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

Description of ADP's Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System for the period April 1, 2019 to March 31, 2020

Always Designing
for People™

Table of Contents

SECTION ONE **PAGE**

Independent Service Auditor's Report provided by Ernst & Young

SECTION TWO

Management Assertion

SECTION THREE

Description of ADP's Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System for the period April 1, 2019 to March 31, 2020

SECTION FOUR

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

SECTION FIVE

Other Information Provided by ADP

SECTION ONE

INDEPENDENT SERVICE AUDITOR’S REPORT PROVIDED BY ERNST & YOUNG

Building a better
working world

Ernst & Young LLP
200 Clarendon Street
Boston, MA 02116

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

INDEPENDENT SERVICE AUDITOR’S REPORT

Management of Automatic Data Processing, Inc.

Scope
We have examined Automatic Data Processing, Inc.’s (ADP) description entitled “Description of ADP’s Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System for the period April 1, 2019 to March 31, 2020” (Description) of its Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System (System) for 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 “ADP Management Assertion” (Assertion). The Control Objectives and controls included in the Description are those that management of ADP believes are likely to be relevant to user entities’ internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

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

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

Service auditor’s responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those

standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period April 1, 2019 to March 31, 2020. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Inherent limitations

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

Description of tests of controls

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

Opinion

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

a. The Description fairly presents the System that was designed and implemented throughout the period April 1, 2019 to March 31, 2020.
b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period April 1, 2019 to March 31, 2020.

c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period April 1, 2019 to March 31, 2020.

Restricted use

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

Ernst + Young LLP

June 11, 2020

SECTION TWO

MANAGEMENT ASSERTION

ADP MANAGEMENT ASSERTION

June 11, 2020

We have prepared the description of Automatic Data Processing, Inc.'s (ADP) Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System entitled, "Description of ADP's Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System for the period April 1, 2019 to March 31, 2020" (Description) for supporting the processing of user entities' transactions or identification of the function performed by the system throughout the period April 1, 2019 to March 31, 2020 for user entities of the system during some or all of the period April 1, 2019 to March 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by the 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 ADP's Global Enterprise Technology & Solutions (GETS) US Organization Information Technology Services System (System) made available to user entities of the System during some or all of the period April 1, 2019 to March 31, 2020 for supporting the processing of their transactions or identification of the function performed by the system 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, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and

- other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring activities that are relevant to the services provided.

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

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

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period April 1, 2019 to March 31, 2020 to achieve those control objectives, throughout the period April 1, 2019 to March 31, 2020. The criteria we used in making this assertion were that:

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

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

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

Automatic Data Processing, Inc.

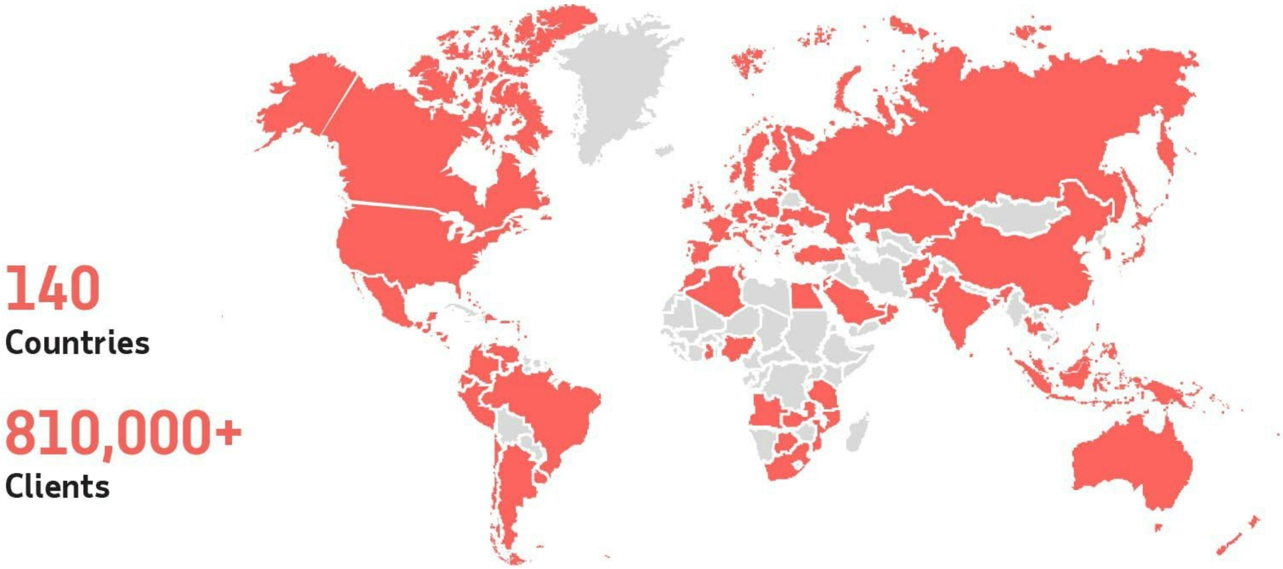
SECTION THREE

DESCRIPTION OF ADP'S GLOBAL ENTERPRISE TECHNOLOGY & SOLUTIONS (GETS) US ORGANIZATION INFORMATION TECHNOLOGY SERVICES SYSTEM FOR THE PERIOD APRIL 1, 2019 TO MARCH 31, 2020

