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

Description of ADP's AutoPay Payroll Services System for the period October 1, 2019 to September 30, 2020

ADP, the ADP logo, and ADP Always Designing for People are registered trademarks of ADP, Inc.
Copyright © 2020 ADP, Inc. adp.com
SOC 1® is a registered trademark of the American Institute of Certified Public Accountants (AICPA).

Always Designing for People™

Table of Contents

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties.
ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

SECTION ONE

INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY ERNST & YOUNG

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Ernst & Young LLP
200 Clarendon Street
Boston, MA 02116

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

Building a better working world

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 AutoPay Payroll Services System for the period October 1, 2019 to September 30, 2020" (Description) of its AutoPay Payroll 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 AutoPay Payroll Services System. The Description includes only the Control Objectives and related controls of AutoPay Payroll 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 and its Global Security Organization 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.

A member firm of Ernst & Young Global Limited

Building a better working world

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 October 1, 2019 to September 30, 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

A member firm of Ernst & Young Global Limited

Building a better working world

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 October 1, 2019 to September 30, 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 October 1, 2019 to September 30, 2020 and if subservice organizations and user entities applied the complementary controls assumed in the design of ADP's controls throughout the period October 1, 2019 to September 30, 2020.
c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2019 to September 30, 2020, if complementary subservice organization and user entity controls assumed in the design of ADP's controls operated effectively throughout the period October 1, 2019 to September 30, 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 the use of management of ADP, user entities of ADP's System during some or all of the period October 1, 2019 to September 30, 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

December 11, 2020

A member firm of Ernst & Young Global Limited

SECTION TWO

MANAGEMENT ASSERTION

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Always Designing for People™

ADP MANAGEMENT ASSERTION

December 11, 2020

We have prepared the description of Automatic Data Processing, Inc.'s (ADP) AutoPay Payroll Services System entitled, "Description of ADP's AutoPay Payroll Services System for the period October 1 2019 to September 30, 2020" (Description) for processing user entities' transactions throughout the period October 1, 2019 to September 30, 2020 for user entities of the system during some or all of the period October 1, 2019 to September 30, 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 AutoPay Payroll 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 AutoPay Payroll Services System (System) made available to user entities of the System during some or all of the period October 1, 2019 to September 30, 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;

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties.
ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- 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 October 1, 2019 to September 30, 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 October 1, 2019 to September 30, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties.
ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

SECTION THREE

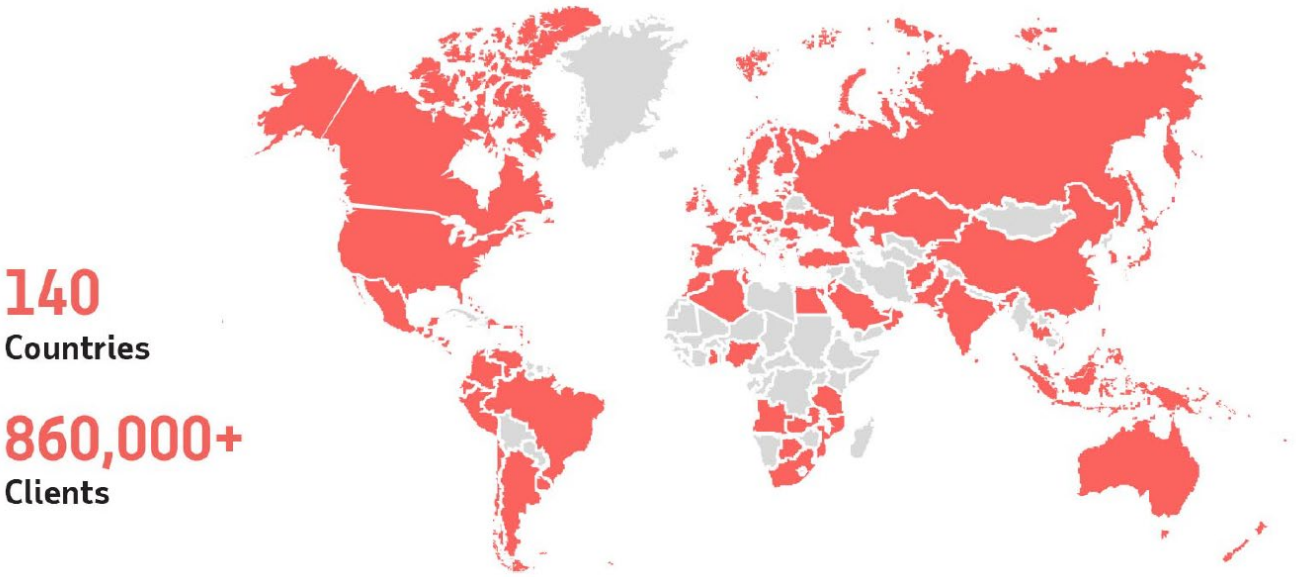
DESCRIPTION OF ADP'S AUTOPAY PAYROLL SERVICES SYSTEM FOR THE PERIOD OCTOBER 1, 2019 TO SEPTEMBER 30, 2020

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 860,000 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 are 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Digital technology is transforming today's workplace and workforce. ADP is accelerating its 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Always Designing for People™

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 690,000 small businesses; ADP Workforce Now®, serving over 75,000 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 60,000 clients with premier global solutions consisting of local in-country solutions and multinational offerings, including ADP GlobalView®, ADP Celergo® and ADP Streamline®.

With WorkMarket, a cloud-based workforce management solution, ADP helps enable clients to manage their extended workforce through freelancer management functionality and reporting insights.

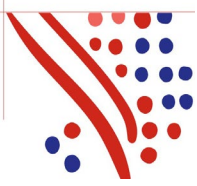
Wisely by ADP® is its latest advancement in the future of pay. ADP's payment offerings support an employer's need for flexible payment solutions to meet the individual needs of its workers. The Wisely Pay by ADP™ payroll card is a network-branded payroll card and digital account that helps enable employers 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.

Also, 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 28 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 445 apps and integrations, allowing them to choose solutions that are tailored to their needs, industry requirements, and preferences.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.



Always Designing for People™

HCM Solutions

Integrated HCM Solutions - 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 22 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. Also, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 85,000 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 touchscreens, 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. Also, 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. Also, ADP Retirement Services offers investment management services to retirement plans through ADP Strategic Plan

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 8,000 federal, state and local tax agencies. In its fiscal year ended June 30, 2020, in the United States, ADP processed and delivered approximately 69 million employee year-end tax statements and moved more than $2.2 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 offers 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 13,000 clients and approximately 530,000 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. Also, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- 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. Also, 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 experts help tailor recommendations to continue to drive their business forward.

ADP Comprehensive Services - 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.

