADP GETS US SOC 1 Report
Control Objective 22: Problem Management		
22.01	A problem management case is automatically generated for third party data error files received for a client. The errors are reviewed and resolution notes are documented by the Benefits Representative.	Control 12.01
22.02	Employee Service Center (ESC) associates use formal and documented client requirements to guide them in performing services for each client.	Control 12.02

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
22.03	Members of the Benefits support groups are responsible for properly documenting incidents (system issues and client inquiries) in the problem management system, determining the priority of the issue, and resolving the issue.	Control 12.03
22.04	Open Service Requests (cases) are reviewed by the Client Service Managers periodically and case notes are updated to provide a status of the open issue.	Control 12.06
22.05	If a client issue cannot be resolved by the Client Services group, the issue is escalated to Client Product Support (CPS) for additional support. If the CPS group cannot resolve the issue, it is escalated to QA.	Control 12.07
22.06	Members of the Solution Center are responsible for documenting and tracking all application/support issues communicated by the client.	Control 12.09
22.07	Issues not resolved within the tiered groups of the Solution Center, are escalated to IT Operations and a ticket is opened to track the status of the issue through to resolution.	Control 12.10
22.08	The Team Leads and Solution Center managers monitor the progress of urgent cases to verify that cases are worked timely.	Control 12.11
22.09	Open Service Requests (cases) are reviewed by the Solution Center Managers periodically and case notes are updated to provide a status of the open issue.	Control 12.12
22.10	The TLM Service Center group documents phone and email interactions, including exceptions, problems, and errors, with clients in the Siebel problem management systems.	Control 12.04

September 30, 2019 Report Control Reference #	*September 30, 2019 Description of Control Activity*	*March 31, 2020 Report Control Reference #*
22.11	Siebel cases are given a priority level and assigned to a member of the TLM Service Center group, based on prior client interaction, necessary skill set, and nature of the issue at hand for resolution.	Control 12.05
22.12	Open case and aging reports from the Tableau system are available to TLM Service Center Management for review and tracking of client cases.	Control 12.06
22.13	Issues that cannot be resolved by the TLM Service Center group are escalated to the Technical Support Services group for resolution by creating a ticket in the Serena Business Manager system. The Technical Service group tracks the escalated issue in the ticket and notifies the requester when the issue is resolved.	Control 12.08
22.14	Issues that cannot be resolved by the TLM Service Center or Technical Support Services group are escalated to the GETS US organization for resolution by creating a ticket in the Service Desk Problem Management system. The GETS US organization tracks the escalated issues in the ticket and notifies the requester when the issue is resolved.	Control 12.08