OVERVIEW OF OPERATIONS

General

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



Business Overview

ADP's Mission

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

ADP's Strategy - Strategic Pillars

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

HCM Solutions

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

HRO Solutions

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

Global Solutions

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

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

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

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

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

Business Segments

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

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

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

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

Products and Solutions

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

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

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

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

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

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

HCM Solutions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HRO Solutions

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

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

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

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

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

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

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

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

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

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

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

Global Solutions

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

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

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

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

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

CONTROL ENVIRONMENT

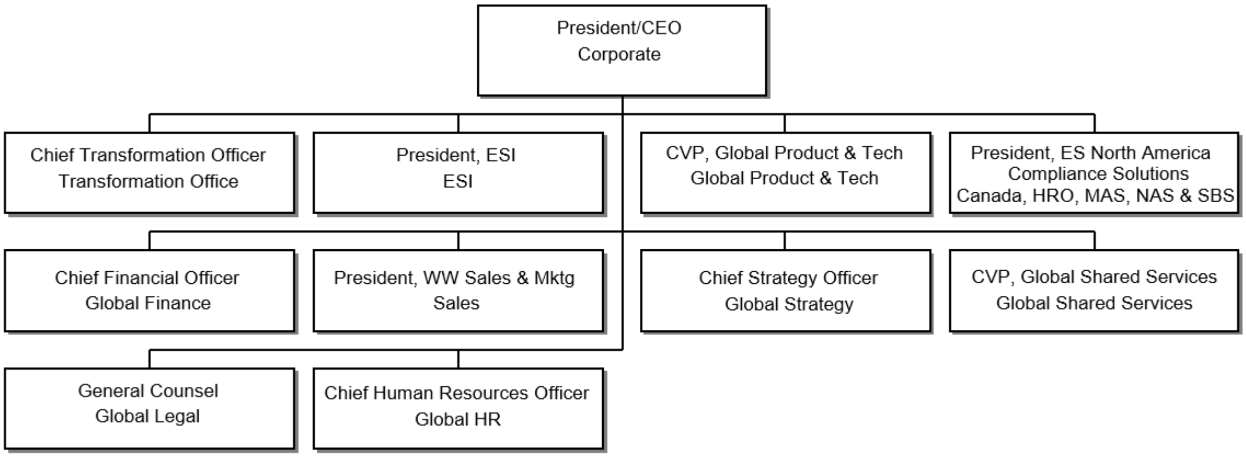
ADP’s control environment reflects the position taken by the management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. Management takes seriously defects identified in internal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

Oversight by ADP’s Board of Directors

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

Organizational Structure

Corporate Structure



Other ADP Corporate Supporting Groups

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

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

Human Resources Policies and Practices

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

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

- Employment
- Equal Employment Opportunity
- Code of Corporate Responsibility
- Ethical Standards
- Honesty and Fair Dealing
- Conflicts of Interest
- Disclosure, Use, and Copying of ADP and Third Party Software

- Harassment
- Substance Abuse
- Confidentiality of Information
- Electronic Communication Systems
- Corrective Actions

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

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

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

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

Corporate Internal Audit Function

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

RISK ASSESSMENT

Enterprise Risk Management Process

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

MONITORING

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

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

Client Satisfaction Monitoring

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

Internal Audit Monitoring

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

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

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

CONTROL ACTIVITIES

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

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

INFORMATION AND COMMUNICATION

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

Employees

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

Clients

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

CONTROL OBJECTIVES AND CONTROLS

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

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

Service Overview

The GETS US IT Services System comprises the data center hosting services and the technology infrastructure hardware and software managed services (e.g., operating systems (OS), databases (DBs), and supporting network devices physically located at the GETS US data centers in Georgia (Data Center 1) and in South Dakota (Data Center 2). The GETS US IT Services System also includes the Network Management Services provided by the GETS US organization comprised of network monitoring and network management/support.

