

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

Description of ADP's Global Enterprise Technology
& Solutions (GETS) North America Organization
Information Technology Services System for the
period October 1, 2022 to September 30, 2023



Always Designing
for People™

Table of Contents

SECTION ONE	PAGE
Independent Service Auditor's Report provided by Ernst & Young	
Independent Service Auditor's Report	4
SECTION TWO	
Management Assertion	
ADP Management Assertion	8
SECTION THREE	
Description of ADP's Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology Services System for the period October 1, 2022 to September 30, 2023	
Overview of Operations.....	11
Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Control Activities, and Information and Communication	20
Control Objectives and Controls	26
Overview of the Global Enterprise Technology & Solutions (GETS) North America Service.....	27
Scope of the Report	29
General Computer Controls	32
Complementary User Entity Controls	43
SECTION FOUR	
Description of Control Objectives, Controls, Tests, and Results of Tests	
Testing Performed and Results of Tests of Entity-Level Controls.....	45
Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity	45
General Computer Control Objectives and Controls.....	46
SECTION FIVE	
Other Information Provided by ADP	
ADP Global Business Resiliency Program.....	73

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.



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 Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology Services System" (Description) throughout the period October 1, 2022 to September 30, 2023 of its Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology system (System) for data center hosting services and technology infrastructure hardware and software managed services supporting the processing of 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 the 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.

Other Information Provided by Service Organization: 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 has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and accordingly we express no opinion on it.

ADP's responsibilities

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

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance

with attestation standards established by the American Institute of Certified Public Accountants (“AICPA”). 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, 2022 to September 30, 2023. 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.

We are required to be independent of ADP and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA’s Quality Control Standards.

Inherent limitations

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

Description of tests of controls

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

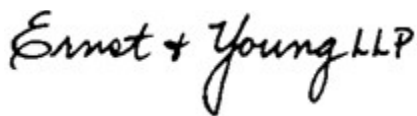
Opinion

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

- a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023.
- 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, 2022 to September 30, 2023 throughout the period October 1, 2022 to September 30, 2023.
- c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2022 to September 30, 2023, throughout the period October 1, 2022 to September 30, 2023.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of ADP, user entities of ADP's System during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material 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.



November 20, 2023

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.



ADP MANAGEMENT ASSERTION

November 20, 2023

We have prepared the description of Automatic Data Processing, Inc.'s (ADP) Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology system entitled, "Description of ADP's Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology Services System for the Period October 1, 2022 to September 30, 2023" (Description) for providing data center hosting services and technology infrastructure hardware and software managed services supporting the processing of user entities' transactions throughout the period October 1, 2022 to September 30, 2023 for user entities of the system during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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

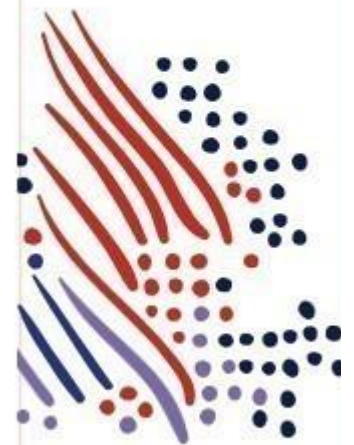
- a. The Description fairly presents the Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology system (System) made available to user entities of the System during some or all of the period October 1, 2022 to September 30, 2023 for providing data center hosting services and technology infrastructure hardware and software managed services supporting the processing of 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, including, if applicable:
 - The types of services provided.
 - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System.
 - The information used in the performance of the procedures, and supporting information; 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.

- 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.
 - Other aspects of our control environment, risk assessment process, information, and communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- (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 Global Enterprise Technology & Solutions (GETS) North America Organization Information Technology 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, 2022 to September 30, 2023 to achieve those control objectives. 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 effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.
- (3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Automatic Data Processing, Inc.

SECTION THREE

ADP'S DESCRIPTION OF ITS GLOBAL ENTERPRISE TECHNOLOGY & SOLUTIONS (GETS) NORTH AMERICA ORGANIZATION INFORMATION TECHNOLOGY SERVICES SYSTEM FOR THE PERIOD OCTOBER 1, 2022 TO SEPTEMBER 30, 2023



OVERVIEW OF OPERATIONS

General

In 1949, the founders established ADP to shape the world of work with a simple, innovative idea: help clients focus on their business by solving their payroll challenges. Today, ADP is one of the world's leading global technology companies providing comprehensive cloud-based human capital management (HCM) solutions that unite HR, payroll, talent, time, tax and benefits administration. ADP serves over 1 million clients and pays over 41 million workers in 140 countries and territories. ADP's common stock is listed on the NASDAQ Global Select Market® under the symbol "ADP."



Business Overview

ADP's Mission

ADP's mission is to power organizations with Human Capital Management (HCM) solutions that meet the changing needs of its clients and their workers. Data, digital technology, artificial intelligence, globalization, new business models and other significant events and disruptions continuously reshape the way people work. ADP's HCM technology, industry and compliance expertise and data insights deliver measurable results and peace-of-mind, and contribute to an engaged, 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 always designing better ways to work through products, services, and experiences that help enable people to reach their full potential.

ADP's Business Pillars

ADP's business is organized around three pillars which represent ADP's core growth areas:

- **U.S. HCM Solutions:** In the United States, ADP provides cloud-based HCM software with supporting service and expertise that assists employers of all types and sizes in managing the entire worker spectrum and employment cycle – from full-time to freelancer and from hire to retire.
- **U.S. HR Outsourcing (HRO) Solutions:** In the United States, ADP offers comprehensive HRO solutions in which it provides 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:** ADP offers international HCM and HRO solutions, comprised of both local, in-country solutions and cloud-based multi-country solutions, to clients wherever they do business around the world.

ADP's Strategy

With a large and growing addressable market, ADP is focused on its core growth areas and further enhancing its market position by executing its Strategy:

- **Lead with best-in-class HCM technology.** ADP designs and develops HCM platforms that simplify work and utilize enabling technologies like artificial intelligence and modern cloud architecture. ADP aims to solve the needs of clients and their workers today by making HCM transactions effortless and compliant, while anticipating their needs of tomorrow by incorporating valuable data insights and guidance into its solutions to help clients better understand their workforce and how they compare to industry peers, and position clients to make better decisions.
- **Provide expertise and outsourcing solutions.** ADP intends to continue to build on its deep expertise and make it readily available to clients through a variety of channels, ranging from traditional call and chat options to self-guided and AI-powered options. ADP will continue to leverage decades of experience, significant data insights, and investments in AI and other enabling technologies to help its clients and their workers navigate the ever-changing world of work.
- **Benefit its clients with its global scale.** ADP will continue to build on these strengths to further improve client experience, and to add to its global footprint to further meet clients where they choose to do business and address their needs for a distributed and flexible workforce.

Business Segments

ADP's two reportable business segments are Employer Services and Professional Employer Organization ("PEO"), and are based on the way that management reviews the performance of, and makes decisions about, ADP's business:

- 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 PEO) 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.

Products and Solutions

In order to serve the unique needs of its clients and their diverse types of businesses and workforce models, ADP provides a range of solutions which businesses of all types and 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 850,000 small businesses; ADP Workforce Now®, serving over 80,000 mid-sized and large businesses across ADP's strategic pillars; and ADP Vantage HCM® and ADP's next-gen HCM platform, serving large enterprise businesses. All 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 over 65,000 clients with premier global solutions consisting of in-country solutions and multinational offerings, including ADP GlobalView®, ADP Celergo®/Streamline® and ADP iHCM.

Innovation at ADP

For over 70 years, ADP has proven that actively listening and responding to what clients and their employees need and want keeps the world of work progressing forward. ADP is a pioneer in HCM automation, HCM in the cloud, mobile HCM and a digital HCM marketplace.

Leveraging the power of data, ADP innovates by anticipating the future of work, the future of HCM and the future of pay to help clients transform their businesses, simplify work and empower their workers.



ADP's data is the basis for the ADP National Employment Report, recently retooled by the ADP Research Institute (DPRI) and the Stanford Digital Economy Lab to provide a more robust, independent high-frequency view of the labor market and trajectory of economic growth in the United States.

ADP is leading its innovation efforts with ADP® DataCloud, its machine learning (ML) and workforce analytics platform. DataCloud analyzes aggregated, anonymized and timely HCM and compensation data from more than 1 million organizations across the U.S., powering solutions that provide clients with in-depth workforce and business insights that help enable critical HR decisions.

ADP's next-gen platforms are designed to provide clients with the flexibility they need to address today's and tomorrow's workplace challenges, and to personalize the experience based on their needs. ADP's next-gen payroll platform is a global solution that supports workers of all types and helps enable real-time, transparent, continuous payroll calculations. It unlocks flexible pay choices for clients so they can provide the best pay experience for their workers.

Additionally, ADP launched Roll™ by ADP, a mobile-first solution reimagining how small business do payroll. This payroll solution utilizes an AI-Powered chat interface to turn traditional payroll management into an intuitive conversation that can complete payroll in under a minute.