ADP Comprehensive Outsourcing Services (ADP COS) - 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. Also, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 14 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 supplies 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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

CONTROL ENVIRONMENT

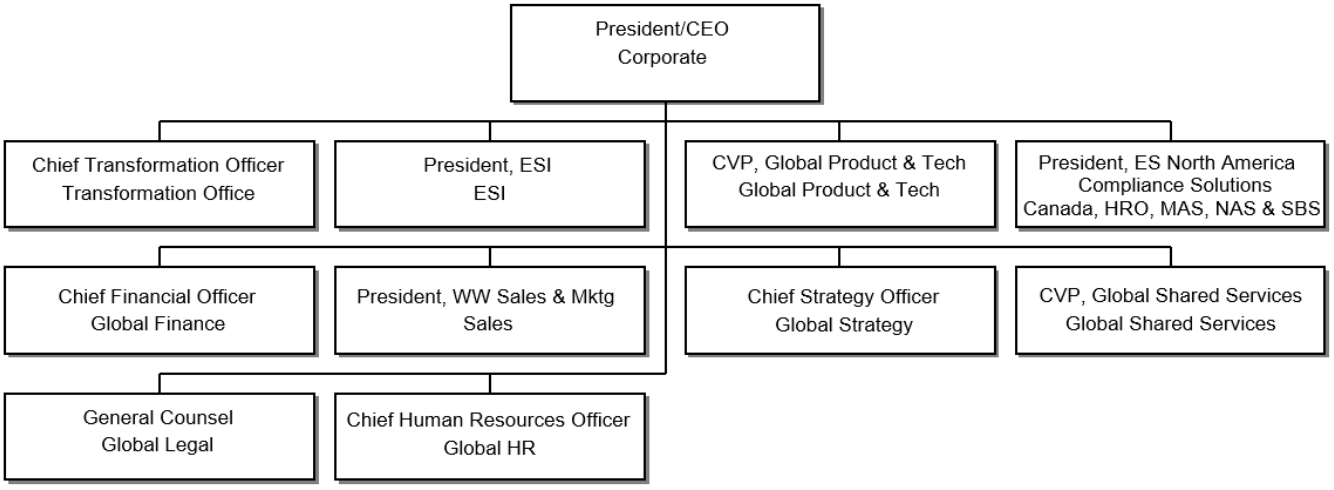
ADP's control environment reflects the position taken by the management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. Management takes seriously defects identified in internal 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



This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 are 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 before 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- 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. Also, associates are required to disclose any previously unreported circumstances or events known by the employee that appears to violate 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 Norfolk, VA, and 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 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 before 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Client Satisfaction Monitoring

Solution Center management communicates regularly with internal staff and clients to discuss issues and client satisfaction. Also, 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). Also, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Sodexo Monitoring

Effective November 1, 2019, ADP has contracted with Sodexo a facilities management services vendor, to provide specific functions (i.e., physical access and environmental safeguard monitoring) 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). Also, 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

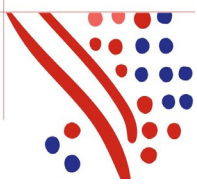
Employees

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. Also, all new employees receive a copy of a handbook that describes ADP policies. Newsletters that summarize significant events and changes to ADP 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 the system and regulatory changes that might affect the client organization. Also, each client organization has a service representative who communicates with the client organization regularly by phone, fax, letter, and email.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.



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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

OVERVIEW OF THE AUTOPAY PAYROLL SERVICE

Service Overview

ADP's AutoPay Payroll Services System is comprised of hosting and outsourced processing that includes:

- 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 throughout the U.S. and Canada 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 AutoPay Payroll Services System is comprised of the applications depicted below, along with the supporting operating systems and database platforms:

Application Name	Operating System Technology	Database Technology	Description
AutoPay Application	Mainframe	IBM DB2	Hosted payroll processing application that stores client employee master data, as well as processes and calculates client payroll. The AutoPay Application also 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,

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Application Name	Operating System Technology	Database Technology	Description
			Employee Master Database (EMP), Management Reporting System (MR 2000), and Statutory (STAT) File database.
Hosted-PCPW	Windows	Oracle	Hosted Input System that allows clients to enter and update payroll information from a single computer, multiple computers, operating on a LAN, or using a web browser with Citrix in the ADP hosted environment. Hosted-PCPW allows clients to setup direct deposit accounts, ADPCheck, wage garnishment, standard deductions, automatic pay for employees with standard hours (eliminating repetitive data entry), automated tax collections for manually written checks, and allocation of hours or earnings to a department or job number.
PayForce	zLinux	Oracle	Hosted Input System that offers the ability to enter and transmit payroll information to the AutoPay Application as well as providing basic HR recordkeeping functionality.
Hosted-Enterprise HR AutoLink	zLinux Solaris	Oracle	Hosted Input Systems for ADP National Account clients that provide screens for clients to enter payroll data and transmit payroll information to the AutoPay Application.
Self Service Portal	VMWARE	N/A	Hosted front-end/web-based Input System that provides single sign-on access to other Input Systems, such as PayForce, Hosted-Enterprise HR AutoLink, and iReports. The Self Service Portal serves as an interface that can be used by clients to view and modify individual data.
iReports	Windows AIX	Oracle	Hosted web-based Output System that provides clients the ability to view PDF copies of their payroll output reports that are produced by the AutoPay Application.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Key Organizational Support Structure

The organizational structure supporting ADP's AutoPay Payroll Services System 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.

ES Group Staff – 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

ES Divisional Staff – The ES Divisional Staff supports the Service Centers. The Divisional staff is responsible for:

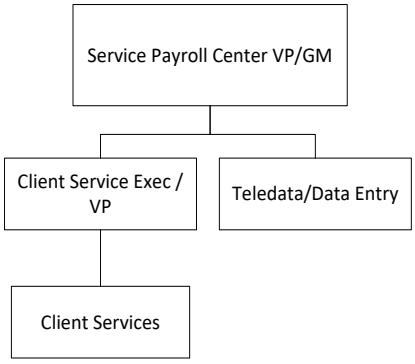
- Coordinating the activities for the Service Centers
- Promoting product and operating efficiency
- Providing technical, sales, financial, and human resources development support to the Service Centers

ES Regional Staff – 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 the 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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.



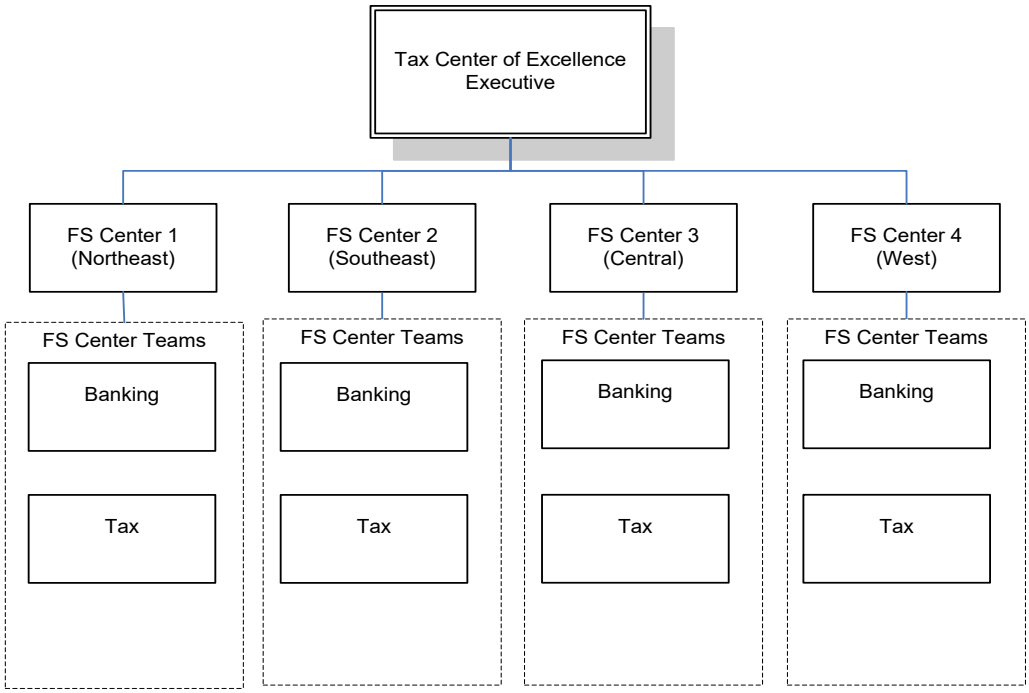
The Service Centers functional groups include:

- *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 AutoPay Application, Client Support Specialists (CSSs) also referred to as Solution Center Consultants, are assigned to the client, allowing clients to contact CSSs directly with AutoPay 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 the processing of worksheet payroll data.

Tax Center of Excellence Service Centers – For each of the Service Centers, the AutoPay 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.

