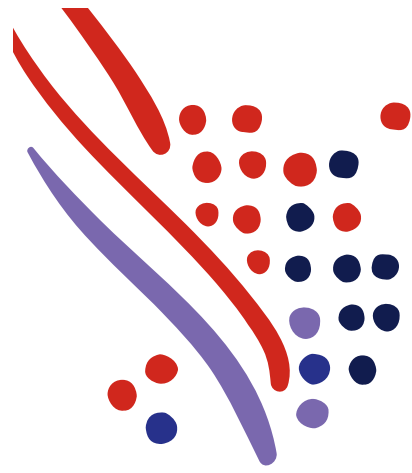




SOC 1® Report on the Suitability of the Design and Operating Effectiveness of Controls

Description of ADP's Netherlands Payroll Managed
Services and Payroll Processing Services System for
the period October 1, 2020 to September 30, 2021

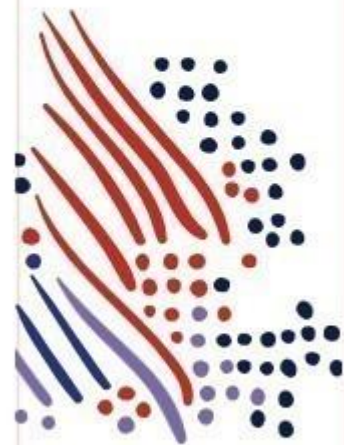
Table of Contents

SECTION ONE	PAGE
Independent Service Auditor's Assurance Report provided by Ernst & Young	
Independent Service Auditor's Assurance Report	4
SECTION TWO	
Management Assertion	
ADP Management Assertion	9
SECTION THREE	
Description of ADP's Netherlands Payroll Managed Services and Payroll Processing Services System for the period October 1, 2020 to September 30, 2021	
Overview of Operations.....	13
Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Control Activities, and Information and Communication	23
Control Objectives and Controls	28
Overview of the ADP's Netherlands Payroll Managed Services and Payroll Processing Services System	29
Scope of the Report	37
Transaction Processing	38
General Computer Controls	45
Subservice Organizations	48
Complementary User Entity Controls	53
SECTION FOUR	
Description of Control Objectives, Controls, Tests, and Results of Tests	
Testing Performed and Results of Tests of Entity-Level Controls.....	58
Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity	58
Transaction Processing Control Objectives and Controls.....	59
General Computer Control Objectives and Controls.....	69
SECTION FIVE	
Other Information Provided by ADP	
ADP Global Business Resiliency Program.....	77
GSO and Security Overview	78



SECTION ONE

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT PROVIDED BY ERNST & YOUNG



INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

Management of Automatic Data Processing, Inc.

Scope

We have examined Automatic Data Processing, Inc.'s (ADP) description entitled "Description of ADP's Netherlands Payroll Managed Services and Payroll Processing Services System" (Description) throughout the period October 1, 2020 to September 30, 2021 of its Payroll Managed Services and Payroll Processing Services System (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in ADP Management Assertion (Assertion). The Control Objectives and controls included in the Description are those that management of ADP believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

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

Carved-out Affiliated/Component Subservice Organization: The Payroll Managed Services (MS) and Payroll Processing Services (PS) system uses certain hosting services and technology infrastructure hardware and software managed services (e.g., databases, operating systems and network) provided by ADP's Global Enterprise Technology & Solutions (GETS) EMEA, a component of ADP. The Description includes only the Control Objectives and related controls of Payroll Managed Services (MS) and Payroll Processing Services (PS) system and excludes the control objectives and controls of ADP's GETS EMEA. The Description identifies the types of complementary controls of ADP's GETS EMEA that are necessary to achieve certain Control Objectives. The scope of this examination did not include the complementary controls of ADP's GETS EMEA.

Management of ADP's GETS EMEA has prepared a separate description of its system used by the System, which includes the aforementioned complementary ADP's GETS EMEA controls, and is presented in ADP's Global Enterprise Technology & Solutions (GETS) EMEA Organization Information Technology Services System for the period October 1, 2020 to September 30, 2021 (ADP's GETS EMEA SOC 1 report). This report should be read in conjunction with our report on the ADP's GETS EMEA SOC 1 report.