ADP's innovative Wisely® payment and financial wellness offering includes a suite of personalized banking-alternative solutions designed to give employees fast and flexible choices to access their pay and other sources of income. Wisely® Pay is a network-branded paycard with a digital account, through which employees can access their pay, make purchases online and in store, deposit checks, load additional funds onto the card, and transfer funds to a bank account in the United States. Wisely® Direct, a network-branded general purpose reloadable card that comes with a digital account, provides similar features and functionality but is offered directly to consumers.

Innovation is also about putting clients first by giving them and their workers a faster, smarter, and easier user experience (UX) designed with and for them. ADP is investing in UX alignment and simplification across its strategic products and solutions, with new UX releases for RUN Powered by ADP®, MyADP, ADP® Mobile Solutions and, most recently, ADP Workforce Now®.

ADP's Mobile app helps simplify how work gets done by helping enable clients to process their payroll anywhere, and giving millions of their employees worldwide access to their payroll and HR information in 32 languages.

HCM Solutions

Integrated HCM Solutions - ADP's premier suite of HCM products offers complete solutions that assist employers of all types and sizes in all stages of the employment cycle, from recruitment to retirement. ADP's suite of HCM solutions are powered by its strategic, cloud-based platforms, including:

- RUN Powered by ADP combines a software platform for 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 over 25 million (approximately 1 out of every 6) workers in the United States. ADP offers flexible payroll services to employers of all 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 provide powerful and agile solutions for employee benefits administration. These options include health and welfare administration services, leave administration services, insurance carrier enrollment services, employee communication services, and dependent verification services. In addition, ADP benefits administration solutions offer employers a simple and flexible cloud-based eligibility and enrollment system that provides their employees with tools, communications, and other resources they need to understand their benefits options and make informed choices.

Talent Management - ADP's Talent Management solutions simplify and improve the talent acquisition, management and activation process, from recruitment to ongoing employee engagement and development. Employers can also outsource their internal recruitment function to ADP. ADP's solutions provide performance, learning, succession and compensation management tools that help employers align goals to outcomes, and enable

managers to identify and mitigate potential retention risks. ADP's talent activation solutions include StandOut® powered by ADP, which provides 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 120,000 employers of all sizes, including time and attendance, absence management and scheduling tools. Time and attendance solutions include time capture via online timesheets, timeclocks with badge readers, biometrics and touch-screens, telephone/interactive voice response, and mobile smartphones and tablets. These tools automate the calculation and reporting of hours worked, helping employers prepare payroll, control costs and overtime, and manage compliance with wage and hour regulations. Absence management tools include accrued time off, attendance policy and leave case management 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 data analytics and reporting tools that provide clients with insights, benchmarks and performance metrics so they can better manage their workforce. In addition, industry-specific modules are available for labor forecasting, budgeting, activity and task management, grant and project tracking, and tips management.

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, collect employment taxes from clients and remit these taxes to more than 8,000 federal, state and local tax agencies.
- 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.

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

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

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

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, ADP's clients gain proven technology and processes and service and support. Whether a client chooses ADP's PEO or other HR Outsourcing solutions, ADP 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 is enabled by ADP Workforce Now and 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 all 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 a full HR department. With ADP's cloud-based HCM software at the core, ADP serves more than 16,000 clients and more than 725,000 worksite employees in all 50 U.S. states. ADP TotalSource is the largest PEO 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 a broad range of HR administrative services, including payroll and payroll tax, employer compliance, HR guidance, employee benefits and benefit administration, talent strategies, and workers' compensation insurance including risk and claims management. Some of the offerings available through ADP TotalSource to address today's workplace challenges include:

- **Better Employee 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 patented approach to help them target the best benefit plan offerings for their employees. They can compare plan options and make more educated decisions about what plan offering is best for their company and budget. In addition, ADP TotalSource integrates with ADP's ADP Marketplace to further tailor offerings, such as helping employees pay off student loans with payroll contributions and integrating a client's U.S. PEO population with its global workforce's HR system of record.
- **Protection and Compliance:** ADP TotalSource HR experts help clients manage the risks of being an employer by advising how to handle properly a range of issues – from HR and safety compliance to employee-relations. This includes access to workers' compensation coverage and expertise designed to help them handle both routine and unexpected incidents, including discrimination and harassment claims.
- **Talent Engagement:** Featuring a talent blueprint, ADP TotalSource HR experts work with clients to help them better engage and retain their workforce through solutions that support the core needs of an employee at work. In addition, ADP's full-service recruitment team is dedicated to helping its clients find and hire new talent, while reducing the stress of uncovering top talent.
- **Expertise:** Each client is assigned a designated HR specialist for day-to-day and strategic guidance. Clients can also access data-driven benchmarks in areas such as turnover and overtime, staffing and understanding profit leaks, and have their ADP HR expert help tailor recommendations to continue to drive their business forward. A payroll specialist is also available to clients to help them ensure their workers are paid correctly, on time and in compliance.

ADP Comprehensive Services - Leveraging its market leading ADP Workforce Now platform, ADP Comprehensive Services partners with clients of all 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 – enabling 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 robust 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) - ADP COS is designed for large business outsourcing for payroll, HR administration, workforce management, benefits administration and talent management. With

ADP 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 ADP COS offers allows clients to focus on strategy and results.

ADP Recruitment Process Outsourcing Services (ADP RPO®) - ADP RPO provides deep talent insights to help drive targeted recruitment strategies for attracting top talent. With global, customizable recruitment services, ADP RPO enables organizations to find and hire the best candidates for hourly, professional or executive positions. In addition, ADP also 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 deep compliance expertise.

ADP Global Payroll is a solution for multinational organizations of all sizes, empowering them to harmonize HCM strategies in 140 countries globally. This improves visibility, control and operational efficiency, giving organizations the insight and confidence to adapt to changing local needs, while helping to drive overall organizational agility and engagement.

ADP also offers comprehensive, country-specific HCM solutions that combine innovative technology with deep local expertise. By operating a flexible service model, ADP helps clients manage 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 over 15 million workers outside the United States with its in-country solutions and with ADP GlobalView, ADP Celergo/Streamline and ADP iHCM – ADP's simplified and intuitive multi-country 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 help elevate the employee experience, from recruitment to ongoing employee engagement and development. ADP's comprehensive HR solutions combined with deep expertise make its clients' global HR management strategies a reality. ADP's configurable, automated time and attendance tools help global clients understand the work being performed and the resources being used, and help ensure the right people are in the right place at the right time.

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

CONTROL ENVIRONMENT

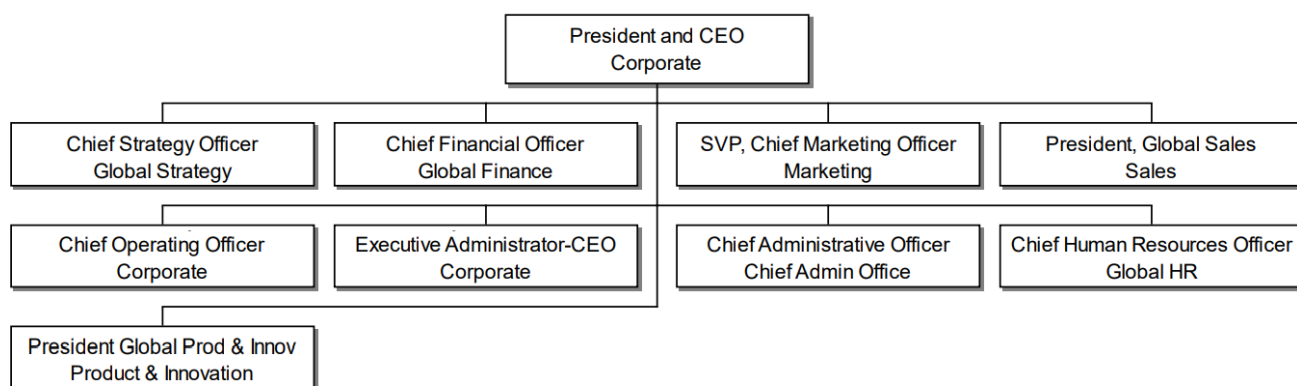
ADP's control environment reflects the position taken by management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. Management takes seriously defects identified in internal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

Oversight by ADP's Board of Directors

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

Organizational Structure

Corporate Structure



Other ADP Corporate Supporting Groups

Global Legal, Compliance, Ethics and Global Security Organization (GSO) - ADP's Global Legal, Compliance, GSO and Ethics departments, headquartered in Roseland, New Jersey, provide legal and compliance support for the company's business and functional organizations, as well as for ADP's Board of Directors.

Global Product & Technology (GPT) - The GPT organization is a driving force of over 10,000 technologists across the globe who design, develop and manage ADP's entire product and infrastructure portfolio to create experiences for clients, their employees and shape the future of work. GPT includes three core areas:

- Global Product & Innovation is a key factor in the design and management of ADP's products, including the user experience across products.
- Global Product Development uses those insights to manage ADP's portfolio and help ensure ease of use, quality, resiliency, and performance with capabilities for clients.
- Global Enterprise & Technology Solutions (GETS) is responsible for internal technology infrastructure for ADP associates and products.