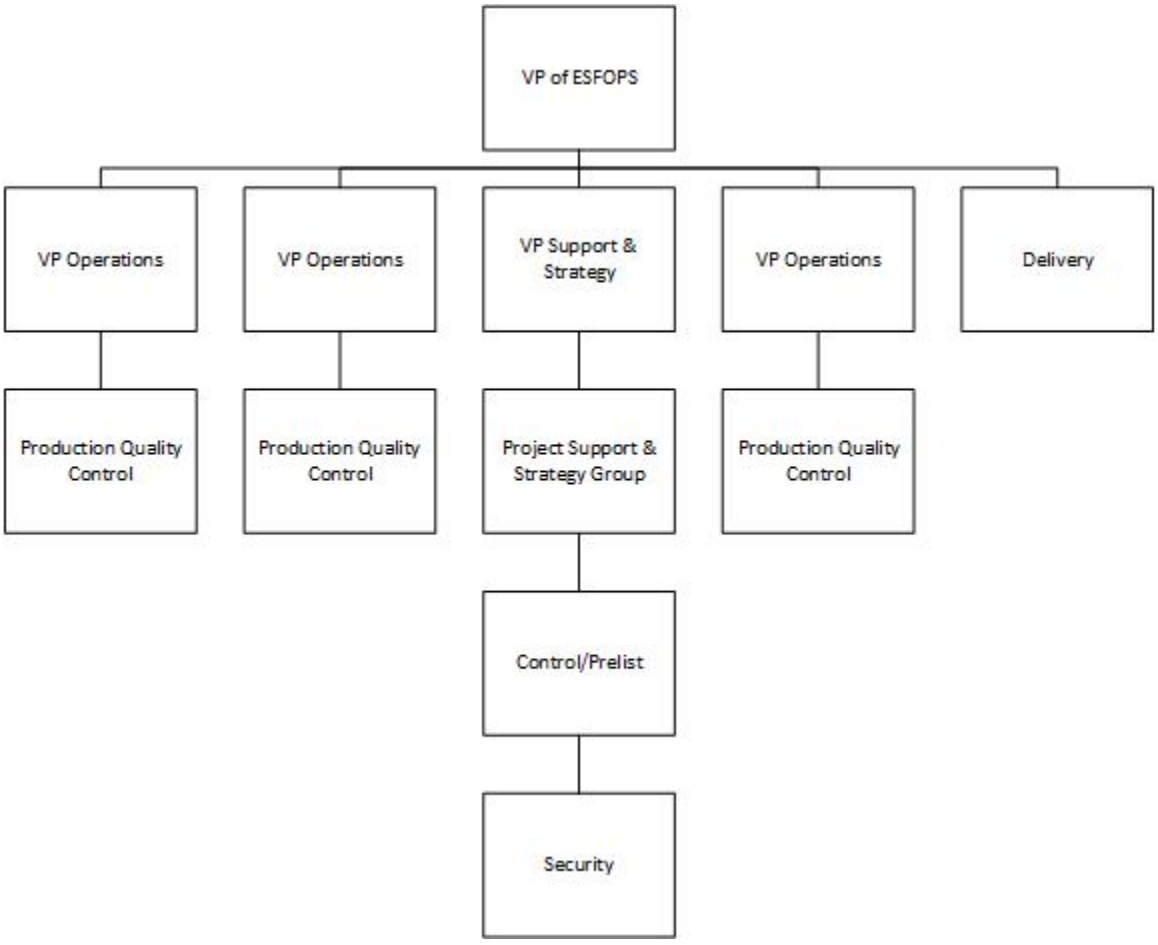
This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.



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 the Associate Technology Management (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 the set-up 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.



Other AutoPay Payroll Supporting Groups

AutoPay Development – AutoPay Development is responsible for the development, maintenance, and quality assurance testing of the AutoPay Application.

Integrated Acceptance Test – Integrated Acceptance Test (iAT) is responsible for testing AutoPay 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 AutoPay Application changes to the production environment.

Payroll Support – Payroll support is responsible for migrating AutoPay Application changes to the AutoPay Application production environment.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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) (formerly known as AutoPay Data Processing Operations (ADPO)).

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

Statutory Research Shared Services – Statutory Research Shared Services is responsible for making inquiries about and obtaining information concerning statutory 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 AutoPay Application's input and output systems.

Access & Identity Management (AIM) – AIM is responsible for developing the Security Management Services (SMS) product hosted at ADP's 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 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 MAS FS New Output System (NOS) balancing and error review/notification between the AutoPay 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 AutoPay Application hosted at ADP's GETS US data center facilities in Georgia. ADP has consolidated certain AutoPay Payroll Services operations into M&MTAM. The M&MTAM organization consists of two groups:

- M&MTAM – AutoPay 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 AutoPay Application console operations. The Command Center staff is responsible for job execution, job monitoring, system monitoring, and workload balancing.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- M&MTAM – Technical Services: This group's primary responsibilities include supporting the AutoPay 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 HR Anytime application was decommissioned and ceased supporting payroll clients as an input system into AutoPay, effective as of October 15, 2019, and as a result, the relevant controls and description have been removed from the scope of this report.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 AutoPay Payroll Services that comprise the hosting and outsourcing of payroll transaction processing applicable to ADP's AutoPay Application and the supporting Input/Output Systems described in the prior section (collectively referred to as the "AutoPay Payroll 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 AutoPay Payroll Services System. New client implementations and any unique client situations are outside the scope of this Description.

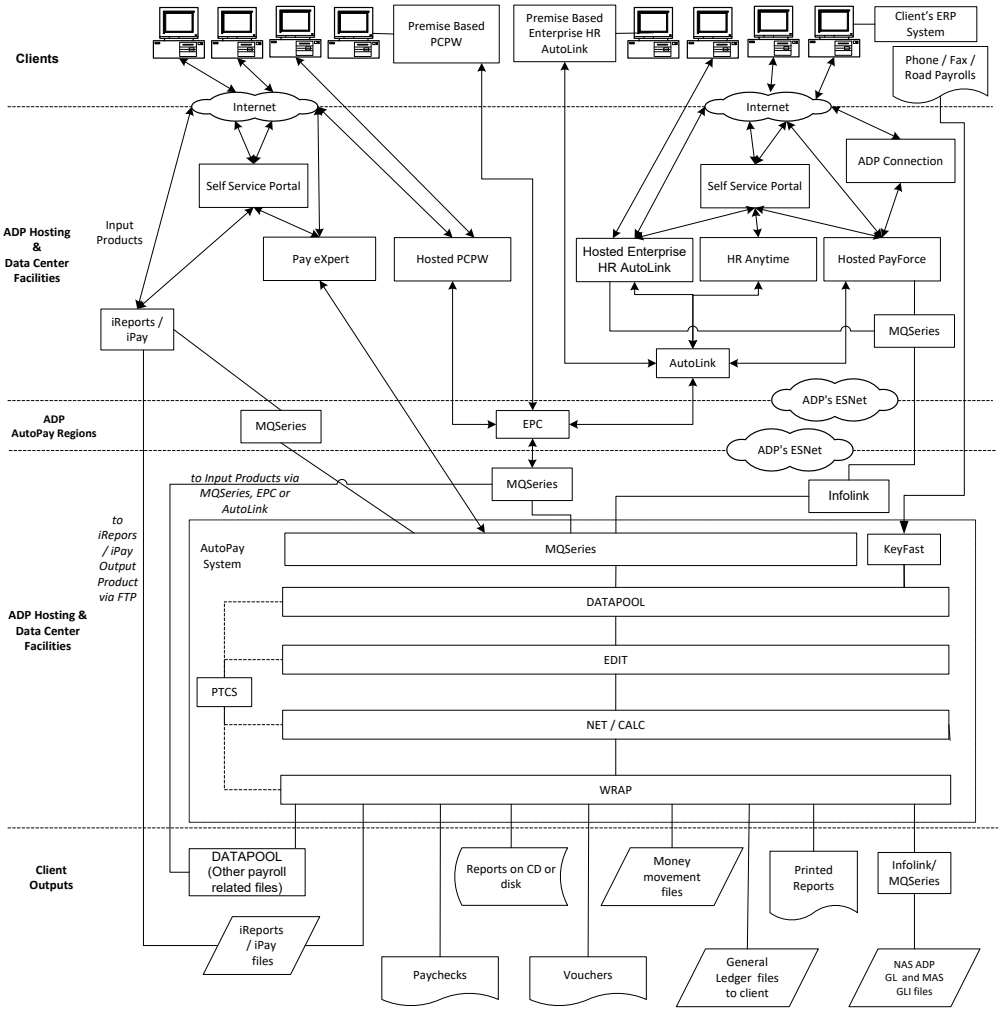
The AutoPay Payroll Services System interfaces with other ADP systems (e.g., NAS ADP GL, MAS GLI) and/or services (e.g., as Payroll Tax Filing, Print Services, WGPS, and Retirement Services). These are optional systems and/or services that clients can contract with ADP. Also, clients may contract with ADP for additional support services via ADP Comprehensive Outsourcing Services (COS). This service allows clients to transfer administrative responsibility for a range of selected processes to ADP. These are optional services that clients can contract with ADP (or use other service providers). This report is not intended to encompass the control aspects of other ADP services or platforms that may interface with the AutoPay Payroll Services Application.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