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

ADP's responsibilities

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

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Our examination was also performed in accordance with International Standard on Assurance Engagements 3402 *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period October 1, 2020 to September 30, 2021. 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.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements set forth in the *Preface:*

Applicable to All Members and Part 1 –Members in Public Practice of the Code of Professional Conduct established by the AICPA and applied the AICPA's *Statements on Quality Control Standards*.

Inherent limitations

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

Description of tests of controls

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

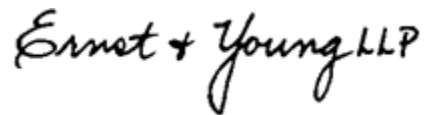
Opinion

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

- a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2020 to September 30, 2021.
- b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period October 1, 2020 to September 30, 2021 and if subservice organizations and user entities applied the complementary controls assumed in the design of ADP's controls throughout the period October 1, 2020 to September 30, 2021.
- c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2020 to September 30, 2021, if complementary subservice organization and user entity controls assumed in the design of ADP's controls operated effectively throughout the period October 1, 2020 to September 30, 2021.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of ADP, user entities of ADP's System during some or all of the period October 1, 2020 to September 30, 2021, 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.



December 16, 2021

SECTION TWO

MANAGEMENT ASSERTION



ADP MANAGEMENT ASSERTION

December 16, 2021

We have prepared the description of Automatic Data Processing, Inc.'s (ADP) Netherlands Payroll Managed Services and Payroll Processing Services System entitled, "Description of ADP's Description of ADP's Netherlands Payroll Managed Services and Payroll Processing Services System" (Description) for processing user entities' transactions throughout the period October 1, 2020 to September 30, 2021 for user entities of the system during some or all of the period October 1, 2020 to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Carved-out Affiliated/Component Subservice Organization: The Payroll Managed Services (MS) and Payroll Processing Services (PS) system uses certain hosting services and technology infrastructure hardware and software managed services (e.g., databases, operating systems and network) provided by ADP Global Enterprise Technology & Solutions (GETS) EMEA, a component of ADP. The Description includes only the Control Objectives and related controls of Payroll Managed Services (MS) and Payroll Processing Services (PS) system and excludes the control objectives and controls of ADP GETS EMEA. The Description identifies the types of complementary controls of ADP GETS EMEA that are necessary to achieve certain Control Objectives.

Management of ADP's GETS EMEA has prepared a separate description of its system used by System, which includes the aforementioned complementary ADP's GETS EMEA controls, and is presented in ADP's Global Enterprise Technology & Solutions (GETS) EMEA Organization Information Technology Services System for the period October 1, 2020 to September 30, 2021 (ADP's GETS EMEA SOC 1 report). This Description should be read in conjunction with the ADP's GETS EMEA SOC 1 report.

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

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

- a. The Description fairly presents ADP's Netherlands Payroll Managed Services and Payroll Processing Services System (System) made available to user entities of the System during some or all of the period October 1, 2020 to September 30, 2021 for processing their

transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

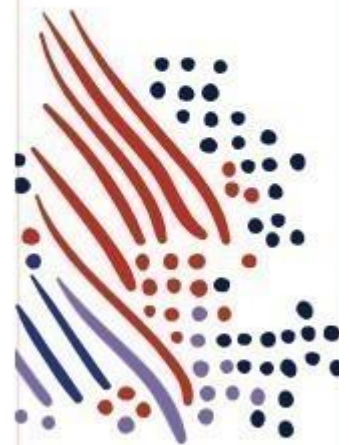
- (1) Presents how the System made available to user entities of the System was designed and implemented to process relevant transactions, including, if applicable:
 - The types of services provided, including, as appropriate, the classes of transactions processed.
 - The procedures, within both automated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

- (2) Includes relevant details of changes to the System during the period covered by the Description.
 - (3) Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.
- b.* The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2020 to September 30, 2021 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of ADP's controls throughout the period October 1, 2020 to September 30, 2021. 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 NETHERLANDS PAYROLL MANAGED SERVICES AND PAYROLL PROCESSING SERVICES SYSTEM FOR THE PERIOD OCTOBER 1, 2020 TO SEPTEMBER 30, 2021



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 920,000 clients in more than 140 countries and territories.



Business Overview

ADP's Mission

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



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 deliver global capabilities to dynamic, team-based organizations.