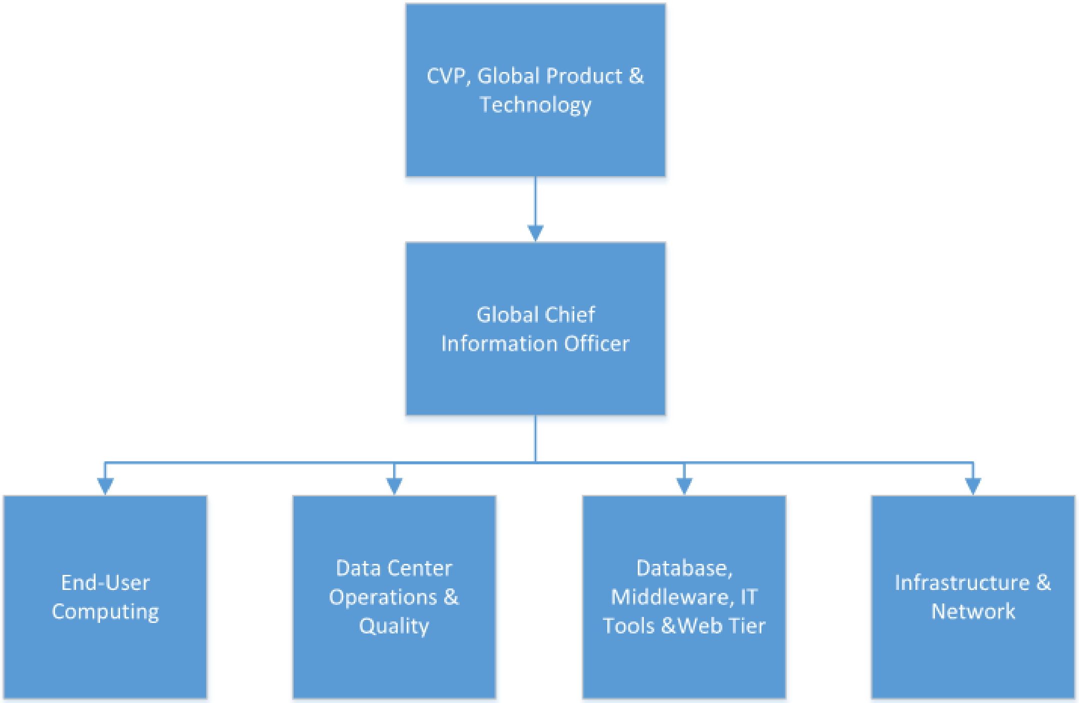
Key Organizational Support Structure

GETS US Organization

The GETS US organization is divided into two functional organizations to meet the technical needs of ADP's Global Employer Services International (GESI) and Multinational Corporations (MNC) international organization's business units:

- The Operations organization is responsible for supporting the business units' needs in terms of infrastructure and operations
- The Solution Engineering organization, responsible for designing, integrating and operating solutions that comply with ADP security and procurement policies
- Both organizations are led by the Global Chief Information Officer (CIO) of the GETS US organization who reports to ADP's Corporate Vice President (CVP) Global Product & Technology

Each organization is divided into functional teams that are centrally based at ADP's Corporate Headquarters as well as locally in each of the business units that are supported.


CVP, Global Product & Technology
Global Chief Information Officer
End-User Computing
Data Center Operations & Quality
Database, Middleware, IT Tools &Web Tier
Infrastructure & Network

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

- End-User Computing: These teams are responsible for end-user computing for any ADP associate (Service Desk, Laptop, Desktop Engineering, Access Management, and Messaging Services).
- Data Center Operation & Quality: This team is responsible for availability, Level 2 support, monitoring, incident management, and standard change management.
- Database, Middleware, IT Tools & Web tier + Infrastructure & Network: These teams are responsible for Level 3 support, availability, performance management, and for managing all changes, problems, and incidents.
- Infrastructure and Network: These teams are responsible for the security administration of the network at ADP's Corporate Headquarters in New Jersey, the data centers, and Regional Business Unit locations and supporting/managing the logical and remote access to ADP's WAN and Corporate Network (i.e., ESNet).

Additional GETS US Operations support:

- Mainframe & Midrange Tech and Apps Management – M&MTAM is responsible for the remote operational support of the Mainframe The M&MTAM organization consists of two groups:
  - M&MTAM – Command Center (CC): The Command Center is located in Illinois with a second Command Center located in Pune, India and both locations support production processing. The Command Centers' primary responsibility is supporting console operations. The Command Center staff is responsible for job execution, job monitoring, system monitoring, and workload balancing.

- M&MTAM – Technical Services: The M&MTAM Technical Services group is located throughout the U.S. and in Pune, India. This group's primary responsibilities include supporting the job scheduling, application change management support, management of mainframe logical access privileges, and problem management.