TRANSACTION PROCESSING

Overview of Key Transaction Processing/Services

AutoPay Payroll Services transaction processing encompasses three major components: Payroll Input, Payroll Processing, and Payroll Output. Payroll 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 into ADP provided Input Systems or communicated directly to ADP for input by phone or fax. 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:



This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Payroll Input

Datapool

Datapool, a component of the AutoPay 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 AutoPay Application until polled by the PTCS. Once polled, the data is submitted to the next processing phase of the AutoPay Application.

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

- Automated Input (primary method) – Clients can use one of several ADP-supplied Input Systems, such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, PayForce, PayForce, or Self Service Portal. Input Systems can be hosted by ADP or installed at a client site (i.e., premised-based systems). Premised-based systems are optional and not in the scope of this Description.
- 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 AutoPay Application for processing.

Automated Input

Clients use the Input Systems to enter and transmit their payroll transactions which are then automatically transmitted to ADP's AutoPay 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 Systems, the transactions are transmitted to AutoPay 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 Systems also promote 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 before being transmitted to the AutoPay Application for processing.

Each of the Input Systems allows 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 AutoPay Application for processing. The data can be recalled by the client from the Input Systems and edited at any time in the Input Systems before transmission. The communication systems receive the data throughout the day and periodically transfers it into Datapool where it is held until processed.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Always Designing for People™

Manual Input

AutoPay 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 AutoPay 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.

Statutory (STAT) File Maintenance

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

The AutoPay Application tax-withholding rate modules are maintained in the STAT database. The STAT File database feeds the AutoPay 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 statutory 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Upon identification of a statutory change, the Statutory Research Shared Services Group creates a tracking item that 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" tracking item, 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 AutoPay Application impacts (e.g., STAT File, quarter, client, region), and creating "Narratives" to be used for further research and development of the proposed change, is also the responsibility of the business analyst.

Each narrative has a developer, tester, and documentation specialist assigned. Elaboration sessions are held to review the narrative's 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 narrative. The status is tracked using tracking software.

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. A point-in-time tracking report lists open tracking items, 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 tracking item and narrative. 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.

Updates requiring coding modifications are coded and tested by either the Payroll Statutory Kanban team or designated AutoPay Scrum teams. Both teams certify and "accept" changes signifying they are ready for release to the AutoPay Application production environment. The process and controls for releasing changes follow the 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 log in using their mainframe user ID and password. The process and controls for STAT File database access follow the Logical Security process described in the *General Computer Controls* section of this Description.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Payroll Processing

Processing is divided into two phases: EDIT and NET/CALC. ADP uses the AutoPay 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 inquiries to track the status of the individual payrolls that are being processed by the AutoPay Application. PTCS also provides online control totals and daily production statistics that are used to track and monitor AutoPay Application processing activities.

EDIT Processing

EDIT is an AutoPay 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 AutoPay 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 AutoPay'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 AutoPay 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 GET US Organization SOC 1 Report.

Output

WRAP Processing

Upon completion of the NET/CALC process, the WRAP process is kicked off to produce multiple outputs. The primary AutoPay 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).

Pay Statements

AutoPay 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- *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 with 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. Also, 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 include:

- 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 Processing Support Organization.

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 have 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 AutoPay 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.

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 AutoPay Application through WRAP batch processing
Payroll Register	Reports current payroll-cycle data by employees including hours, earnings, statutory and voluntary deductions. Shows totals by department and company levels.	Automated from the AutoPay 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 AutoPay 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 AutoPay 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 AutoPay 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 AutoPay Application through WRAP batch processing

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Report/File Name(s)	Description	Source and Preparation
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 AutoPay 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.

Data Files

Upon successful completion of a payroll run, the AutoPay Application automatically produces a series of payroll data files that are either used by other ADP systems or transmitted back to the input systems 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 AutoPay to the Input Systems 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.

Money Movement/Direct Deposit Files

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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- 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 uses AutoPay'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, email 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 AutoPay 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 AutoPay 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 AutoPay 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 the scope of this report and are covered in ADP's TotalPay Service System and TotalPay Service and PayCard System SOC 1 reports.

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 work with Regional LAN Services to monitor input data transmissions from the Input Systems to the AutoPay Application and data transmissions between ADP entities.
- The Micro Tech Support (MTS) group monitors the status of file transmissions between the Input Systems and the AutoPay Application based on MQSeries status notifications.
- The Corporate Systems Engineering Group monitors the status of the transmissions of the iReports files from the AutoPay 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 AutoPay 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 AutoPay 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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
- System Backups

Information Security

Information security encompasses the controls that prevent and detect unauthorized access to information resources including physical access to facilities and 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 only authorized users.

All Information Security policies are on ADP's Intranet and they provide overall guidance for data security administration, the 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

ADP's GSO is responsible for developing corporate-wide security standards. The individual business unit's IT departments or security groups are responsible for complying with corporate standards and administering logical security for internal ADP personnel on selected systems and applications. Formal policies and procedures are followed to establish appropriate access to information assets.

Network Access

To access the AutoPay Application, ADP users must first authenticate to ADP's ESNet network. The GETS US Organization is responsible for the overall security and architecture of ADP's trusted network infrastructure (ESNet and LANs) as well as user administration. These controls are covered in ADP's GETS US Organization SOC 1 Report.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

AutoPay Application – Mainframe Access

Once authenticated at the network-level, logical access to the AutoPay Application is controlled through IBM's Customer Information Control System (CICS) using the 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 AutoPay 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.

AutoPay 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 AutoPay Application production environment security administration:

- Authorized members of the Infrastructure & Operations Mainframe Security and ATM groups have system administrator privileges for the AutoPay 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 AutoPay 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 AutoPay 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

The Mainframe Security Group executes a mainframe job on a weekly basis to identify terminated employees with an active RACF user ID and revoke access to the AutoPay 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.

An audit trail of AutoPay 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 M&MTAM Technical Services group is responsible for performing an annual review of access to the AutoPay 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 the 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. Also, database access for application support purposes is also granted to authorized personnel, the use of application database accounts is managed by the individual application support teams for the AutoPay environment.

Input/Output Systems Database Layer – Security Administration

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.