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

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

Business Segments

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

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

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

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



Products and Solutions

To serve the unique needs of diverse types of businesses and workforce models, ADP provides a range of solutions, which businesses of different types, sizes, and across geographies, can use to recruit, pay, manage, and retain their workforce. ADP addresses these broad market needs with its cloud-based strategic platforms: RUN Powered by ADP®, serving over 750,000 small businesses; ADP Workforce Now®, serving over 75,000 mid-sized and large businesses across ADP's strategic pillars; and ADP Vantage HCM®, serving over 500 large enterprise businesses. Each of these solutions can be combined with ADP SmartCompliance® to address the increasingly broad and complex needs of employers. Outside the United States, ADP addresses the needs of approximately 60,000 clients with premier global solutions consisting of local in-country solutions and multinational offerings, including ADP GlobalView®, ADP Celergo®, and ADP Streamline®.

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

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

ADP also launched Wisely Direct by ADP®, a network-branded general-purpose reloadable card and digital account, which provides similar features and functionality as Wisely Pay by ADP but is offered directly to consumers. ADP's digital card offerings are banking alternatives that feature services such as savings, budgeting, digital wallet, and other personal financial management features.

Also, ADP's mobile apps simplify how work gets done by helping to enable clients to process their payroll, and giving millions of their employees' convenient access to their payroll and HR information around the world and in 28 languages. ADP has also opened access for developers and system integrators to some of its platforms' application programming interface libraries through ADP Marketplace.

With ADP Marketplace, clients can integrate employee data from ADP's core services across their other business systems or platforms. This access enables the exchange of client data housed in ADP's databases and creates a unified HCM ecosystem for clients informed by a single, comprehensive repository of their workforce data. Clients can choose from over 445 apps and integrations, allowing them to choose solutions that are tailored to their needs, industry requirements, and preferences.



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

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



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 100,000 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. Also, industry-specific modules are available for labor forecasting, budgeting, activity and task management, grant and project tracking, and tips management.

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

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

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



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

- ADP SmartCompliance - In the United States, ADP SmartCompliance integrates client data delivered from its integrated HCM platforms or third-party payroll, HR, and financial systems into a single, cloud-based solution. ADP's specialized teams use the data to work with clients to help them manage changing and complex regulatory landscapes and improve business processes. ADP SmartCompliance includes HCM-related compliance solutions such as Employment Tax and Wage Payments, as well as Tax Credits, Health Compliance, Wage Garnishments, Employment Verifications, Unemployment Claims, and W-2 Management.
- ADP SmartCompliance Employment Tax - As part of its full-service employment tax services in the United States, ADP prepares and files employment tax returns on its clients' behalf and, in connection with these stand-alone services, collects employment taxes from clients and remits these taxes to more than 8,000 federal, state and local tax agencies. In its fiscal year ended June 30, 2021, in the United States, ADP processed and delivered approximately 69 million employee year-end tax statements, and moved more than \$2.3 trillion in client funds to taxing and other agencies and to its clients' employees and other payees.
- ADP SmartCompliance Wage Payments - In the United States, ADP offers compliant pay solutions for today's workforce, including electronic payroll disbursement options such as payroll cards, digital accounts, and direct deposit, as well as traditional payroll checks, which can be integrated with clients' ERP and payroll systems.

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 14,500 clients and approximately 620,000 worksite employees in the 50 U.S. states. ADP TotalSource is one of the largest PEOs certified by the Internal Revenue Service as meeting the requirements to operate as a Certified Professional Employer Organization under the Internal Revenue Code.

As a full-service PEO, ADP TotalSource provides complete HR management and core administrative services while the client continues to direct the day-to-day job-related duties of the employees. With constantly changing business regulations, global economies, and technology, ADP's clients benefit from partnering with ADP TotalSource to help them protect their business and drive growth and success. Some of the offerings available through ADP TotalSource to address today's workplace challenges include:

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

ADP Comprehensive Services - Leveraging its market-leading ADP Workforce Now platform, ADP Comprehensive Services partners with clients of different types and sizes to tackle their HR, talent, benefits administration, and pay challenges with help from ADP's expertise, experience, and best practices. ADP Comprehensive Services is flexible – helping to enable clients to partner with ADP for managed services for one,



some, or all areas across HR, talent, benefits administration and pay. ADP provides outsourced execution that combines processes, technology, and a service and support team that acts as an extension of its client's in-house resources - so their HCM and pay operations are executed with confidence.