Together, they are the backbone of ADP - a technology powerhouse with a unique purpose to provide a global HR program and solutions.

ADP GSO - ADP's Chief Security Officer oversees ADP's GSO and reports to the Chief Administrative Officer. The GSO consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined for all members of the GSO. The GSO is charged with the design, implementation and oversight of ADP's information security program based on corporate policies. The GSO's activities are overseen by the Executive Security Committee, whose members include ADP's Chief Executive Officer, Chief Operating Officer, ADP President, Chief Administrative Officer, Chief Human Resources Officer, Chief Legal Officer, Chief Financial Officer, and Corporate Vice President of Global Product & Technology.

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
- 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 personnel and a user awareness program is in place to familiarize employees with these core values. Associates are required to participate in the new hire orientation program which contains information about ADP's general operating practices, policies, and procedures, and assist 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 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 directors, officers, and employees of ADP. This policy covers areas of business conduct and ethics when working with clients, suppliers, the public, and other employees, and conflicts of interest that could arise between each associate's personal conduct and their positions with ADP. Associates who violate ADP's ethical standards and security policies are subject to progressive discipline, up to and including termination.

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

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

Corporate Internal Audit Function

The Corporate Internal Audit department is based at ADP's Corporate Headquarters in New Jersey, United States, and also has personnel located in Norfolk, VA, Europe and India. 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 is led by the Chief Audit Executive, who reports to ADP's Audit Committee and administratively to the Chief Financial Officer.

RISK ASSESSMENT

Enterprise Risk Management Process

The Board of Directors of ADP is in charge of overseeing ADP's enterprise risk and integrated risk management activities and initiatives, which are intended to identify, prioritize, analyze, monitor, and mitigate different risks that ADP faces, including risks relating to the ADP's operational and financial strategy execution. The Enterprise Risk Management (ERM) function is responsible for the day-to-day management of ADP's standard enterprise risk management process and the monitoring of the enterprise risk profile. ADP's Risk Taxonomy classifies ADP's risk profile into five families: strategic, digital and technology, operational, legal and compliance, and financial management and financial reporting. The risk taxonomy is reviewed and revised periodically with the advice of the Integrated Assurance Steering Committee and the Executive Risk Committee.

Executive leadership, senior leadership, and business function and corporate function areas are expected to participate in the annual enterprise risk assessment by assessing ADP's risk profile in terms of likelihood of occurrence, potential impact, and velocity, as well as emerging risks. The risk assessment results are communicated to the Executive Risk Committee, the Board Audit Committee, the Integrated Assurance Committee, Corporate Internal Audit, business unit and functional/regional leadership teams, and other relevant stakeholders annually.

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.

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

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

Third-Party Vendor Monitoring

ADP assesses, measures, monitors, and controls the risks associated with third parties through its Third-Party Risk Management program. Responsibility for the overall Third-Party Risk Management program resides within ADP's Global Procurement Organization and ADP's Global Third-Party Assurance Office (TPAO) within the GSO. Global Procurement is responsible for the third-party selection and on-boarding process and the managing

of the third-party relationship. The TPAO is responsible for the third-party risk monitoring process, as a preventive risk mitigation strategy against potential third-party threats, which includes developing and approving policies and procedures, communication of changes and updates to the policies.

CONTROL ACTIVITIES

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

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

INFORMATION AND COMMUNICATION

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

Employees

ADP has implemented various communication methods to assist employees in understanding their individual roles and corporate controls, and to encourage timely communication of significant events. The particulars vary from region to region but include orientation and training programs for new employees. 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.

CONTROL OBJECTIVES AND CONTROLS

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

OVERVIEW OF THE GLOBAL ENTERPRISE TECHNOLOGY & SOLUTIONS (GETS) NORTH AMERICA ORGANIZATION INFORMATION TECHNOLOGY SERVICE

Service Overview

ADP's Global Enterprise Technology & Solutions (GETS) North America organization (collectively referred to as the "GETS North America IT Services System") comprises the data center hosting services and the technology infrastructure hardware and software managed services (e.g., operating systems (OS)) and supporting network devices physically located at the GETS North America data centers in Georgia (Data Center 1) and in South Dakota (Data Center 2). The GETS North America IT Services System also includes the Network Management Services provided by the GETS North America organization comprised of network monitoring and network management/support.

Key Organizational Support Structure

GETS North America Organization

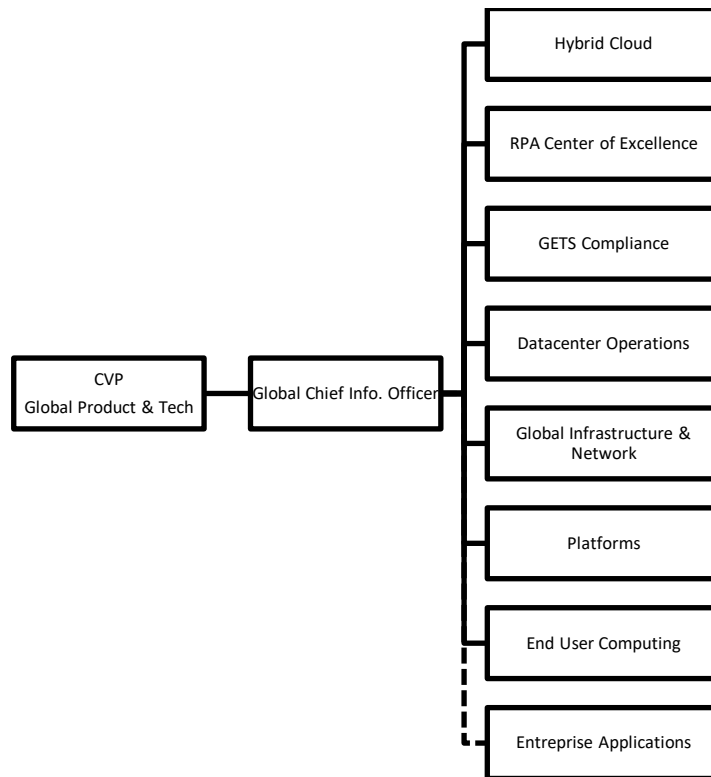
The GETS North America organization is led by the Global Chief Information Officer (CIO) who reports to ADP's President of Global Product and Innovation.

The GETS North America organization is divided into functional teams to meet the technical needs of ADP's business units.

The following is a description of the GETS North America Operations organization's relevant functional and support areas:

- Hybrid Cloud – Responsible for the design and operation of the hybrid cloud infrastructure
- Robotic Process Automation (RPA) Center of Excellence – Manages the administration of the BluePrism tool and governance over RPA
- GETS Compliance – Oversees operation of controls and compliance with company policies and standards
- Datacenter Operations – Responsible for datacenter availability, and Level 2 support
- Global Infrastructure & Network – Responsible for Level 3 support, availability, performance management, and for managing changes, problems, and incidents
- Platforms – Responsible for systems engineering (including servers, databases, middleware, and mainframe), Level 3 support, availability, performance management, and for managing changes, problems, and incidents
- End-User Services – Responsible for end-user computing for any ADP associate (service desk, laptop and desktop engineering, messaging services)
- Global Identity and Access Management – Responsible for network access provisioning and deprovisioning, manages administration of IDM tools and provides support to Product teams

Below is a chart of the GETS North America Operations organization relevant functional and support areas:



Changes to the Control Environment

Blue Prism, a tool used to develop Robotic Process Automation (RPA) tools has been added to the scope of this GETS North America SOC 1 Report. This includes standard tools testing (testing that the tool requires authentication with a username and password that abides by ADP’s GSO guidelines, and testing that administrative users to the tool are appropriate) and periodic user access review of users of the tool, which is centrally managed by GETS personnel (control 3.17).

The Network Security section has been expanded to include remote access controls, such as Virtual Private Network (VPN) and two-factor authentication (control 2.02).

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

SCOPE OF THE REPORT

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

This report covers the information technology (IT) services provided by ADP's GETS North America IT Services System.

The GETS North America IT Services System supports other ADP business units whose services are covered by other SOC 1 reports produced by ADP. Refer to Figure 1 below for a listing of the ADP ES services that issue SOC 1 reports that are supported by this Description.