Password restrictions are enforced at the OS level through local server settings, LDAP, or through Windows AD policies. Password restrictions are configured in compliance with corporate standards that include periodic forced password changes, password complexity, and password history.

Input/Output Systems Application Layer – Security Administration

ADP associates are granted update access to the Input/Output Systems, except for Hosted-PCPW, for troubleshooting purposes through SMS which permits ADP support personnel to log into a client environment using a valid username and password. The client is responsible for administering access to Input/Output Systems for its employees.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

A valid user ID and password are required to authenticate to the Input/Output System. Password controls (except for Hosted-PCPW) include expiration after a specific number of days, required minimum length, and password history tracking. Due to technical specifications, the Hosted-PCPW Input System only requires that the password be a minimum length.

Application Development and Change Management

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

Application Development and Change Management

The AutoPay Development Group is responsible for maintaining and developing changes supporting the AutoPay 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.

Change Request Management

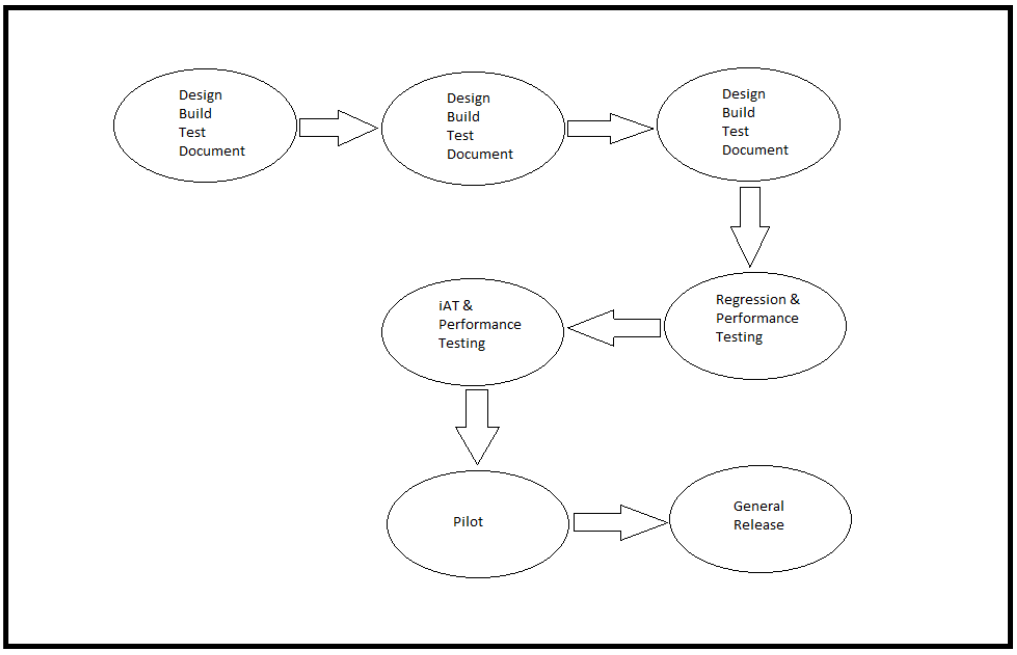
Requests for program changes go through formalized reviews and approvals which are documented in tickets. Management of Release Management and AutoPay Development collaborate to review and authorize program change requests.

Software Development, Testing, and Implementation Procedures

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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

AutoPay 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 AutoPay 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 tracking 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.

AutoPay 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 AutoPay Application operations process a higher number of client transactions and statutory changes, thus minimizing the implementation of non-critical systems 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

AutoPay 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.

Agile Roles

Product Owner

- The 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
- The 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Always Designing for People™

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 the 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.

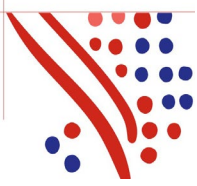
Sprint Review Meeting

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.



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. AutoPay development uses Benchmarking information for capacity planning purposes.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

iAT Phase

iAT testing replicates the testing that was originally performed by Autopay 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 AutoPay 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 Autopay 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 Autopay 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 Autopay 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 the 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 before 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 AutoPay Application LPARs to support the 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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 AutoPay 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 Autopay 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 Autopay Delivery, Service and Support, or the Payroll Support group, can make Patch and STAT File releases available to the AutoPay 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.

Input/Output Systems Development and Change Management

Changes to the Input/Output Systems, 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 Input/Output Systems.

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 to a project manager and a development team to make any required coding changes.

Segregated development and test environments from the production environment exist for each of the Input/Output Systems. Upon completion of development, testing of changes commences and is performed by the Autopay development testers and 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, testers and iAT members will email the respective project manager, product owner, and/or business unit management for the Input/Output 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 & Hosting Product Support.

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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

AutoPay 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.

Policy and Methodology

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 before being deployed to the production environment. OS Release Changes require testing in the iAT environment and two pilots before general release. Product Version/Release Changes or New Product Installations require iAT testing and a minimum of one pilot before 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 AutoPay 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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.

System Backups

The GETS US organization is responsible for the computer operations and backup and recovery controls for the AutoPay Payroll System except for data mirroring which is covered in this report. The controls covered by GETS are included in ADP's GETS US Organization SOC 1 Report.

ADP uses peer-to-peer technology to automatically copy and create a mirror data image of required data sets from the production application located at the GETS US hosting and data center facility in Georgia to a backup environment at a geographically distant GETS US hosting and data center facility in South Dakota. The mirrored data sets are created to bring the application online at the backup hosting and data center facility if needed. Thus, in the event of a disaster, the application will continue processing from the last valid system state.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

SUBSERVICE ORGANIZATIONS

ADP GETS US Organization

Overview of Subservice Provider Relationship

The AutoPay Payroll 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 AutoPay Payroll application that are covered in the scope of this report (AutoPay Payroll SOC 1 Report) and those that are covered in the scope of ADP's GETS US Organization SOC 1 Report:

Control Process Name	ADP's GETS US Organization SOC 1 Report	AutoPay Payroll Services System SOC 1 Report
Application Development and Change Management		✓
Operating System (OS) Software, Hardware, and Infrastructure Change Management		
a. Mainframe OS – AutoPay Application		✓
b. Other OS – Input/Output Systems	✓	
c. Hardware and Infrastructure Change Management	✓	
Network Monitoring and Incident Management	✓	
Logical Security		
a. Input/Output Systems, AutoPay Application, and Mainframe OS		✓
b. Network Administration	✓	
c. Other OS – Input/Output Systems	✓	
d. OS and Database Administration*	✓	✓
Physical Security	✓	
Environmental Safeguards	✓	

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Process Name	ADP's GETS US Organization SOC 1 Report	AutoPay Payroll Services System SOC 1 Report
System Backups		
a. Data Backups	✓	
b. Data Mirroring		✓
Payroll Input		✓
Payroll Processing		✓
Payroll Output		✓

* ADP's GETS US organization is responsible for supporting the OS and Database Administration at the infrastructure level. Also, database access support for the AutoPay Payroll application 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.
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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Process Area	Sub-Service Organization Controls
System 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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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: Payroll Data Input

Client management is responsible for:

- Notifying ADP of changes in the authorized contacts list
- Validating the accuracy of initial data entry when using the Input Systems
- 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 AutoPay Application after initial account set-up, to confirm that employee-level and company-level information was initially recorded completely and accurately

Control Objective #2: 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 the intended payroll transactions were accurately reflected before providing payroll processing approval
- Reviewing the employee changes and any errors presented during payroll preview to determine if any corrections are needed

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

- Reviewing the Master Control report distributed after payroll processing to determine if any corrections are needed

Control Objective #3: Payroll Processing

Client management is responsible for:

- Validating 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 #4: Payroll Output

Client management is responsible for:

- Notifying ADP of changes required to their payroll output
- Printing and secure check distribution, if done in-house by the 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 #5: Payroll Output – 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 client elects Regular Direct Deposit)
- Confirming accuracy and completeness of direct deposit funds disbursement information provided to ADP