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

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

Global Solutions

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

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

ADP also offers comprehensive, country-specific HCM solutions that combine innovative technology with deep local expertise. By operating a flexible service model, we help customers manage various combinations of payroll services, HR management, time and attendance management, talent management and benefits management, depending on the country in which the solution is provided.

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



ADP pays over 14 million workers outside the United States with its in-country solutions and with ADP GlobalView, ADP Celergo/Streamline, and ADP iHCM – ADP’s simplified and intuitive multi-country payroll solutions. As part of its global payroll services, ADP supplies year-end regulatory and legislative tax statements and other forms to its clients’ employees. ADP’s global talent management solutions elevate the employee experience, from recruitment to ongoing employee engagement and development. ADP’s comprehensive HR solutions combined with deep expertise make its clients’ global HR management strategies a reality. ADP’s configurable, automated time and attendance tools help global clients understand the work being performed and the resources being used, and help ensure the right people are in the right place at the right time.



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

CONTROL ENVIRONMENT

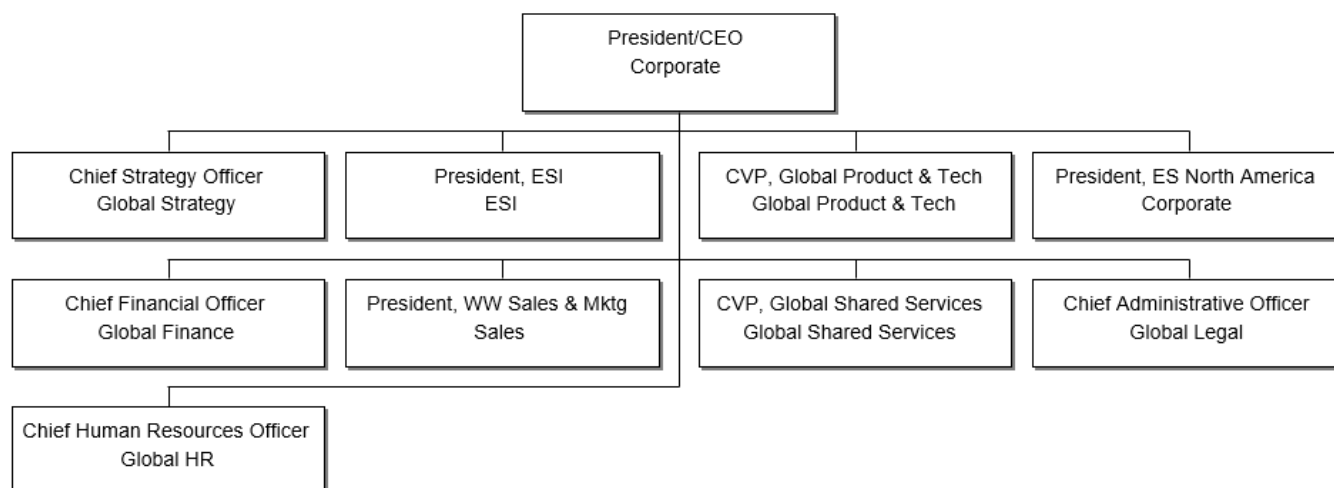
ADP's control environment reflects the position taken by the management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. Management takes seriously defects identified in internal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

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

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



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

ADP's core values are posted on ADP's Corporate Intranet and include Integrity is Everything, Service Excellence, Inspiring Innovation, Each Person Counts, Results-Driven, and Social Responsibility. In-depth explanations of these values are available to 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 assist employees in becoming acclimated to ADP's business philosophy. The orientation activities assist new associates in understanding ADP's overall mission and core values, departmental operation practices, and individual performance objectives.