Changes to the Control Environment

The scope of this report has been expanded to include the backup and IT job scheduling controls for ADP's Mainframe production system managed by the GETS US organization. These controls were previously included in the respective ADP business units' reports, where relevant.

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 Global Enterprise Technology & Solutions (GETS) US organization (collectively referred to as the "GETS US IT Services System").

The GETS US IT Services System supports various other ADP business units whose services are covered by other SOC 1 reports produced by ADP. Refer to Figure 1 on the following page for a listing of other ADP ES services who issue SOC 1 reports that are supported by this Description.

<u>Figure 1</u>

ADP ES Services – SOC 1 Reports	OS Change Management	Network Logical Security & Monitoring	Logical Security (OS & DB)	Physical Security & Environmental Safeguards	System Backup	Operational Monitoring & Incident Management
	In-scope Processes – ADP's GETS US Organization					
AutoPay Payroll Services (US and Canada)	✓	✓	✓	✓	✓	✓
Retirement Services – Participant Record Keeping	✓	✓	✓	✓	✓	✓
Retirement Services – Executive Deferred Comp	✓	✓	✓	✓	✓	✓
Enterprise Benefits and Total Absence Management and Enterprise 2000	✓	✓	✓	✓	✓	✓
MAS ezLabor Manager	✓	✓	✓	✓	✓	✓
Managed Payroll Services (MPS)	✓	✓	✓	✓	✓	✓
Health and Welfare Benefits (Service Engine)	✓	✓	✓	✓	✓	✓
NAS & MAS Enterprise eTime	✓	✓	✓	✓	✓	✓
Carrier Enrollment Services (CES)		✓		✓		✓

ADP ES Services – SOC 1 Reports	OS Change Management	Network Logical Security & Monitoring	Logical Security (OS & DB)	Physical Security & Environmental Safeguards	System Backup	Operational Monitoring & Incident Management
	In-scope Processes – ADP's GETS US Organization					
TotalPay & PayCard, 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	✓	✓	✓			
Workforce Now (US and Canada) & Vantage	✓	✓	✓	✓	✓	✓
Benefits Marketplace	✓	✓	✓	✓	✓	✓
United Kingdom Payroll Managed Services and Payroll Processing (Freedom Application)	✓	✓	✓	✓	✓	✓

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 and Infrastructure Change Management
- Network Monitoring
- Information Security
- Logical Security
- Computer Operations and Data Backup
- Physical Security
- Environmental Safeguards
- Problem/Incident Management

OS and Infrastructure Change Management

The Distributed Systems group is responsible for identifying security updates for Windows and UNIX/Linux 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 monthly patching cycles for Internet facing servers (e.g., on ESNet and hosting web tier) and quarterly patching cycles for Intranet servers (e.g., application tier, DB tier). Change Orders are submitted to authorize the deployment of the patches. The automated patch deployment technology analyzes the servers and applies all 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 US hosting and data center facilities.

OS software, hardware, and infrastructure changes are requested by the GETS US teams and submitted to the Data Center Site Management group located at the GET US hosting and data center facilities using the CA Service Desk tool (Service Desk). Service Desk hardware and infrastructure change requests go through pre-determined 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 work flow steps leading up to implementation and receipt of required approvals, the Data Center Site Management group implements the changes based on the provided specifications.

The CAB consists of management representatives from various groups within the GETS US 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.

Network Monitoring

The ADP network is managed and controlled to protect information within systems and applications. The network architecture is segregated into segments and firewalls, network-based Intrusion Detection Systems (IDS), and Network Address Translation (NAT) devices are in place to monitor and restrict access to authorized network activity. Global Network Services, under the Data Networks group, is responsible for the configuration of the network. Network equipment, including firewalls, network-based IDS, and NAT are maintained and monitored by the Global Network Services group at the Network Command Center (NCC) in Elk Grove Village, Illinois. 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 the Trusted Platform Security Infrastructure (TPSI). TPSI globally integrates best of breed products to enable ADP to proactively monitor and identify potential security incident or exposure. TPSI captures 6 billion events daily (i.e., Twitter feeds, unusual network connections, IDS alerts, internally reported), which are analyzed, correlated, and reviewed by the Critical Incident Response Center (CIRC).

The CIRC utilizes the RSA Archer GRC tool, specifically the Archer Incident Management module, to track and report potential incidents that are created by the TPSI 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 of threats. Initial correlations of these incidents are performed by the various inputs into TPSI and the results are sent to Archer for investigation.