Figure 1

ADP ES Services – SOC 1 Reports	In-scope Processes – ADP's GETS North America					
	Organization OS and Mainframe Change Management	Network Logical Security & Monitoring	Logical Security (OS, DB, & Mainframe)	Physical Security & Environment al Safeguards	System Backup	Operational Monitoring & Incident Management
AutoPay Payroll Services (US and Canada)	✓	✓	✓	✓	✓	✓
Retirement Services – 401(k) Participant Record Keeping	✓	✓	✓	✓	✓	✓
Retirement Services – Executive Deferred Comp	✓	✓	✓	✓	✓	✓
Total Absence Management	✓	✓	✓	✓	✓	✓
Enterprise 2000	✓	✓	✓	✓	✓	✓
MAS eLabor Manager	✓	✓	✓	✓	✓	✓
Managed Payroll Services (MPS)	✓	✓	✓	✓	✓	✓
Health and Welfare Benefits (Service Engine)	✓	✓	✓	✓	✓	✓

ADP ES Services – SOC 1 Reports	In-scope Processes – ADP’s GETS North America					
	Organization OS and Mainframe Change Management	Network Logical Security & Monitoring	Logical Security (OS, DB, & Mainframe)	Physical Security & Environment al Safeguards	System Backup	Operational Monitoring & Incident Management
NAS & MAS Enterprise eTime	✓	✓	✓	✓	✓	✓
Global WFM Enterprise eTime	✓	✓	✓	✓	✓	✓
Carrier Enrollment Services (CES)		✓		✓		✓
TotalPay & Wisely	✓	✓	✓	✓	✓	✓
TotalPay	✓	✓	✓	✓	✓	✓
Payroll Tax	✓	✓	✓	✓	✓	✓
Wage Garnishments Process Service (WGPS)	✓	✓	✓	✓	✓	✓
Wage Payments	✓	✓	✓	✓	✓	✓
MasterTax	✓	✓	✓	✓	✓	✓
ProBusiness		✓	✓	✓	✓	✓
TimeSaver on Demand	✓	✓	✓	✓	✓	✓
SBS RUN Payroll System	✓	✓	✓	✓	✓	✓
Tax Credit Services	✓	✓	✓	✓	✓	✓
Canada PayTech	✓	✓	✓	✓	✓	✓
Canada PayTech Restricted		✓	✓			
Canada IMM		✓				✓
Workforce Now (US and Canada) & Vantage	✓	✓	✓	✓	✓	✓
Benefits Marketplace	✓	✓	✓	✓	✓	✓
United Kingdom Payroll Managed Services and Payroll Processing (Freedom Application)	✓	✓	✓	✓	✓	✓
Next Gen Human Capital Management (HCM)		✓				
Workforce Now Next Gen		✓				
Celergo		✓				

ADP ES Services – SOC 1 Reports	In-scope Processes – ADP’s GETS North America					
	Organization OS and Mainframe Change Management	Network Logical Security & Monitoring	Logical Security (OS, DB, & Mainframe)	Physical Security & Environment al Safeguards	System Backup	Operational Monitoring & Incident Management
WorkMarket	✓	✓		✓		✓
TotalSource	✓	✓	✓	✓	✓	✓

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:

- OS, Infrastructure, and Mainframe Change Management
- Network Security and Monitoring
- Information Security
- Logical Security
- System Backup
- Physical Security
- Environmental Safeguards
- Operational Monitoring and Incident Management

OS, Infrastructure, and Mainframe Change Management

OS and Infrastructure

The Distributed Systems group is responsible for identifying security updates for Windows and Unix environments and for notifying personnel responsible for deploying the identified updates to the production environment. Patching is managed as part of the release management process by the Release Coordination group that uses automatic deployment technology to support quarterly patching cycles. Change Orders are submitted to authorize the deployment of the patches. The automated patch deployment technology analyzes the servers and applies relevant patches to each server, as needed, during the monthly or quarterly scheduled patching process.

The Distributed Systems group is also responsible for sending OS update notifications to other ADP groups responsible for installing the OS patches for servers located outside the GETS North America hosting and data center facilities and groups that opt out of the mass-patching process.

OS software, hardware, and infrastructure changes are requested by the GETS North America or Product teams and submitted using the CA Service Desk tool (Service Desk). Service Desk hardware and infrastructure change requests go through predetermined workflow steps through to implementation that includes obtaining approval(s) from the designated department(s). OS software, hardware, and infrastructure changes are tested in a non-production environment and approved by the designated system owner and/or the Change Advisory Board (CAB) before deployment. Upon completion of workflow steps leading up to implementation and receipt of required approvals, changes are implemented in production based on the provided specifications.

The CAB consists of management representatives from various groups within the GETS North America organization. The CAB holds weekly change control meetings with operating units to review, discuss, and

approve planned changes for implementation. Changes to the production environment are deployed by authorized personnel from the Data Processing Operations group.

Emergency changes (OS software, hardware, and infrastructure) follow the same initiation and approval process as standard changes but are also approved by ADP's Senior Management and are required to be implemented outside of normal maintenance schedules. Approvals are documented in a Change Request ticket.

Mainframe

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.

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 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.

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.

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 Mainframe production environment and installs the updates. With each release, the Corporate Mainframe System

Technology Group reviews system logs to determine whether the installation of the OS changes to the Regions' LPARs was successful and investigates identified problems until resolution.

Network Security and Monitoring

The ADP network is managed and controlled to protect information within systems and applications. The network architecture is segregated into security zones using firewalls and other ACL constructs to restrict access to authorized network activity.

Connections to the data centers from external networks are protected using encryption technologies. ADP associates working remotely use Virtual Private Network (VPN) via two-factor authentication.

Network Detection and Response (NDR) systems are in place to monitor network activity. Global Network Services, under the Data Networks group, is responsible for the configuration of the network. Network equipment, including firewalls and other ACL constructs, are maintained and monitored by the Global Network Services group. If necessary, the Global Network Services personnel initiate corrective actions to resolve issues. Automated network and infrastructure monitoring tools are deployed to control and monitor the network and critical networking equipment. Issues are documented in Service Desk tickets.

ADP has developed a global infrastructure of security tools, referred to as T3. T3 globally integrates best-of-breed products to enable ADP to proactively monitor and identify potential security incidents or exposures. T3 captures billions of events daily (i.e., security logs, unusual network connections, Intrusion Detection System (IDS) alerts, etc.), which are analyzed, correlated, and reviewed by the Critical Incident Response Center (CIRC).

The CIRC utilizes the Security Orchestration Automation and Response (SOAR) platform to track and report potential incidents that are created by the T3 infrastructure reported by associates, third parties, and/or clients. Archer supports both 'push' and 'pull' methods for incident creation, allowing for rapid triage and response to threats. Initial correlations of these incidents are performed by the various inputs into the SOAR platform where analysis and validation occur, and the results are memorialized in Archer and the security information data warehouse.

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.

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 ADP business units.

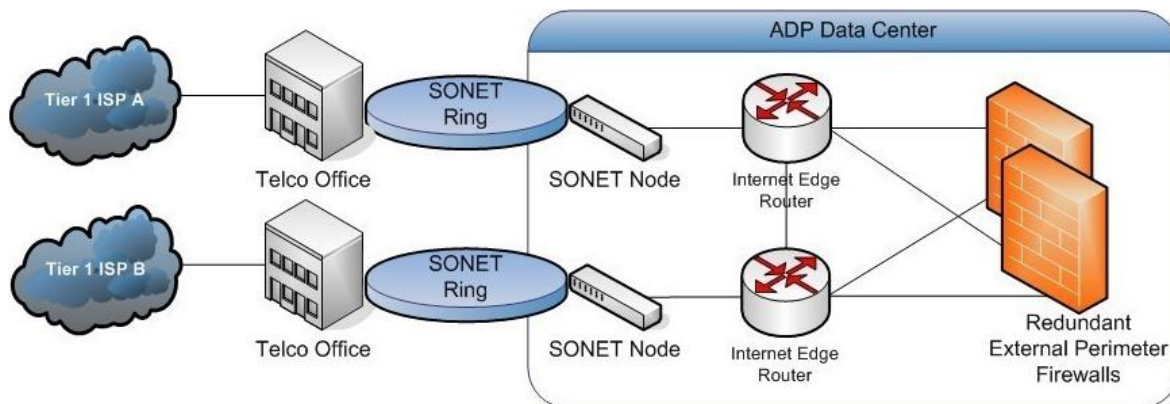
Logical Security

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.

The GETS North America organization is responsible for authorizing and provisioning network and OS administrative access and for provisioning authorized network and OS-level access needed by application support personnel. The ADP business units are responsible for application logical access controls that are covered in the specific product SOC 1 reports and are excluded from the scope of this report.

Network Access

ADP supports broadband Internet communications as the connectivity method to the GETS North America hosting and data center facilities. File transfers are supported by secure file transfer protocol standards and redundancy is supported through 10-gigabit Internet communication circuits and independent tier-1 Internet Service Providers (ISP). A logical view of the ADP redundant Internet connectivity architecture is depicted in the following diagram:



The processes and controls for network logical access are part of the GETS North America organization's common services provided to ADP's US, Canada, Philippines, and India-based ES business units. Network logical access controls including Active Directory (AD) access authorization, access revocation, access reviews,

and administrator access are included in the scope of this Description for North America-based ES business units and business units in the Philippines and India are described as follows.

The Associate Technology Management (ATM) group, part of the End-User Computing and End-User Support group, is responsible for assigning privileges to network user accounts. Each user requires a unique user ID and password before access is granted to the network. In the US and Canada, ADP uses an IDM (Identity Management) system that automates the process of managers granting and revoking network access privileges for their direct reports. The process for provisioning and deprovisioning network access is initiated by HR either through direct notification or through the IDM system. The IDM system interfaces with AD to automatically create or disable the AD account.