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

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

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



Corporate Internal Audit Function

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

RISK ASSESSMENT

Enterprise Risk Management Process

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

MONITORING

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

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



Client Satisfaction Monitoring

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

Internal Audit Monitoring

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

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

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

CONTROL ACTIVITIES

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

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

INFORMATION AND COMMUNICATION

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



Employees

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

Clients

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

CONTROL OBJECTIVES AND CONTROLS

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



OVERVIEW OF THE ADP'S NETHERLANDS PAYROLL MANAGED SERVICES AND PAYROLL PROCESSING SERVICES SYSTEM

Service Overview

ADP Employer Services Netherlands B.V. (“ADP ESI NL”), an Employer Services International (ESI) business unit, offers flexible and scalable services and payroll software solutions. ADP ESI NL, as a leading provider of outsourced business solutions, assists the employers of 1.4 million Dutch workers to increase productivity, ensure regulatory compliance, improve employee retention, and control costs. ADP ESI NL’s offerings include traditional, web-based comprehensive outsourcing products and services through its Payroll Services. These services include payroll, HR management, and comprehensive outsourcing, and consulting services.

ADP ESI NL provides its services from offices located in Capelle aan den IJssel and Amsterdam, the Netherlands.

ADP ESI NL offers the following two services to its clients:

- Payroll Processing Services (PS) - A software-as-a-service (SaaS) front-end solution service model that is delivered to clients to keep their personnel and HR administration data current. The client is responsible for providing, to ADP, changes that affect payroll processing. Upon receipt of the changes, ADP processes them in conjunction with the payroll data that they already hold. The output is generated for the client payroll professionals and pay slips are generated for individual employees. Pay slips are provided in digital format. As part of its services, ADP also keeps the calculation rules current and in compliance with changes in the laws or in the client’s collective labor agreement. In this service model, the client is responsible for timely and accurate payroll processing. The client must have qualified payroll experts in its own organization to perform the process correctly.
- Payroll Managed Services (MS) - A service model in which ADP processes the client’s payroll. ADP makes advance agreements with its clients about the manner in which changes are to be received. Once received, ADP enters the data, checks the input, processes the data, and checks the output. Responsibility and liability for the administration and the final results rest with ADP. Depending on the choices made by the client, various methods to provide ADP with payroll data can be used (e.g., changes using the ADP SaaS front-end or input data that was provided using ADP’s standard input method). The Managed Services model requires that the client have only a minimum payroll processing knowledge.

IT Applications and Supporting Infrastructure

ADP ESI NL provides its Payroll Managed Services and Payroll Processing Services offerings using the following solutions and in-scope systems.



In-Scope Systems

A number of computerized systems are used to support ADP ESI NL's Payroll Managed Services and Payroll Processing Services. The following table describes the in-scope systems and includes the technology and a brief description overview:

Applicable Payroll Solution	Application Front-End	Description	Market Target	Application Front-End Technology	Application Back-End
Payroll Managed Services and Payroll Processing Services	ADP Perman	ADP Perman, developed by ADP, is a web application, used to input data into Multipay. ADP Perman is designed modularly. After employee data changes are recorded in ADP Perman, ADP processes the payroll. ADP Perman's infrastructure is managed by and hosted at the ADP Global Enterprise Technology & Solutions (GETS) EMEA organization in Pantin, France by Equinix.	Small Mid-sized Large	Windows Server, Oracle RDBMS	Multipay
	ADP Workforce	ADP Workforce, developed by ADP, is an integrated web solution used to input data into Multipay and Prisal. ADP Workforce offers standard business intelligence and can be adapted to specific operating conditions, requirements, and wishes. ADP's Workforce infrastructure resides at the client's side or at the ADP GETS EMEA organization in Pantin, France by Equinix.	Mid-sized Large Government Care	Windows Server, Oracle RDBMS	Multipay, Prisal