Information Security

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

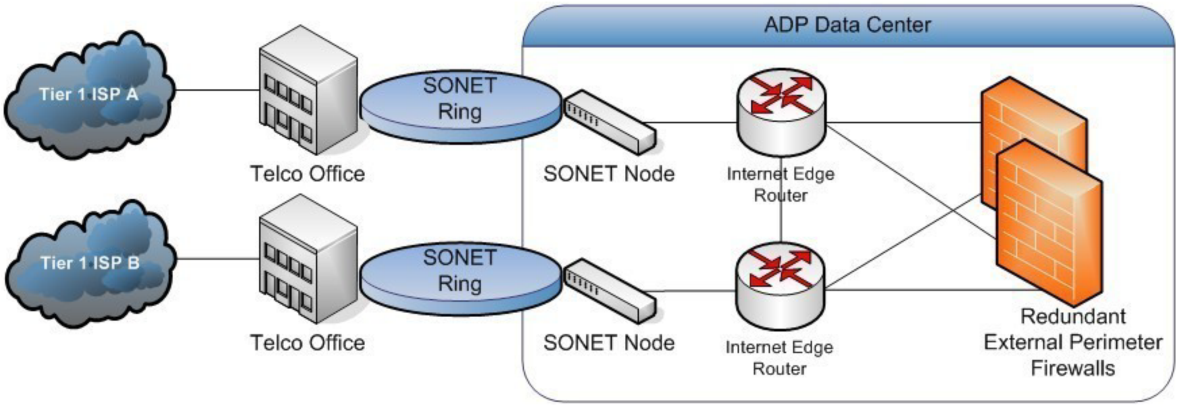
All Information Security Policies are on the ADP Intranet, which provides overall guidance for data security administration, use of third party software, virus protection, and internal/external user security. These guidelines provide a minimum-security baseline and apply to all ADP business units.

Logical Security

The GETS US 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 US 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 US organization’s common services provided to ADP’s US, 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 US-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, ADP uses an identity management system (IDM) that automates the process of managers granting and revoking network access privileges for their direct reports. The process for provisioning and de-provisioning network access is initiated by HR either through direct notification or the IDM system. The IDM system interfaces with AD to automatically create or disable the AD account. IDM does not extend to provisioning logical user access to other ADP systems/applications. Reconciliations of network access for terminated US associates is performed by the IT Compliance Group (US) and the Information Security Management Systems Group (US) using activity lists from HR and the current access in ESNet on a weekly basis and Lightweight Directory Access Protocol (LDAP) on a monthly basis to monitor compliance with policies.

The process for provisioning and de-provisioning ADP India associates' network access is initiated by HR. To obtain network access, a ticket is submitted to ATM. 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. Reconciliations of network access for terminated India associates is performed by the IT Compliance Group (US) and the Information Security Management Systems Group (US) using activity lists from HR and the current access in ESNet on a monthly basis.

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. Reconciliations of network access for terminated Philippines associates is performed by the IT Compliance Group (US) and the Information Security Management Systems Group (US) using activity lists from HR and the current access in ESNet on a monthly basis.

Operating System and Database Access

A process is in place to grant and revoke access to ADP employees at the OS and DB level. For new hires and transfers that require OS or DB access, management approval is required to grant access. For terminations, HR and/or authorized personnel submit a request to revoke OS or DB access. Distributed Database Systems' (DDS) access to the DB is managed at the OS level and grants them the ability to directly access the DB servers where they manage DB system accounts to perform standard DB services. The use of application DB accounts is managed by the individual applications. Depending upon circumstances, the employee's user account is revoked immediately or at the effective termination date. Only authorized personnel can submit a request to grant or revoke OS access which is then routed to the appropriate ADP group for processing.

The Access Control List (ACL) dashboard is an internally-developed application that is used to manage access privileges to the OS for servers and DBs hosted at the GETS US organization hosting operations and data center management facilities. Within the ACL dashboard, reports can be created listing each user's OS and DB logical access privileges.

The Logical Access Team (LAT), part of Client Product Support, is responsible for coordinating a monthly review of a selection of users' ACLs. The ACLs that are reviewed monthly are determined based on a predefined review schedule. GETS US personnel and product support business personnel are authorized access custodians and are responsible for verifying that access is appropriately restricted. The Logical Access Team initiates the review through the ACL Dashboard System by opening a Service Desk ticket. After reconciling the current access list to the corresponding ACL and resolving any identified discrepancies, the custodians approve the access privileges of the users listed on the ACL report to complete the review. Discrepancies identified are documented in a Desk ticket. The LAT tracks the review process through to completion and sends email notifications to the custodians who still have outstanding reviews after 15 days. All reviews must be completed within 30 days. Once the custodians have completed and approved their respective ACLs, the LAT closes the ticket.

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

The Privileged Identity Management (PIM) password vaulting utility is installed on servers hosted at the GETS US 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 log in 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.