Control Objective #8: Logical Security

Client management is responsible for:

- Determining that only authorized client personnel are granted logical access to ADP Input/Output Systems
- Granting and revoking access to the Input/Output Systems
- Periodically reviewing assigned employee access to the Input/Output Systems for appropriateness
- Reviewing the Audit Trail log, within the respective Input/Output System (highlighting any updates made to payroll data), to identify any unauthorized activity and notifying ADP of any discrepancies

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

SECTION FOUR

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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

TRANSACTION PROCESSING CONTROL OBJECTIVES AND CONTROLS

Payroll Data Input

Control Objective 1: Controls provide reasonable assurance that payroll data is received from authorized sources and initially recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.01	Client users require a valid user ID and password for authentication to the ADP supplied Input/Output Systems (such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, PayForce, Self Service Portal, and iReports).	Inspected the log in screen for each of the Input/Output Systems (such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, PayForce, Self Service Portal, and iReports) to determine whether a valid user ID and password were required for authentication to the systems. Observed an ADP associate attempt to authenticate to a sample Input/Output System to determine whether a valid user ID and password were required to access the system.	No deviations noted No deviations noted
1.02	The ADP Input Systems (such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, PayForce, and Self Service Portal) restrict erroneous data input and incomplete data from being entered through pre-formatted data entry screens.	Observed an ADP associate attempt to submit incorrect/incomplete data (SSN, zip code, employee name, pay frequency) into each of the ADP Input Systems (such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, PayForce, and Self Service Portal) and inspected the related error messages generated to determine whether pre-defined data validation rules were in place to detect and identify erroneous data input and incomplete data.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 1: Controls provide reasonable assurance that payroll data is received from authorized sources and initially recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.03	Teledata operators require a valid user ID and password to access the Key-Fast Input System to enter client-provided data. Also, Teledata operators authenticate the client contacts before inputting the client-provided payroll information into Key-Fast.	For a sample of days and clients, observed Teledata operators enter client payroll data into Key-Fast to determine whether they: • Authenticated to the Key-Fast system using a valid user ID and password; • Authenticated the client contact that provided the payroll data according to documented client specifications before input.	No deviations noted
1.04	Key-Fast restricts erroneous and incomplete data from being entered through pre-formatted data entry screens.	Observed a Teledata operator enter erroneous and incomplete data (invalid modifier, missing state tax code, invalid SSN, invalid file number) into the Key-Fast data entry screens on a sample day to determine whether the data was rejected and an error message was presented, and only valid and complete data was accepted.	No deviations noted
1.05	Before submitting the phone or fax payroll data entered for processing by the AutoPay Application, Teledata operators compare control totals provided to data entered into the Key-Fast system. Out-of-balance conditions are corrected with the client.	For a sample of days and clients, inspected system records and payroll information provided by the client to determine whether the Teledata operator compared the control totals provided by the client to the control totals entered into the Key-Fast system and out-of-balance conditions were corrected with the client.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 1: Controls provide reasonable assurance that payroll data is received from authorized sources and initially recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.06	Secure Socket Layer (SSL) technology with encryption is used to securely transmit payroll data entered from the Input Systems (such as PayForce, Hosted-Enterprise HR AutoLink, and Self Service Portal) into the AutoPay Application.	Observed an ADP associate log into the application site for a sample Input System on a sample day to determine whether the sites use SSL technology with encryption. For a sample file from each of the Input Systems: • Inquired of a Principle Quality Assurance Engineer to determine whether SSL technology with encryption was used to securely transmit payroll data entered from the Input Systems into the AutoPay Application; • Inspected a data string within the file to determine whether data was not presented in clear text.	No deviations noted No deviations noted

Control Objective 1: Controls provide reasonable assurance that payroll data is received from authorized sources and initially recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.07	Data file transmissions between the Input Systems and the AutoPay Application are monitored and identified issues, if any, are documented, reported, and followed up to resolution.	Observed an ADP employee monitoring data file transmission alerts on a sample day to determine whether automated monitoring tools were used to monitor for issues or exceptions with data file transmissions between the Input Systems and the AutoPay Application. For a sample of identified file transmission issues between the Input Systems and the AutoPay 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 payroll data is received from authorized sources and initially 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, tax jurisdiction) entered into the Input Systems (such as Hosted-PCPW, Hosted-Enterprise HR AutoLink, and PayForce) is transmitted to the AutoPay Application successfully (or entered successfully into Key-Fast) and automatically updates the Employee Master Database (EMP) within the AutoPay 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 AutoPay Application to determine whether the data was successfully transmitted and automatically updated in the Employee Master Database. Inspected relevant documentation from the Input Systems (Hosted-PCPW, Hosted-Enterprise HR AutoLink, and PayForce) and the AutoPay 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 1: Controls provide reasonable assurance that payroll data is received from authorized sources and initially recorded completely and accurately.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.09	The AutoPay 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 before the payroll being released for further processing.	Observed members of the Production Support (Editing) group perform EDIT processing real-time in the AutoPay Application on a sample day to determine whether errors identified appeared on EDIT screens. Observed a member of the Production Support (Editing) group on a sample day reviewing and investigating the errors that appeared on Edit screens for a sample day to determine whether the errors were resolved before the payrolls being released for further processing.	No deviations noted No deviations noted

Deductions and Tax Withholdings Specifications

Control Objective 2: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the AutoPay Application in accordance with statutory and/or client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.01	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 WIP item's history page 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
2.02	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 change management 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 WIP item's history page 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 2: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the AutoPay Application in accordance with statutory and/or client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.03	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 6.*	For a sample of statutory changes that required coding modifications, inspected the documented testing results to determine whether the change was tested and certified for production release by the appropriate testing group.	No deviations noted
2.04	Statutory changes that do not require coding modifications are applied to the STAT File database by appropriate 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 2: Controls provide reasonable assurance that payroll deductions and tax withholdings are maintained in the AutoPay Application in accordance with statutory and/or client specifications.

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

Payroll Processing

Control Objective 3: 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*
3.01	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
3.02	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 AutoPay 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 a sample Input System for a sample of employees and inspected the agreed pay rate amount to the AutoPay payroll register generated upon completion of the selected payroll run.	No deviations noted
		Inspected the relevant tax withholding settings and deduction screen maintained in a sample Input System for a sample of employees and:	No deviations noted

Control Objective 3: 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*
		• agreed the amounts for any deductions to the AutoPay 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 AutoPay payroll register generated upon completion of the selected payroll run. *Hourly Employee* Inspected the pay rate from the employee profile maintained in a sample 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 AutoPay payroll register generated upon completion of the selected payroll run. Inspected the relevant tax withholding settings and deduction screen maintained in the sample Input System for the sample employee above and • Agreed the amounts for any deductions to the AutoPay 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 AutoPay payroll register	No deviations noted No deviations noted

Control Objective 3: 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.	
3.03	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.	Observed a member of the Prelist/Editing team confirm the status of jobs processed within AutoPay on a sample day and clear "inventory" for a sample Regional LPAR to determine whether job completion status was reviewed and any identified issues were investigated and resolved. 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 No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 3: 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*
3.04	Automated reconciliations are performed daily and weekly to compare the Payroll Ledger to the EMP totals for each client. The Processing Support Organization reviews the reconciliation report and investigates any differences to resolution.	Inspected the out-of-balance report job schedule in the AutoPay Application to determine whether the reconciliation to compare the Payroll Ledger to the EMP totals for each client was scheduled to run automatically daily and weekly.	No deviations noted
		Observed a member of the Processing Support Organization 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Payroll Output