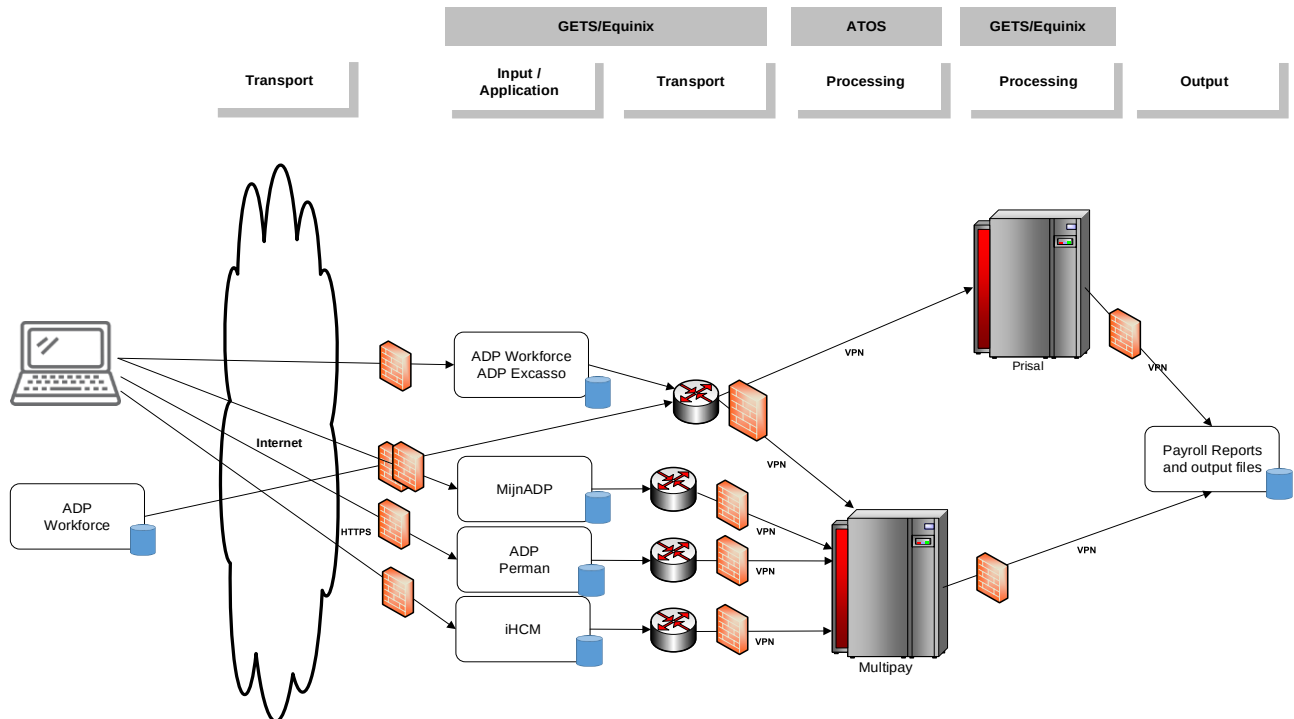
Applicable Payroll Solution	Application Front-End	Description	Market Target	Application Front-End Technology	Application Back-End
	ADP Excasso	ADP Excasso is an ADP Workforce variant for the life insurance and pension markets.	Life Insurance/Pensions	Windows Server, Oracle RDBMS	Multipay, Prisal
	iHCM	Native-Web platform developed by ADP used to input data into Multipay. iHCM infrastructure resides at the ADP GETS EMEA organization in Pantin, France by Equinix.	Small Mid-sized Large	Windows Server, MS SQL	Multipay
	MijnADP	MijnADP gives very limited access to some constants in Multipay used in the payroll processing of clients. It's a web-based application used by clients mainly at the end of every year to prepare their payroll for the processing of the next payroll year. MijnADP infrastructure resides at the ADP GETS EMEA organization in Pantin, France by Equinix. MijnADP application does not process any payroll data (only Multipay does). MijnADP is used to access payroll tables only (control 2.01).	Small Mid-sized Large	Windows Server, Oracle RDBMS	Multipay