Physical Security

Access to the GET US 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 US hosting and data center facilities are required to request access ahead of their visit. GETS US 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 US hosting and data center facilities. Access to the hosting and data center facilities is restricted to ADP’s associates and authorized permanent vendors. GETS US management approval is required to gain access to sensitive areas. Changes to physical access over the GETS US 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 US employees is revoked on or before the last day of employment based on notification from GETS US 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 US hosting and data center facilities. Discrepancies are followed up and resolved in a timely manner.

Environmental Safeguards

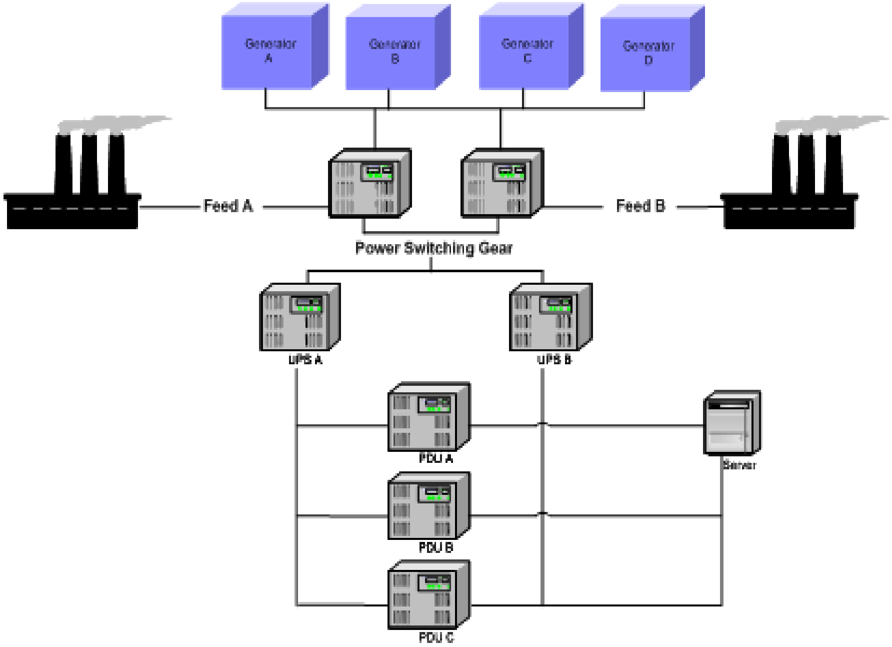
Equipment is installed for controlling environmental conditions in the computer rooms, telecommunications, and related technology equipment areas at each of the GETS US hosting and data center facilities. Enterprise Technology Operations and third party contractors test and maintain the fire suppression, 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 US 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 US 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.



Systems Backup

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

The Distributed System group's Storage Management team configures the automated backup schedules for open systems (e.g., Windows, UNIX, and Linux) 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. Data backups to virtual disk are performed in one data center and are copied to the other. 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.

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

Data Backup and Replication – Mainframe

IBM's virtual tape servers and physical tape drives located at ADP's GETS US 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 US 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 to a virtual tape in one data center is replicated to a virtual disk 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

Command Centers, Technical Support, and Service Desk organizations continuously monitor batch job streams, on-line 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 command center operators, technical support analysts, an engineering group, or to 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 command centers 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 US 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 Command Centers, network engineers, and mainframe engineers, the GETS US hosting and data center facilities personnel support the overall incident resolution and management process. In general, incidents requiring onsite attention to GETS US 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 US & 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 Monitoring – Windows and UNIX/Linux

The enterprise job scheduler system (e.g., AutoSys) is used to schedule and perform batch jobs related to the systems hosted at the GETS US organization hosting operations and data center management facilities. Access to the scheduler tool is limited to appropriate Client Product Support personnel. The Client Product Support team is responsible for monitoring jobs and creating cases to document that the file transfer completed successfully. Email status notifications are sent automatically to Client Product Support confirming the success/failure of each scheduled job. Daily reports are also generated for jobs processed. Any outstanding issues with job failures are investigated and the resolution is documented. Members of Client Product Support document major issues and errors in Service Desk. Only select members of Client Product Support staff have administrative (edit) rights to the job scheduler.