The process for provisioning and deprovisioning ADP India associates' network access is initiated by HR. To obtain network access, a ticket is submitted to the ATM group. The ATM group grants network access to the new or transferred associate. For terminations and transfers out, management or HR submits a ticket to revoke access. The user account is disabled in AD by the system administrators in India and a ticket is submitted to ATM to remove the user account.

For ADP employees based in the Philippines, network access requests (for new hires and transfers in) are initiated by HR through a Service Desk ticket. A Service Desk ticket is then submitted to the System Administrators in the Philippines who grant network access.

OS, Database, and Mainframe Access

Once network access is provisioned, associates can be given further access, including operating system, database, and Mainframe, based on their job responsibilities. Access is requested using the IDM system and requires proper approval by corresponding entitlement owners. If access is no longer needed, managers or entitlement owners submit a request to remove access using the IDM system. For terminated associates, request to remove access to operating systems, databases, and Mainframes is automatically submitted by the IDM system, which is either processed automatically via an interface or routed to the appropriate ADP group for processing.

ADP is in the process of transitioning to a new IDM system for access review and recertification. For systems that have been successfully migrated to the new tool, the LAT (Logical Access Team) team is responsible for coordinating the review of user listings based on a predefined review schedule. The review is initiated by the Campaign Owner using the IDM system. The IDM system sends email notifications to assigned reviewers and tracks their responses. Once the reviewers have validated their respective user listings, the campaign is finalized, and action is taken to modify user access where needed.

In addition to the IDM termination and recertification process, the Corporate Mainframe Security group has set up automated scripts that run periodically and automatically delete inactive RACF (Mainframe) accounts and flag users with extended (administrative) privileges for additional investigation.

Authentication and Security – Non-Mainframe

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

The Privileged Identity Management (PIM) password vaulting utility is installed on servers hosted at the GETS North America hosting and data center facilities and is used to control the default local administrative accounts and enforce password changes. Access to the PIM password vaulting utility is governed by AD groups created on ADP's network. OS administrator access to the stand-alone servers is restricted to authorized personnel through vaulted accounts. Associates must initially login to ADP's network and then, if they belong to an authorized AD group, they can access the PIM password vaulting utility. Revoking access to the PIM password vaulting utility relies on the revocation of the underlying AD access or removal from the AD group granting access to the vaults. Only a limited number of authorized personnel, based on assigned job responsibilities, have privileged (administrator level) access to the PIM password vaulting utility.

Authentication and Security – Mainframe

For Mainframe, logical access 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 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.

An audit trail of 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.

Tools

The GETS North America organization is responsible for authorizing and provisioning administrative access to the following tools needed by support personnel:

- Siebel
- CA Service Desk
- Bitbucket
- Ansible
- ADAPT
- Brainwave
- Control M
- Commvault
- Cyber Ark
- Blue Prism
- Centrify
- MFA

Administrative access to these tools is limited to appropriate associates.

RPA

GETS North America has implemented an RPA tool for developing and managing robotic processes used by Product teams. A governance model is in place to follow to ensure effective and efficient process automation. This includes controls over privileged access and periodic user access reviews.

Physical Security

Access to the GETS North America hosting and data center facilities is controlled by physical access systems (e.g., multi-level card access, biometrics, etc.). These facilities are monitored using a combination of surveillance cameras, motion detection cameras, and security guards.

Personnel must wear and display their ADP identification badges at all times. Visitors are required to sign a Visitor's Log, wear a visitor's badge, and are escorted by ADP personnel to their destination. Visitors to the GETS North America hosting and data center facilities are required to request access ahead of their visit. GETS North America management approves visitor access. Visitors requiring a temporary badge are required to present valid identification and sign the Visitor Log. Temporary badges expire twelve hours after activation.

Only Data Center security officers and authorized personnel have access to the badge access control system to grant and revoke badges for access to the GETS North America hosting and data center facilities. Access to the

hosting and data center facilities is restricted to ADP's associates and authorized permanent vendors. GETS North America management approval is required to gain access to sensitive areas. Changes to physical access over the GETS North America hosting and data center facilities (i.e., additions, modifications, and deletions) require authorization from appropriate ADP management and are executed and documented timely. Access for terminated or transferred GETS North America employees is revoked on or before the last day of employment based on notification from GETS North America management, the IDM system, and/or HR. Terminated employees are required to surrender their badge on or before their employment end date.

Management performs monthly reviews to verify the appropriateness of physical access to the GETS North America hosting and data center facilities. Discrepancies are followed up and resolved in a timely manner.

Environmental Safeguards

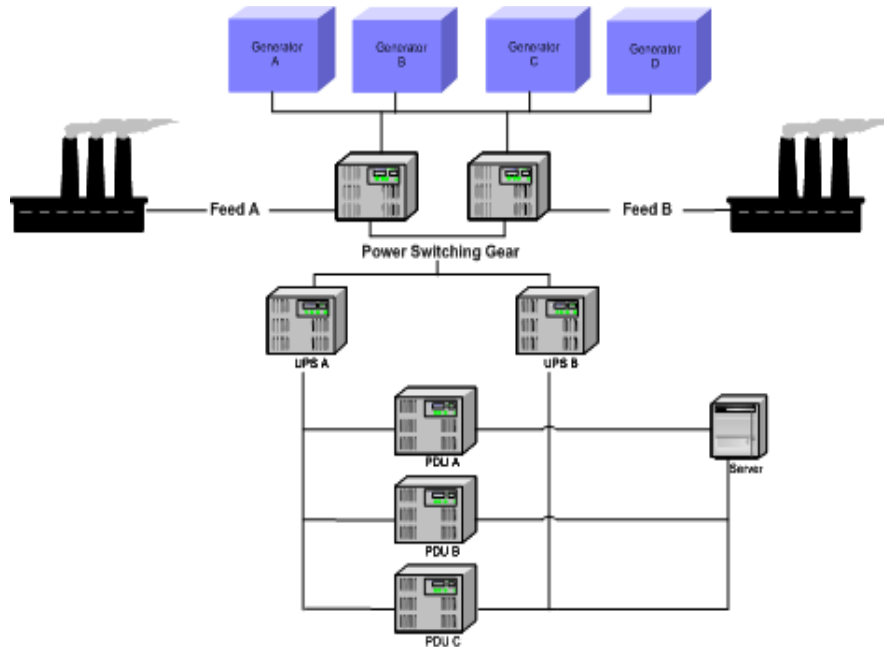
Equipment is installed for controlling environmental conditions in the computer rooms, telecommunications, and related technology equipment areas at each of the GETS North America hosting and data center facilities. Enterprise Technology Operations and third-party contractors test and maintain the fire suppression, heating, ventilation, air conditioning (HVAC), power supply, and water detection equipment regularly. Environmental safeguard issues are tracked and resolved following established problem-management procedures.

The GETS North America hosting and data center facilities that house the ADP production environments have deployed environmental safeguards including:

- Building fire alarms
- Fire, heat, and smoke detection systems
- Fire suppression systems
- Fire extinguishers
- HVAC systems comprised of Computer Room Air Handling (CRAH) units, chillers, cooling towers, steam humidification units, and a supplemental cooling system
- Uninterruptible Power Supply (UPS) equipment and generators to provide continuous power
- Redundant electrical and mechanical support equipment
- Water sensors
- Building automation systems (electrical power monitoring and building management that continuously monitor and control critical building systems)

Cables and wires connected to or coming from, computing equipment, and peripherals are stored away from normal traffic. Computer equipment power distribution cabling is located in trays under raised floors or in conduits above the dropped ceilings.

Power to the GETS North America hosting and data center facilities is supplied by two independent feeds. In the event one power feed experiences an outage, the second feed will provide power from the backup line. The power feeds, generators and distribution units are logically depicted in the diagram on the following page.



System Backup

Data Backup – Windows, UNIX, and OS and DB Servers

The Distributed System Group's Storage Management team configures the automated backup schedules for open systems (e.g., Windows and UNIX) according to the ADP business units' defined requirements. Daily incremental backups and weekly full backups are stored onsite, using a virtual disk. Data is also replicated from production systems to disaster recovery systems in live mode. The Storage Management team monitors the results of the scheduled backup jobs. Any identified backup issues or exceptions are documented in the problem management system and followed up on to resolution.

Data Backup and Replication – Mainframe

IBM's virtual tape servers and physical tape drives located at ADP's GETS North America hosting and data center facilities are used to perform incremental and full backups of the Mainframe application. The incremental backups are performed daily (overnight) Monday to Friday and full backups are performed weekly, on Saturday night, using IBM's virtual tape servers and physical tape drives located at ADP's GETS North America hosting and data center facilities. EMC 5500 servers are used for full-disk mirroring. The backup processes are automated and scheduled using the Control-M Scheduling Software. Point-in-time backups are used for restoring

data from prior dates. Data backed up in one data center is replicated and stored at another data center based on the schedule requested by ADP business units.

The backup policy requires that the system be backed up before new releases are installed and new products are implemented.