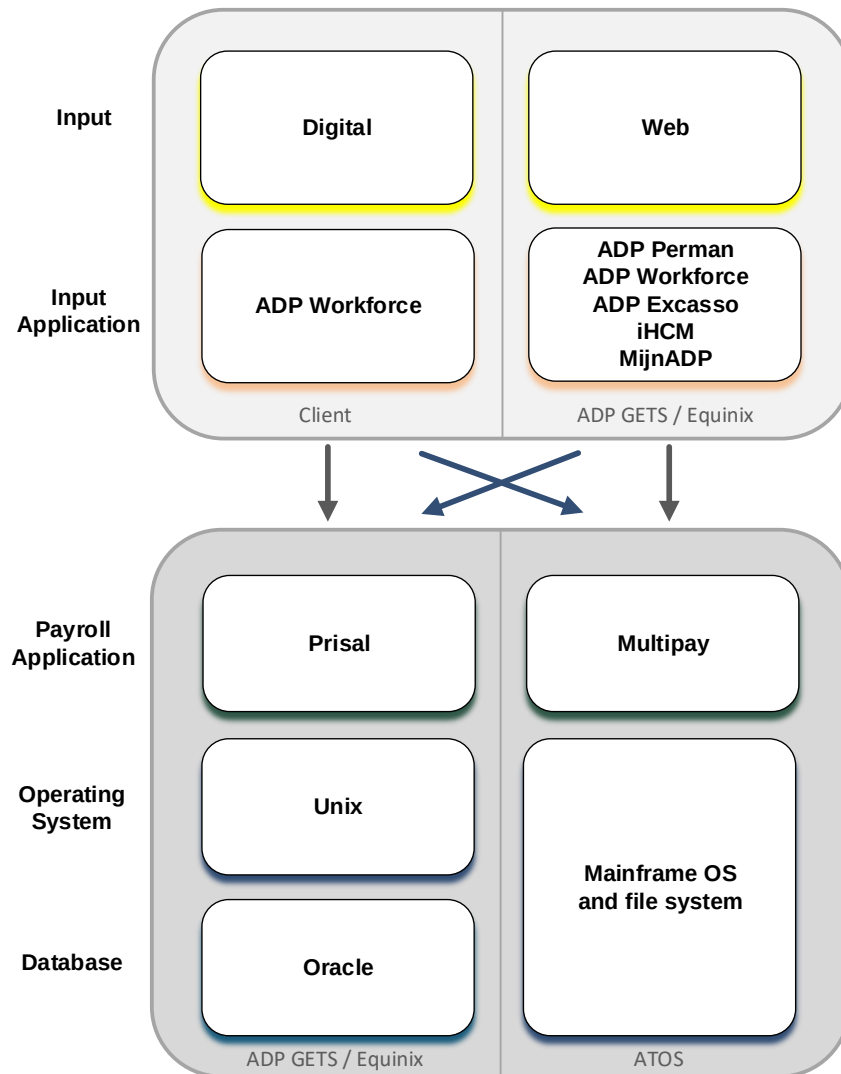
Application Back-End Systems

Application Name	Description	Application Technology
Multipay	Multipay, developed by ADP, calculates payroll data and generates the corresponding output including client-employees' pay slips. Changes in laws and regulations are applied directly to Multipay. Multipay uses client data that resides on the mainframe. The Multipay infrastructure is managed by the ADP GETS EMEA organization and located at Atos in Frankfurt, Germany.	Mainframe
Prisal	Prisal, developed by ADP, calculates payroll data and generates the corresponding output including client-employee pay slips for "Overheid, Non-profit en de Zorg" (ONZ), which means "Government, Non-profit and Healthcare". Changes in laws and regulations are applied directly in Prisal. Prisal infrastructure is managed by the ADP GETS EMEA organization and is hosted by Equinix located in Pantin, France.	UNIX, Oracle RDBMS

Processing layer



Hosting overview



ADP Perman, ADP Workforce, ADP Excasso and iHCM (ADP GETS EMEA organization hosted)

Clients connect to ADP ESI NL from their networks through the Internet and can logon to the front-end applications using a username and a matching password. ADP associates supporting Payroll Managed Services and Payroll Processing Services clients use the same front-end applications.

ADP Workforce (client-hosted version)

Clients can use a client-hosted version of ADP Workforce.



Transpay (file transfer to Multipay)

Transpay is a file transfer functionality embedded within the MijnpADP application. Transpay is used to securely transfer the data which is input into the front-end systems by the clients or by the ADP associates to Multipay application.

The front-end systems working with Transpay to transfer data to Multipay are the following:

- ADP Perman, ADP Workforce, ADP Excasso and iHCM (ADP GETS EMEA organization hosted)
- ADP Workforce (client-hosted version)
- Client's HR dedicated system

Transpay (file transfer to ADP ESI NL/Upload Data Sheets) – for Payroll Managed Services clients only

Transpay can also be used by the Payroll Managed Services clients to securely transfer payroll data in an ADP-predetermined format (Excel spreadsheets) to ADP ESI NL. Clients connect to the MijnpADP application and upload the Excel files into Transpay for the ADP payroll specialist to receive and process.

Key Organizational Support Structure

To effectively deliver both Payroll Managed Services and Payroll Processing Services to its payroll clients, ADP ESI is organized into local business units (BUs) e.g., France, Germany, United Kingdom, Italy, and the Netherlands.