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 Command Centers are 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 Command Center 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 complementary user entity controls as the GETS US IT Services System provides direct support to other ADP business unit services as described in the *Scope of this Description* 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 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.01	*Policies* ADP has a formal Change Management Process that outlines the requirements for documenting and making system changes (OS software, hardware, and infrastructure).	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, and infrastructure changes.	No deviations noted
1.02	*Authorization* OS software, hardware, and infrastructure changes are formally authorized by management according to established procedures.	For a sample of OS software, hardware, and infrastructure changes deployed to the production environment, inspected the ticket to determine whether the changes were authorized by management according to established procedures.	No deviations noted
1.03	*Testing/Approval* OS software, hardware, and infrastructure 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, and infrastructure 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 prior to deployment.	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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.04	*Deployment to Production Environment* OS software, hardware, and infrastructure changes are deployed to the production environment by authorized personnel.	For a sample of OS software, hardware, and infrastructure changes deployed to the production environment, inspected the ticket to determine whether the change was deployed by authorized personnel. 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.	No deviations noted No deviations noted
1.05	*Emergency Changes* Emergency OS software, hardware, and infrastructure changes are approved by ADP management.	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.	No deviations noted

Network 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.01	*Architecture & Security* 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 observed real-time functioning of network devices to determine whether the ADP network is 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	*Problem Identification* 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.	No deviations noted
		For a sample of identified network issues, inspected the ticket to determine whether the issue and the corresponding resolution was documented.	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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.03	*Security Incident Monitoring* 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.	Observed personnel within ADP's Critical Incident Response Center on a sample day to determine whether they were actively identifying potential security incidents (i.e., monitoring Twitter feeds, unusual network connections, receiving internal calls) and capturing incidents within the GRC reporting tool.	No deviations noted
		Observed an 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 are 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.01	*Information Security Policy* 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	*Network User Authentication* Each user requires a valid user ID and password for network authentication through Active Directory.	Inquired of the network administrator and observed an ADP user log into the network to determine whether a valid user ID and password was required for successful authentication through Active Directory.	No deviations noted
3.03	*Network Password Policies* 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.04	*User Access Management* User account additions, modifications, and deletions require authorization from appropriate ADP management. Changes are documented and executed by an individual separate from the requestor according to policy and as requested.	For a sample of employee and contractor new hires (e.g., additions) inspected the documented network user access notification and current system user listings to determine whether the access was requested by appropriate ADP management and the access was granted as requested by an individual separate from the requestor.	No deviations noted
		For a sample of employee and contractor terminations (e.g., deletions), inspected the documented network user access notification, network user access listing, and in-scope production OS/DB access listings to determine whether access was revoked.	No deviations noted
		For a sample of OS/DB additions and modifications, inspected the ACL dashboard request, the corresponding ACL custodian list, and the system generated OS and DB user listings to determine whether the request was submitted by authorized personnel and access was granted as requested by an individual separate from the requestor.	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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.05	*Network, OS, and DB Administrative Access* Only appropriate users have been granted administrator privileges for ADP's network, operating system, and database environments.	For a sample of users with administrator access to ADP's network and in-scope operating system and database environments, inspected system generated user listings and inquired of ADP management to determine whether access appeared appropriate based on job responsibilities.	No deviations noted
3.06	*Network Access Review* ESNet and LDAP network user accounts belonging to terminated employees and contractors are reviewed weekly (US users on ESNet) and monthly (India and Philippines users on ESNet and LDAP users) by IT to confirm access has been appropriately removed.	For a sample of weeks and months, inspected the reconciliation documentation to determine whether a review of ESNet network accounts belonging to terminated employees/contractors was performed by IT and issues identified were documented and resolved.	No deviations noted
		For a sample of months, inspected the reconciliation documentation to determine whether a review of LDAP network accounts belonging to terminated employees/contractors was performed by IT and issues identified were documented and resolved.	No deviations noted
3.07	*OS/DB User Authentication* A valid LDAP or AD user ID and password are required for OS and DB authentication.	Observed an ADP associate log into a sample of Windows, UNIX, and Linux operating systems and SQL and Oracle databases to determine whether a valid LDAP or AD user ID and password was required for successful authentication.	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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.08	*OS/DB Password Policies* Password rules/restrictions are enforced at the server level through Active Directory or LDAP and are configured according ADP's security policies and standards.	Inspected the relevant Active Directory and LDAP password configuration settings governing access to the OS and DB production environments and ADP's password policies to determine whether password rules/restrictions including forced periodic password changes, password complexity, and password history were configured according to ADP's security policies and standards.	No deviations noted

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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.09	*OS/DB Access Review* The Logical Access Team reconciles the list of users with OS/DB and shared drive access to the Access Control Lists (ACL). In addition, the ACL Custodians review and approve the ACL based on a predetermined monthly schedule. Any issues are documented and resolved.	For a sample of months and ACLs, performed the following procedures: • Inspected the ticket and supporting review documentation to determine whether the ACLs were reviewed by the ACL Custodians based on the pre-defined schedule and issues identified were documented and resolved. • Inspected the ticket and supporting review documentation to determine whether the Logical Access Team reconciled the system-generated list of users with OS/DB and shared drive access to the ACL and issues identified were documented and resolved. • Re-performed the access review by inspecting the list of users with access in the ACL and corresponding system-generated list of users with OS/DB and shared drive access to determine whether access was granted to appropriate users based on job responsibilities and any issues were identified and resolved.	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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
3.10	*Administrator Access – PIM Password Vaulting Utility* 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