Control Objective 4: Controls provide reasonable assurance that AutoPay Payroll Services System outputs are produced completely, accurately, and distributed in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.01	Client output reports and data files (e.g., NAS ADP GL, MAS GLI, other payroll-related output, money movement, and direct deposit) are automatically generated from the AutoPay Application upon completion of each payroll run.	For a sample test client in the AutoPay 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 AutoPay 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 AutoPay Application to determine whether the amounts were completely and accurately produced: • NAS ADP GL data file • MAS GLI data file • Other payroll related files • Money movement file • Direct deposit file	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 4: Controls provide reasonable assurance that AutoPay Payroll Services System outputs are produced completely, accurately, and distributed in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.02	Client output reports (e.g., payroll register) and other payroll-related data files are automatically transmitted and made available to AutoPay clients through iReports output reports and Input Systems (data files).	For a sample test client in the AutoPay 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 AutoPay 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 AutoPay Application production environment, executed a sample payroll run and inspected the payroll-related data files to determine whether the data files were automatically transmitted to the in-scope Input Systems.	No deviations noted

Control Objective 4: Controls provide reasonable assurance that AutoPay Payroll Services System outputs are produced completely, accurately, and distributed in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.03	Data files (e.g., NAS ADP GL, MAS GLI, other payroll-related output, money movement, direct deposit) and output report files are made available to clients and other ADP systems using Secure Socket Layer (SSL) technology encryption to secure the transmission of payroll data.	Inspected a sample data file and output report file made available to clients and 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
4.04	The Corporate Systems Engineering group monitors the results of data files (e.g., iReports, NAS ADP GL, and MAS GLI file) and output report file transmissions and is alerted of any identified issues or exceptions. Issues are documented, reported, and followed to resolution.	Observed a member of the Corporate Systems Engineering group monitoring data file transmission alerts within the monitoring tools to determine the results of data file and output report files transmissions between the Input Systems and the AutoPay Application were monitored. 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 No deviations noted

Control Objective 4: Controls provide reasonable assurance that AutoPay Payroll Services System outputs are produced completely, accurately, and distributed in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.05	For client output reports printed by ADP, the Regional Payroll Production Operations group monitors the transmissions of the output print files from the AutoPay Application to the ADP printers and is alerted of any identified issues or exceptions and those exceptions are followed up to resolution.	For a sample Region LPAR, utilized video conferencing technology assisted by ADP personnel to observe 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
4.06	Production Support and Quality Control personnel review printed client-output reports and electronic media for defects.	For a sample Region LPAR, utilized video conferencing technology assisted by ADP personnel to observe 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 4: Controls provide reasonable assurance that AutoPay Payroll Services System outputs are produced completely, accurately, and distributed in accordance with client specifications.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.07	Print Operations Quality Control personnel are restricted from having access to modify the output print files within the Autopay Application.	Inspected the access rights screen within the AutoPay Application for the Operations Quality Control personnel to determine whether the Quality Control personnel were restricted from having access within the AutoPay Application to modify the output print files. 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 AutoPay Mainframe was restricted to appropriate personnel based upon job responsibilities.	No deviations noted No deviations noted

Payroll Output – Money Movement/Direct Deposit Files

Control Objective 5: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the AutoPay 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
5.01	Money movement/direct deposit files are automatically generated from the AutoPay 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 AutoPay Application upon completion of the payroll cycle. For a sample client and payroll run, inspected the money movement in the AutoPay Application and direct deposit file to determine whether the payroll information (net pay amounts) agreed to the corresponding records contained in the AutoPay Application.	No deviations noted No deviations noted
5.02	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 transmitted to the ADP ETS system or client bank in accordance with client specifications.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 5: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the AutoPay 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
5.03	The Banking Group confirms by telephone, VRU, email 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 AutoPay Application.	For a sample client and payroll run, observed an ADP Banking associate confirm bank totals with the client via email on a sample day to determine whether the bank's total number of payments and the total monetary amount received agreed to the totals within the AutoPay 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 AutoPay Application.	No deviations noted No deviations noted
5.04	Clients electing Full Service Direct Deposit (FSDD) of payrolls complete an authorization form (e.g., the "Client Account Agreement") that is signed by the client.	For a sample of clients that elected FSDD, inspected the "Client Account Agreement" form and the AutoPay Application to determine whether the form was completed and signed (authorized) by the client, and the FSDD was set up per the client request.	No deviations noted
5.05	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 transmitted to ADP's CAPS system upon completion of the payroll run.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 5: Controls provide reasonable assurance that transmissions of money movement files/direct deposit files from the AutoPay 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
5.06	Banking personnel review the transmission status and compare the information available on the AutoPay Application to the information available on the CAPS system. Identified differences are followed-up 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 AutoPay 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

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

GENERAL COMPUTER CONTROL OBJECTIVES AND CONTROLS

Application Development and Program Change Management

Control Objective 6: 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*
AutoPay Application (Mainframe)			
6.01	A formal and documented application development and change management policy has been developed for mainframe application development projects to guide the AutoPay Development group.	Inspected the application development and change management policy documentation to determine whether development requirements were documented for mainframe application development projects to guide the AutoPay Development group.	No deviations noted
6.02	AutoPay Application change requests are formally documented and authorized by appropriate ADP management personnel.	For a sample of months, inspected the Release Coordination Schedule for the major releases to the AutoPay Application to determine whether the change request was documented and authorized by appropriate ADP management. For a sample of minor changes made to the AutoPay Application, inspected the monitoring ticket to determine whether the change request was documented and authorized by appropriate ADP management.	No deviations noted No deviations noted

Control Objective 6: 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*
6.03	Changes to the AutoPay Application are tested (unit, regression, and functional testing) in a segregated test environment and the results are approved by ADP management before deployment.	For a sample of months, inspected test documentation for the major releases to the AutoPay Application to determine whether testing was executed, and the test results were documented and approved by ADP management before deployment.	No deviations noted
		For a sample of minor changes made to the AutoPay Application, inspected test documentation to determine whether testing was executed, and test results were documented and approved by ADP management before deployment.	No deviations noted
		Inspected the relevant AutoPay application system configurations to determine whether separate development, test and production environments were established.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 6: 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*
6.04	Source code is controlled using the ChangeMan version control system and the ability to migrate code to the AutoPay Application production environment is restricted to authorized personnel and excludes those responsible for development functions.	Inspected the system-generated listing of users with the ability to migrate code to the AutoPay 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 access to migrate code to the production environment was appropriate based on the individual's job responsibility and excluded those responsible for development functions.	No deviations noted
6.05	The Release Management group monitors the installation process of changes made to the AutoPay Application production environment and problems are documented for investigation and resolution.	For a sample of months, inspected Post-Release change tickets for the major releases to the AutoPay Application and inquired of the Director of Application Development to determine whether the Release Management group monitored the change installation process to the production environment and any problems identified were documented for investigation and resolution.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 6: 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*
Input/Output Systems			
6.06	Change requests to the Input/Output Systems are documented and authorized by appropriate product owners or business unit management personnel.	For a sample of changes made to the Input/Output Systems, inspected change documentation (emails, meeting minutes) to determine whether the change was authorized by appropriate ADP management personnel.	No deviations noted
6.07	Changes to the Input/Output Systems are tested in a non-production environment by the Autopay development testers and iAT groups and approved by ADP management before deployment.	For a sample of changes made to the Input/Output Systems, inspected change documentation (emails) to determine whether testing was performed by the Autopay development testers and iAT groups in a non-production environment and results are approved by ADP management before deployment to production.	No deviations noted
6.08	Changes to the Input/Output Systems are approved for migration to the production environment by the project manager before deployment.	For a sample of changes made to the Input/Output Systems, inspected the change order to determine whether the change was approved by the project manager before deployment to production.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 6: 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*
6.09	Access to deploy changes to the Input/Output System production environment is restricted to properly authorized personnel based on job function.	Inspected the user access listings from each of the Input/Output Systems, inspected job titles, and inquired of the IT Compliance Manager to determine whether the assigned access to deploy changes to the production environment was restricted to appropriate personnel based upon job responsibilities.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Operating Systems (OS) and Database Change Management