Operational Monitoring and Incident Management

Problem/Incident Management

Technical Support and Service Desk organizations continuously monitor batch job streams, online applications, third-party tools, transmission systems, e-mail, user requests, morning reports, etc., to identify abnormal conditions and possible incidents. Several tools are utilized to facilitate monitoring. These tools are programmed to recognize certain conditions and to generate alerts when these conditions are encountered.

Alerts may be directed either to support group operators, technical support analysts, an engineering group, or management team members. Certain important alerts may be directed simultaneously to multiple organizations.

When an alert is generated, it is evaluated for significance. Low impact incidents are handled within the support group and a ticket is created, as needed, to document the action taken to respond to the alert. Higher impact incidents require ticket creation and are processed, as instructed, by the incident management process.

The GETS North America hosting and data center facilities are staffed with ADP support teams 24 hours a day, 7 days a week, 365 days a year. Identified problems, including hardware incidents, are documented and managed via the problem management system. Upon request from other ADP teams, including the Support Group, network engineers, and Mainframe engineers, the GETS North America hosting and data center facilities personnel support the overall incident resolution and management process. In general, incidents requiring onsite attention to GETS North America hosting and data center facilities hardware, supporting infrastructure, or environmental equipment are assigned to the DC Site Management team for resolution.

Third-party monitoring tools are deployed to alert Data Processing Operations personnel of issues with production environments. GETS North America & Open System Engineering personnel are responsible for tracking the issues to resolution.

For major outages or an outage that affects multiple client environments, Data Processing Operations notifies the business units about planned and unplanned major outages and provides status updates periodically.

Job Scheduling and Monitoring – Mainframe

The M&MTAM Technical Services group is responsible for scheduling jobs, including data backup jobs, and problem management for the Mainframe applications. The M&MTAM Support Group is responsible for job execution, job monitoring, system monitoring, and workload balancing.

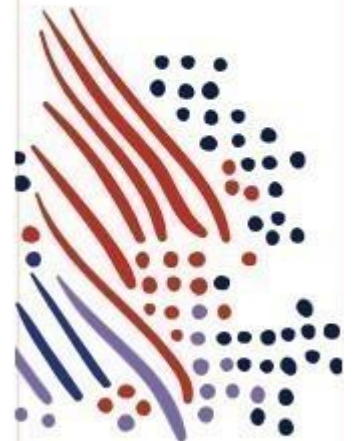
ADP uses the Control-M Scheduling Software to execute required jobs and tasks. The scheduled jobs support transaction processing and backup processing. The M&MTAM Support Group monitors the job scheduling status screens to verify that scheduled jobs are processed in accordance with established routines and procedures. Upon the identification of a backup issue or error, a ticket is automatically generated within the ticketing system that facilitates identifying recurring issues and enables tracking and researching problems through to resolution. The M&MTAM Technical Services group and Operations groups in the regions are responsible for promptly resolving identified issues.

COMPLEMENTARY USER ENTITY CONTROLS

There are no complimentary user entity controls as the GETS North America IT Services System provides direct support to other ADP business unit services as described in the *Scope of the Report* section of this Description. Clients are responsible for understanding which ADP business unit services they have contracted for and for evaluating the controls described within the applicable ADP SOC 1 report for those services as well as the controls described within this report.

SECTION FOUR

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



TESTING PERFORMED AND RESULTS OF TESTS OF ENTITY-LEVEL CONTROLS

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

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

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

GENERAL COMPUTER CONTROL OBJECTIVES AND CONTROLS

Operating System and Infrastructure Change Management

Control Objective 1: Controls provide reasonable assurance that the implementation of and changes to operating system software, hardware, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>OS Software, Hardware, Infrastructure, and Mainframe</i>			
1.01	<i>Policies</i> ADP has a formal Change Management Process that outlines the requirements for documenting and making system changes (OS software, hardware, infrastructure, and Mainframe).	Inspected the Change Management Policy document to determine whether ADP has established and documented a formal process that defines the requirements for documenting and making OS software, hardware, infrastructure, and Mainframe changes.	No deviations noted
1.02	<i>Authorization</i> OS software, hardware, infrastructure, and Mainframe changes are formally authorized by management according to established procedures.	For a sample of OS software, hardware, infrastructure, and Mainframe changes deployed to the production environment, inspected the ticket and compared to the Change Management Policy to determine whether the changes were authorized by management according to established procedures.	No deviations noted

Control Objective 1: Controls provide reasonable assurance that the implementation of and changes to operating system software, hardware, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.03	<i>Testing/Approval</i> OS software, hardware, infrastructure, and Mainframe changes are tested in a non-production environment as deemed necessary based on risk level and approved by the designated system owner and/or the Change Advisory Board (CAB) before deployment.	For a sample of OS software, hardware, infrastructure, and Mainframe changes deployed to the production environment, inspected the ticket to determine whether the change was tested in a non-production environment as required by the change type and approved by the designated system owner and/or the CAB before deployment.	No deviations noted
1.04	<i>Deployment to Production Environment</i> OS software, hardware, infrastructure, and Mainframe changes are deployed to the production environment by authorized personnel.	For a sample of OS software, hardware, infrastructure, and Mainframe changes deployed to the production environment, inspected the ticket to determine whether the change was deployed by authorized personnel.	No deviations noted

Control Objective 1: Controls provide reasonable assurance that the implementation of and changes to operating system software, hardware, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.05	<p><i>Access to Deploy to Production Environment</i></p> <p>Access to deploy OS software, hardware, infrastructure, and Mainframe changes to the production environment is restricted to appropriate personnel.</p>	<p>Inspected the RACF user access listing to identify individuals with the ability to migrate OS and database changes to the Mainframe production environment, inspected job titles and inquired of the Senior Director – Technical Services to determine whether access was appropriate based on job responsibilities.</p> <p>Inspected the system-generated listing of users with access to the deployment tool used for OS software, hardware, and infrastructure changes and inquired of Release Coordination Management regarding job responsibilities to determine whether access to the tool was restricted to authorized personnel.</p>	<p>No deviations noted</p> <p>No deviations noted</p>
1.06	<p><i>Emergency Changes</i></p> <p>Emergency OS software, hardware, and infrastructure changes are approved by ADP management.</p>	<p>For a sample of emergency OS software, hardware, and infrastructure changes deployed to the production environment, inspected the ticket to determine whether the emergency change was approved by ADP management.</p>	<p>Inquired of management and inspected supporting documentation to determine that no emergency changes occurred during the examination period. Outside of these procedures, no testing was performed.</p>

Control Objective 1: Controls provide reasonable assurance that the implementation of and changes to operating system software, hardware, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>Mainframe-only</i>			
1.07	<i>Source Code – Mainframe</i> Source code is controlled and monitored using the ChangeMan version control system and the ability to migrate code to the Mainframe production environment is restricted to authorized personnel and excludes those responsible for development functions.	Inquired of the Director of Mainframe Security to determine whether ChangeMan was utilized to control source code for the Mainframe. Inspected the system generated listing of users with the ability to migrate code to the Mainframe production environment, compared the users against the system generated listing of developers, and inquired of the Director of Mainframe Security to determine whether access was appropriate based on the individual's job responsibility and excluded those responsible for development functions.	No deviations noted No deviations noted

Network Security and Monitoring

Control Objective 2: Controls provide reasonable assurance that ADP’s network is monitored, and security mechanisms are in place to protect from external threats and interruptions.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
2.01	<i>Architecture & Security</i> The network architecture is segregated into segments and firewalls, and network-based Intrusion Detection Systems (IDS), and Network Address Translation (NAT) devices are in place to monitor and restrict access to authorized network activity.	Inspected relevant system settings and network diagrams and utilized video conferencing technology assisted by ADP personnel to observe real-time functioning of network devices to determine whether the ADP network was segregated into segments and firewalls, and network-based IDS, and NAT devices are in place to monitor and restrict access to authorized network activity.	No deviations noted
2.02	<i>Remote Access</i> ADP associates authenticate to ADP’s network remotely using VPN that requires two-factor authentication.	Inspected relevant network configuration to determine whether a user must use two-factor authentication for remote access.	No deviations noted
2.03	<i>Problem Identification</i> ADP network personnel control and monitor the network and critical network equipment in real-time and are responsible for documenting network issues and the corresponding resolution.	Observed Global Network Services personnel on a sample day monitoring the network and critical network equipment to determine whether ADP network personnel used network and infrastructure monitoring tools to perform real-time monitoring and corrective actions were initiated by opening tickets when issues were identified, as necessary. For a sample of identified network issues, inspected the ticket to determine whether the issue and the corresponding resolution was documented.	No deviations noted No deviations noted

Control Objective 2: Controls provide reasonable assurance that ADP's network is monitored, and security mechanisms are in place to protect from external threats and interruptions.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
2.04	<p><i>Security Incident Monitoring</i></p> <p>Security incidents identified by internal monitoring tools (i.e., IDS), reported by clients or reported by ADP associates are captured in ADP's GRC reporting tool and followed through to resolution.</p>	Utilized video conferencing technology assisted by ADP personnel to observe personnel within ADP's Critical Incident Response Center on a sample day actively identifying potential security incidents to determine whether incidents were captured within the GRC reporting tool.	No deviations noted
		Observed a sample alert from the IDS monitoring tool automatically create a ticket within the GRC reporting tool to determine whether security incidents identified by internal monitoring tools were captured.	No deviations noted
		For a sample of security incidents logged within the GRC reporting tool, inspected the corresponding GRC ticket to determine whether the security incidents were investigated through to resolution and documented.	No deviations noted