Physical Security

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.01	*Physical Access Mechanisms* 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, walked through and observed the facilities to determine whether: • 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	*Access Administration* 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 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.	No deviations noted
		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

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.03	*Access Privilege Review* 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 appropriateness of access based on users' job responsibilities and any identified discrepancies were documented and resolved.	No deviations noted
4.04	*Access to Badge System* 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
5.01	*Environmental Safeguards* The hosting and data center facilities are equipped with the following environmental safeguards: • A fire suppression system • A heating, ventilation, air conditioning (HVAC) system • UPS • Generators • Water sensors	For each of the in-scope hosting and data center facilities, walked through and observed the facilities to determine whether the following environmental safeguards were present: • A fire suppression system • HVAC system • UPS • Generators • Water sensors	No deviations noted
5.02	*Equipment Maintenance* Management and/or third parties regularly test and maintain environmental safeguards within the hosting and data center facilities.	For a sample of months and 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

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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
5.03	*Problem Management* 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Windows and UNIX/Linux			
6.01	*Data Mirroring* Data in one primary database server is mirrored to a secondary database server in an alternate data center.	For a sample of in scope databases, inspected the configuration management database to determine whether data in one primary database server was mirrored to a secondary database server in an alternate data center.	No deviations noted
6.02	*Scheduling* 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
6.03	*Monitoring and Problem Management* 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 were monitored and followed through to resolution.	No deviations noted
6.04	*Onsite Backup Storage* 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, walked through and observed the facilities to determine whether backups are 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Mainframe			
6.05	*Backup Scheduling* 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 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 to 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
6.06	*Monitoring and Problem Management* The M&MTAM Command Center group monitors the results of the backup procedures and is alerted by the application through an automatically generated ticket of any identified backup issues or exceptions. Issues, if any, are documented, reported, and followed up on to resolution.	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

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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
6.07	*Job Scheduler Access* Access to the backup control systems 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 to determine whether access to backup schedules is limited to authorized ADP associates based on inquiry with Operations personnel and assessment of job titles/responsibilities.	No deviations noted
6.08	*Offsite Backup Replication* Data backed up to a virtual tape in one data center is replicated to a virtual disk 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 to a virtual tape in one data center was scheduled to be replicated to virtual disk and stored at another data center. For a sample of LPARs and days, inspected the job log file 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Windows and UNIX/Linux			
7.01	*Operational Monitoring* Automated tools are in place to monitor system availability, performance, hardware issues, backup equipment, and other system-related issues.	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.	No deviations noted
		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.	No deviations noted
7.02	*Incident Management* 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.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
7.03	*Job Scheduling Monitoring* Client Product Support monitors the failure of jobs through automated status notifications and automatically generated tickets. Any issues are investigated, and the resolution is documented.	Observed Client Product Support personnel on a sample day monitoring failure of jobs in real-time to determine whether automated status notifications and tickets are generated upon job failure.	No deviations noted
		Inspected relevant online system settings to determine whether notifications are configured to automatically notify Client Product Support personnel upon job failure.	No deviations noted
		For a sample of days and job failures, inspected the incident ticket and job log to determine whether the job failure was investigated, and the resolution was documented.	No deviations noted
7.04	*Job Scheduler Access* Access to the job scheduler tool is limited to appropriate Client Product Support personnel.	Inspected the system listing of users with access to the job scheduler tool, inspected user job titles and inquired of ADP management regarding job responsibilities to determine whether access was limited to appropriate Client Product Support personnel.	No deviations noted

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Mainframe			
7.05	*Mainframe Job Scheduling Monitoring* M&MTAM personnel monitor the status of the scheduled jobs and are alerted of any identified processing issues or exceptions. Issues/exceptions are documented, reported, and followed up on to resolution.	Observed the M&MTAM Command Center personnel 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.	No deviations noted
		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.	No deviations noted
		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.	No deviations noted

SECTION FIVE

OTHER INFORMATION PROVIDED BY ADP

ADP GLOBAL BUSINESS RESILIENCY PROGRAM

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

Disaster Recovery Planning

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

Disaster Recovery plans have been developed to:

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

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

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

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

Business Continuity Planning

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

Business Continuity plans are:

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

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

Business Continuity plan components include but are not limited to:

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

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

GSO AND SECURITY OVERVIEW

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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