Control Objective 7: Controls provide reasonable assurance that the implementation of and changes to operating system software and data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
AutoPay Application			
7.01	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 AutoPay Application operating system and database were documented.	No deviations noted
7.02	Operating system and database changes to the AutoPay production environment are authorized, tested, and approved by management prior to deployment.	For a sample of operating system and database changes to the AutoPay Application production environment, inspected change orders and testing documentation to determine whether the related change was authorized, tested, and approved by management prior to deployment.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 7: Controls provide reasonable assurance that the implementation of and changes to operating system software and data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
7.03	Access to deploy operating system and/or database changes to the AutoPay 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 AutoPay Application production environment, inspected job titles and inquired of the Senior Director – Technical Services to determine whether access was appropriate based on job responsibilities. For a sample of operating system and database changes to the AutoPay 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 No deviations noted

Logical Security

Control Objective 8: 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*
8.01	ADP associates accessing the Input/Output Systems and AutoPay Application are required to authenticate using a valid user ID and password compliant with ADP's security policies and standards.	Inspected the relevant password configuration settings governing access to each of the Input/Output Systems, the AutoPay Application and the documented Information Security Standards to determine whether password settings (history, length, expiration, complexity) comply with ADP's security policies and standards. Observed an ADP associate attempt to authenticate to a sample Input/Output System (such as, Hosted-PCPW, Enterprise HR AutoLink, PayForce, Self Service Portal, and iReports) and the AutoPay Application to determine whether a valid user ID and password was required to access the systems.	No deviations noted No deviations noted
8.02	Only appropriate IT personnel have access to the administrative functionality for the Input/Output Systems and AutoPay Application and key mainframe datasets (specific to the AutoPay Application).	Inspected the system-generated listings of users with access to the key mainframe datasets in the AutoPay Application and inquired of Corporate Mainframe Security management regarding job responsibilities to determine whether access was restricted to authorized personnel. For a sample of users with administrative level privileges to the Input/Output Systems, inspected job titles and inquired of ADP management regarding the job	*AutoPay Application* No deviations noted *Input/Output Systems* Deviation noted

Control Objective 8: 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*
		responsibilities to determine whether access was restricted to authorized personnel.	For three (3) of a total population of forty-three (43) users with administrative access to the Input/Output Systems through SMS, access to the Self Service Portal, PayForce, and Hosted-Enterprise HR AutoLink input systems 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.*

Control Objective 8: 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*
8.03	User access additions and modifications to the Input/Output Systems 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 Input/Output Systems was documented and authorized by appropriate ADP management. • Inspected system-generated user access listings from the Input/Output Systems to determine whether access was granted as requested.	No deviations noted
8.04	User access additions and modifications to the AutoPay 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 AutoPay Application was documented and authorized by appropriate ADP management. • Inspected system-generated user access listings from the AutoPay Application to determine whether access was granted as requested.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 8: 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*
8.05	User access deletions to the Input/Output Systems 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 Input/Output Systems. For a sample of user terminations, inspected system-generated user access listings from the Input/Output Systems to determine whether access was revoked as requested.	No deviations noted No deviations noted

Control Objective 8: 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*
8.06	On a 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 AutoPay system.	Inspected the configuration of the relevant mainframe terminations job within the AutoPay 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 AutoPay Application.	No deviations noted
		For a sample week, inspected a sample terminated employee identified on the mainframe termination job script output and in the AutoPay Application to determine whether access was revoked following execution of the mainframe termination job.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 8: 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*
8.07	The Corporate Mainframe Security group configures the audit policy within the AutoPay Application so that an audit log of operator activity is generated. The a. its 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 AutoPay Application logged the device access, configuration changes, and user actions. For a sample of Region LPARs, inspected the relevant audit log settings to determine whether the AutoPay Application was configured to generate the audit log of the operator's activities.	No deviations noted No deviations noted
8.08	The Corporate Mainframe Security group has set up automated scripts that run periodically and automatically delete inactive RACF accounts and flag users with extended (administrative) privileges for additional investigation.	Inspected the configuration of the relevant automated script within the AutoPay 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. 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 No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 8: 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*
		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
8.09	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. Also, 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 as requested.	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	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Control Objective 8: 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*
		review access on the AutoPay Application was complete and accurate.	
8.10	Auditing has been enabled at the application level for the in-scope Input/Output Systems. 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 in-scope Input/Output Systems to determine whether auditing was enabled, and transactional data was being logged and made available for review. Observed a Technical Services Manager log into a sample Input/Output System 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 Input/Output System 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
8.11	Input/Output Systems provide the ability for clients to restrict user access based on roles and functions.	Inspected the relevant security screens for the in-scope Input/Output Systems to determine whether the applications provide the ability for clients to manage user access based on roles and functions.	No deviations noted

Control Objective 8: 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*
8.12	Only authorized individuals have update access to the Input/Output Systems production databases.	For a sample of production databases supporting the in-scope Input/Output Systems, inspected the system-generated listing of users with update access and inquired of ADP Management to determine whether access was limited to authorized individuals based on job responsibilities.	No deviations noted
8.13	A valid LDAP user ID and password is required for authentication to the Input/Output Systems production databases.	Observed an ADP associate log into a sample Oracle database for each Input/Output system to determine whether a valid LDAP user ID and password was required for successful authentication.	No deviations noted
8.14	Password rules/restrictions for authentication to the Input/Output Systems production databases are enforced at the server level through LDAP and is configured according to ADP's security policies and standards.	Inspected the relevant password configuration settings governing access to the DB production environments and ADP's password policies to determine whether password rules/restrictions including forced periodic password changes, password complexity, and password history were configured according to ADP's security policies and standards.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

Management Response to Testing Deviations:

Control 8.02 – Input/Output Systems

Management agrees that access for the three (3) associates with administrative access to the Self Service Portal, PayForce, and Hosted-Enterprise HR AutoLink input systems through SMS was confirmed as no longer required based on their job function and responsibilities. Management confirmed that the access for the associates has been suspended, and validated that the users did not log into the Self Service Portal, PayForce, and Hosted-Enterprise HR AutoLink input systems after the date their managers deemed the access inappropriate. Management identified control 8.10 as a compensating control in that it serves to mitigate any potential risk with logging of changes to payroll data which allows clients to identify unauthorized activity and notify ADP of any discrepancies.

Additional Procedures Performed by Ernst & Young:

Control 8.02 – Input/Output Systems

For the three (3) out of a total population of forty-three (43) users granted administrative access to the Self Service Portal, PayForce, and Hosted-Enterprise HR AutoLink input systems through SMS that was not appropriate, EY inspected access logs for each of the users and inquired with each user's manager to determine that the users did not log into the Self Service Portal, PayForce, and Hosted-Enterprise HR AutoLink input systems after access was no longer appropriate. Additionally, EY inspected evidence to validate that the users' accounts were suspended as of November 2, 2020, following identification.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

System Backups

Control Objective 9: Controls provide reasonable assurance that data and applications are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
9.01	Data in one primary database is mirrored to a secondary database in an alternate datacenter.	Inspected the configuration management for the production database to determine whether data in the production database was mirrored to a secondary database in an alternate data center.	No deviations noted

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

SECTION FIVE

OTHER INFORMATION PROVIDED BY ADP

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are trademarks of ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are ADP, Inc.

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.

This report is intended solely for use by the management of Automatic Data Processing, Inc., its clients, and the independent auditors of its clients, and is not intended and should not be used by anyone other than these specified parties. ADP, the ADP logo and Always Designing for People are ADP, Inc.