Logical Security

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.01	<i>Information Security Policy</i> ADP's Information Security Policies are available on the corporate intranet and provide overall guidance for data security administration, internal/external user security, and access to information systems.	Inspected the ADP intranet and the documented Information Security Policies to determine whether they were available on ADP's intranet and contained guidance for data security administration, internal/external user security, and access to information systems.	No deviations noted
3.02	<i>Network User Authentication</i> Each user requires a valid user ID and password for network authentication through Active Directory (AD).	Inquired of the network administrator and observed a sample ADP user log into the network to determine whether a valid user ID and password was required for successful authentication through AD.	No deviations noted
3.03	<i>Network Password Policies</i> Password rules/restrictions are enforced at the network-level according to the Global User Authentication Standard Policy.	Inspected the relevant network password configuration settings and ADP's password policies to determine whether network-level password rules/restrictions, including periodic forced password changes, password complexity, and password history were configured according to the Global User Authentication Standard Policy.	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.04	<i>User Access Management – Network, OS, Mainframe</i> User account additions and modifications (Network/OS/Mainframe only) require authorization from appropriate ADP management. Changes are documented and executed by an individual separate from the requestor according to policy and as requested.	For a sample of new network and OS/Mainframe user access requests (additions and modifications), inspected the documented user access IDM ticket and current system user listings to determine whether the access was requested and approved by appropriate ADP management who is different from the individual who executed the change and access was granted as requested.	No deviations noted
3.05	<i>Network and OS Administrative Access</i> Only appropriate users have been granted administrator privileges for ADP's network and operating systems.	Inspected system-generated user listings of users with administrator access to ADP's network and in-scope operating systems and inquired of ADP management to determine whether access was appropriate based on job responsibilities.	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.06	<p><i>Access Deprovisioning – Network, OS, Mainframe</i></p> <p>For terminated associates, request to remove access to operating systems, databases, and Mainframes is automatically submitted by the IDM system, which is either processed automatically via an interface or routed to the appropriate ADP group for processing.</p>	<p>Inspected relevant IDM source code to determine whether network user accounts belonging to terminated employees and contractors were automatically disabled upon termination date.</p> <p>For a sample terminated user, inspected a screenshot of the user's termination status in the IDM system and the ticket opened to determine whether a ticket was automatically opened upon termination.</p> <p>For a sample of terminated users, inspected the ticket to request removal of Mainframe access and the Mainframe user listing to determine whether Mainframe access was removed for each terminated user.</p>	<p>No deviations noted</p> <p>No deviations noted</p> <p>No deviations noted</p>
3.07	<p><i>OS User Authentication</i></p> <p>A valid LDAP or AD user ID and password are required for OS authentication.</p>	<p>Observed an ADP associate log into a sample of Windows and UNIX OS to determine whether a valid LDAP or AD user ID and password was required for successful authentication.</p>	<p>No deviations noted</p>

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.08	<i>OS Password Policies</i> Password rules/restrictions are enforced at the server level through AD or LDAP and are configured according to ADP's security policies and standards.	Inspected the relevant AD and LDAP password configuration settings governing access to the OS 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
3.09	<i>Active Directory Access Review</i> Management reviews and approves user access within the North America hosting domain based on a predetermined schedule. Any issues are documented and resolved.	For a sample of Active Directory Groups, performed the following procedures: <ul style="list-style-type: none"> • Inspected the ticket and supporting review documentation within the North America hosting domain to determine whether the AD groups were reviewed by the users' managers based on the pre-defined schedule and issues identified were documented and resolved. • For a sample of user access changes identified during the review, inspected the relevant system-generated list of users and IDM tickets to determine whether access was modified as requested. 	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.10	<i>Administrator Access – PIM Password Vaulting Utility</i> A limited number of appropriate personnel have administrator access to the PIM password vaulting utility that provides access to the operating system administrator account.	Inspected the system-generated list of users with administrator access to the PIM password vaulting utility, inquired of management, and inspected job titles to determine whether access was assigned to a limited number of appropriate individuals based on job responsibilities.	No deviations noted
3.11	ADP associates accessing the Mainframe 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 the Mainframe 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 the Mainframe to determine whether a valid user ID and password was required to access the system.	No deviations noted No deviations noted
3.12	<i>Privileged Access - Mainframe</i> Only appropriate IT personnel have access to the administrative functionality and key Mainframe datasets	Inspected the system-generated listings of users with access to key Mainframe datasets in the Mainframe and inquired of Corporate Mainframe Security management regarding job responsibilities to determine whether access was restricted to authorized personnel.	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.13	<i>Privileged Groups Review - Mainframe</i> IT Management reviews the list of users with privileged rights (DBA, Storage, CICS, MVSYS) on a monthly basis.	For a sample of months, 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 monthly 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 monthly review, inquired of the M&MTAM Manager and re-performed the review for a sample of users to determine whether the process to review access on the Mainframe was precise.	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.14	<p><i>Inactive Accounts - Mainframe</i></p> <p>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.</p>	<p>Inspected the configuration of the relevant automated script within the Mainframe 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.</p>	No deviations noted
		<p>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.</p>	No deviations noted
		<p>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.</p>	No deviations noted

Control Objective 3: 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.

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

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.16	<p><i>Access Review – Mainframe</i></p> <p>On a semi-annual basis, management reviews the list of users with access to the RACF and confirms that access is appropriate for the users' current job responsibilities.</p>	Inspected the access recertification tool and a sample RACF application review documentation to determine whether management completed the semi-annual review of RACF accounts for business users.	No deviations noted
		For a sample of changes requested during the semi-annual review, 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 semi-annual review, inquired of the M&MTAM Manager and re-performed the review for a sample of users to determine whether the process to review access on the Mainframe was complete and accurate.	No deviations noted

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.17	<p><i>Access Review – RPA</i></p> <p>On a semi-annual basis, management reviews the list of users with access to Blue Prism and confirms that access is appropriate for the users' current job responsibilities.</p>	<p>Inspected the RPA recertification tool review documentation to determine whether the semi-annual review of Blue Prism RPA privileged users was completed.</p> <p>For a sample semi-annual review, inspected the confirmation emails and user listings to determine whether the Blue Prism RPA review accounts belonging to privileged users was completed.</p> <p>For a sample of changes requested during the semi-annual review, inspected updated user listings to determine whether identified changes were completed as requested.</p>	<p>No deviations noted</p> <p>No deviations noted</p> <p>No deviations noted</p>
3.18	<p><i>Password Policies – In-scope Tools</i></p> <p>Password rules/restrictions are configured according to ADP's security policies and standards.</p>	<p>Inquired of ADP Management and inspected the relevant authentication configuration settings governing access to in-scope tools 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.</p>	<p>No deviations noted</p>

Control Objective 3: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.19	<p><i>Administrator Access – In-scope Tools</i></p> <p>A limited number of appropriate personnel have administrator access to supporting tools used for hosting operations.</p>	For the in-scope tools, inspected system generated user listings and inquired of ADP management to determine whether administrator access appeared appropriate based on job responsibilities.	No deviations noted

Physical Security

Control Objective 4: Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized and appropriate personnel.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
4.01	<i>Physical Access Mechanisms</i> Access to the hosting and data center facilities is controlled by physical access mechanisms such as card key access, biometrics, etc., and is monitored by surveillance cameras.	For each of the in-scope hosting and data center facilities, utilized video conferencing technology assisted by ADP hosting and data center facilities personnel or walked through and observed the facilities in person to determine whether: <ul style="list-style-type: none"> Physical access mechanisms (e.g., card key, biometric) were installed and operating before entering the facilities. Physical access to the facilities was monitored by surveillance cameras. 	No deviations noted
4.02	<i>Access Administration</i> Changes to physical access over the hosting and data center facilities (i.e., additions, modifications, and deletions) require authorization from appropriate ADP management and are executed and documented timely.	For a sample of additions, modifications, and deletions (terminations), inspected the documented request to grant, modify, remove access to the in-scope hosting and data center facilities to determine whether the requests were completed and approved by authorized ADP management timely. For a sample of additions, modifications, and terminations, inspected physical access listings generated from the badging system to determine whether access was granted/revoked in accordance with the request.	No deviations noted No deviations noted

Control Objective 4: Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized and appropriate personnel.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
4.03	<i>Access Privilege Review</i> On a monthly basis, management reviews the list of users who have physical access to the hosting and data center facilities and confirms that the access is appropriate for the users' current job responsibilities.	For a sample of months, inspected the physical access review documentation to determine whether management reviewed the system-generated listing of users with access to each of the in-scope hosting and data center facilities to confirm the appropriateness of access based on users' job responsibilities and any identified discrepancies were documented and resolved.	No deviations noted
4.04	<i>Access to Badge System</i> Access to the badge access control system used to grant and revoke badges is restricted to appropriate personnel.	Inspected the system-generated list of users with access to the badge access control system used to grant and revoke badges to each of the in-scope hosting and data center facilities and inquired of management regarding job responsibilities to determine whether access was restricted to appropriate personnel.	No deviations noted

Environmental Safeguards

Control Objective 5: Controls provide reasonable assurance that 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
5.01	<p><i>Environmental Safeguards</i></p> <p>The hosting and data center facilities are equipped with the following environmental safeguards:</p> <ul style="list-style-type: none"> • A fire suppression system • A heating, ventilation, air conditioning (HVAC) system • UPS • Generators • Water sensors 	<p>For each of the in-scope hosting and data center facilities, utilized video conferencing technology assisted by ADP hosting and data center facilities personnel or walked through and observed the facilities in person to determine whether the following environmental safeguards existed:</p> <ul style="list-style-type: none"> • A fire suppression system • HVAC system • UPS • Generators • Water sensors 	No deviations noted

Control Objective 5: Controls provide reasonable assurance that 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
5.02	<i>Equipment Maintenance</i> Management and/or third parties regularly test and maintain environmental safeguards within the hosting and data center facilities.	For a sample of quarters for the in-scope hosting and data center facilities, inspected maintenance records and inquired of hosting and data center facility personnel to determine whether test and maintenance activities were performed for UPS, HVAC, generators, and waters sensors according to schedule. Inspected the most recent annual maintenance records and inquired of hosting and data center facility personnel to determine whether test and maintenance activities were performed for the fire suppression system according to schedule for the in-scope hosting and data center facilities.	No deviations noted No deviations noted
5.03	<i>Problem Management</i> Environmental safeguard issues are tracked and resolved following established problem-management procedures.	For a sample of identified environmental safeguard issues within each of the in-scope hosting and data center facilities, inspected the ticket to determine whether the issue was documented, tracked, and resolved following established problem management procedures.	No deviations noted

System Backup

Control Objective 6: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>Windows and UNIX</i>			
6.01	<i>Scheduling</i> Backup jobs are executed according to the schedule and retention requirements provided by the ADP business unit owners and in accordance with infrastructure platform requirements.	For a sample of in-scope servers, inspected the backup configuration settings and inquired of the business unit owners to determine whether programs and data were scheduled to be backed up and retained in accordance with ADP business unit owners and infrastructure platform requirements.	No deviations noted
6.02	<i>Monitoring and Problem Management</i> ADP personnel monitor the backup procedure results and are alerted by the application of any backup issues or exceptions. Issues are monitored and followed through to resolution.	For a sample of in-scope servers and days, inspected backup system logs and tickets to determine whether scheduled backup jobs were completed successfully, and issues identified, if any, were monitored and followed through to resolution.	No deviations noted
6.03	<i>Onsite Backup Storage</i> Backups are stored within the hosting and data center facilities using virtual disk storage.	For each of the in-scope hosting and data center facilities, utilized video conferencing technology assisted by ADP hosting and data center facilities personnel or walked through and observed the facilities in-person to determine whether backups were stored using virtual disk storage.	No deviations noted

Control Objective 6: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>Mainframe</i>			
6.04	<i>Backup Scheduling</i> Backup jobs are executed according to the backup schedule and take place automatically through the Control-M tool scheduling system.	For a sample of LPARs, inspected the relevant configuration settings within the Control-M tool scheduling system to determine whether the programs and data that have been identified as requiring periodic backup were scheduled for automatic backups. For a sample LPAR and date, inspected the backup log to determine whether backups were successfully completed.	No deviations noted No deviations noted
6.05	<i>Monitoring and Problem Management</i> The M&MTAM Support Group monitors the results of the backup procedures and is alerted by the application through an automatically generated ticket of any identified backup issues or exceptions. Issues, if any, are documented, reported, and followed up on to resolution.	For a sample of backup issues or exceptions, inspected the automatically generated ticket to determine whether the identified backup issue or exception was documented, followed up to resolution, and the backup subsequently ran successfully.	No deviations noted
6.06	<i>Job Scheduler Access</i> Access to the backup control system used to schedule backup jobs is restricted to authorized personnel.	Inspected the list of individuals with access to schedule backup jobs in the backup control system and inquired of Operations personnel to determine whether access to backup schedules was limited to authorized ADP associates based on assessment of job titles/responsibilities.	No deviations noted

Control Objective 6: 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.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
6.07	<i>Offsite Backup Replication</i> Data backed up in one data center is replicated and stored at another data center based on the schedule requested by ADP business units.	For a sample of LPARs, inspected the data replication configuration settings to determine whether data backed up in one data center was scheduled to be replicated and stored at another data center. For a sample of in-scope LPARS, inspected the job log file for a sample day to determine whether the backup data was replicated to a second data center in accordance with ADP business unit requirements.	No deviations noted No deviations noted

Operational Monitoring and Incident Management

Control Objective 7: Controls provide reasonable assurance that operational problems are identified and resolved in a timely manner.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>Windows and UNIX</i>			
7.01	<i>Operational Monitoring</i> Automated tools are in place to monitor system availability, performance, hardware issues, backup equipment, and other system-related issues.	<p>Inspected documented operational monitoring and problem management procedures to determine whether guidelines for monitoring system availability, performance, hardware issues, backup equipment, and other system-related issues were established and maintained.</p> <p>For each of the in-scope hosting and data center facilities, utilized video conferencing technology assisted by ADP hosting and data center facilities personnel or walked through and observed hosting and data center facilities personnel on a sample day monitoring system availability, performance, hardware, backup equipment, and other system-related issues to determine whether automated monitoring tools were used to monitor system issues.</p>	<p>No deviations noted</p> <p>No deviations noted</p>
7.02	<i>Incident Management</i> System-related issues are documented, reported, and followed through to resolution.	For a sample of system-related issues identified by the monitoring tools, inspected the ticket to determine whether the issue was reported, documented, and resolved timely.	No deviations noted

Control Objective 7: Controls provide reasonable assurance that operational problems are identified and resolved in a timely manner.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
<i>Mainframe</i>			
7.03	<p><i>Mainframe Job Scheduling Monitoring</i></p> <p>The M&MTAM Support Group monitor the status of the scheduled jobs and are alerted of any identified processing issues or exceptions. Issues/exceptions are documented, reported, and followed up on to resolution.</p>	<p>Observed the M&MTAM Support Group monitoring scheduled job processing alerts on a sample day to determine whether identified processing issues or exceptions were monitored in real-time using the Control-M tool.</p> <p>For a sample of job processing issue/exception alerts, inspected the automatically generated ticket to determine whether identified processing issues were documented, reported, and followed up on to resolution.</p> <p>Inspected the system-generated listing of users with access to Control-M and inquired of the Director Technical Services to determine whether access to the Control-M scheduling tool is restricted to appropriate individuals based on job responsibilities.</p>	<p>No deviations noted</p> <p>No deviations noted</p> <p>No deviations noted</p>

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 is committed to keeping its services and operations running smoothly so that ADP can provide its clients with the best service possible. It's ADP's priority to identify technology, environmental, process and health risks, and 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 has been developed, in compliance with applicable regulations and guidelines, to establish a single global framework for how ADP manages, and controls identified risks resulting from disasters and other significant business disruptive events. ADP has created an integrated framework that lays out mitigation, preparedness, response, and recovery processes.

Disaster Recovery Planning

Disaster Recovery plans are developed to recover and/or restore critical systems. Redundancies are built into the systems as deemed appropriate. Recovery times vary according to the criticality of the impacted system.

The Disaster Recovery plans are 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, thereby reducing the impacts resulting from service interruptions
- Recover essential Data Center operations in a timely manner, increasing ADP's ability to recover from a loss to a Data Center

The Disaster Recovery plans are designed to create a state of readiness that will provide 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 Data Center facility access such as closure due to a storm, an emergency building evacuation due to a threat, or an external threat such as a fire to a nearby facility
- Impending or unexpected regional disasters such as an earthquake, hurricane, typhoon, or flood
- External incidents, which potentially could cause a service interruption, such as loss of electrical or telecommunication services

The Disaster Recovery plans are reviewed, revised, and tested annually. Various components may be subject to semi-annual or quarterly reviews and revisions.

Business Continuity Planning

Business Continuity plans are developed to maintain or restore business operations in certain time frames following interruption to, or failure of, critical business processes and systems.

The 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 process owners
- Subjected to formal change control procedures
- Distributed to all individuals who would need them in case of an emergency

The Business Continuity plans are intended to provide prompt response and subsequent recovery from an unplanned business interruption, such as a loss of critical service, loss of building access or physical facility catastrophe. ADP's Business Continuity plans are focused on restoring specific services to clients.

The Business Continuity plans are required to be reviewed and revised at least annually, and various components may be subject to off-cycle reviews and revisions. A pre-planned walkthrough must be conducted annually, and an exercise (i.e., tabletop, simulation, integrated) must be conducted every two years.