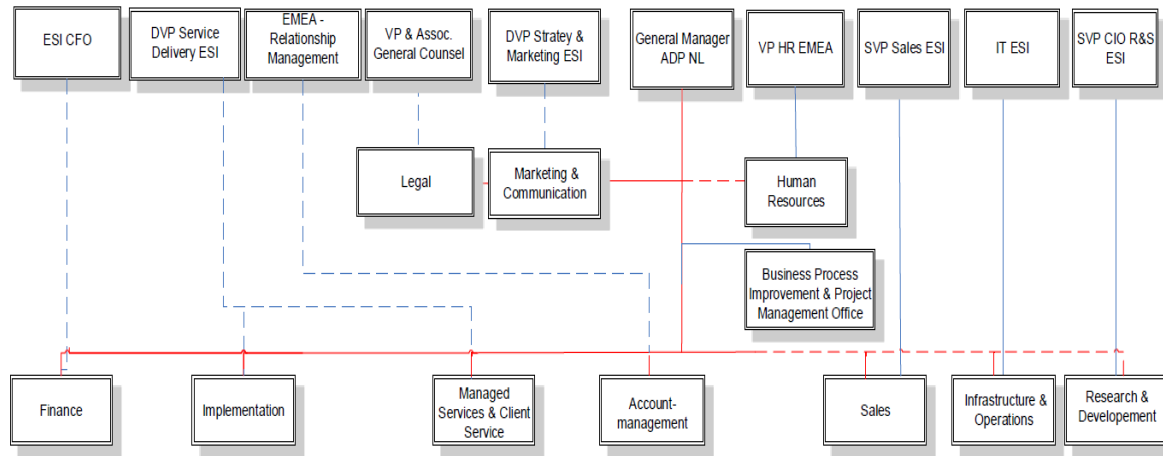
Each BU has local management that is responsible for providing its payroll services. The ADP ESI NL business management is responsible for handling core business processes and operations related to the systems described in the Overview of Operations section. Information Technology services for most BUs, including ADP ESI NL, are handled at the ADP GETS EMEA organization.

ADP ESI NL is part of the Global ES International organization's European region. A Managing Director heads ADP ESI NL and a Director Committee governs its overall strategy. ADP ESI NL Board of Directors meets regularly during the year. The activities of the local Boards are complementary to those of ADP's main Board of Directors. At these meetings, the local Board reviews:

- Local financial results
- Strategy
- Legal matters
- Risk management

A General Manager heads ADP ESI NL and a Senior Management Team governs its overall operations. The Senior Management Team consists of the Marketing & Communication, Sales, Infrastructure & Operations, Product Development, Quality & Process Improvement Implementation & Projects, Managed Services & Client Service, and Account Management department managers.





The following seven (7) departments are responsible for providing clients both Payroll Managed Services and Payroll Processing Services:

Research and Development (R&D) is responsible for:

- Product management, including the strategic and tactical management of product lines and service offerings and for ensuring that the client products are positioned properly in the market, meet the current and future needs of existing and prospective clients, and support the overall strategic product direction.
- Product development of hosted payroll & HR systems, web (payroll & HR) input, and reporting systems. Specific activities include analysis, design, programming, testing, and maintenance.

Implementation is responsible for:

- Implementing ADP ESI NL's payroll products and services, or merging existing payrolls once the client is live, and migrating payrolls from one service to another.

Infrastructure & Operations (ADP GETS EMEA) organization is responsible for:

- Service Assurance – providing payroll application services and support to ADP associates e.g., internet, hosting, and PCs as well as supporting ADP's main payroll engines and other business systems. This team also produces product-related client communications.
- Technical Services – maintaining and supporting critical data processing systems, voice, and data communications, Information Security Services, and technical IT service management.
- Information Security – locally implementing and managing relevant security tools and applications.
- Payroll Production Department – managing the actual payroll processing.



Managed Services & Client Service is responsible for:

- Client payroll configuration product and technical support.
- Payroll Managed Services payroll processing support including verifying and correcting payroll-engine processed data, and correcting client-input scheduling errors, and properly processing client input.

Account Management is responsible for:

- Assisting clients with strategic and tactical issues and monitoring contractual obligations.

The Sales group is responsible for:

- Generating leads and driving activities for new sales and sales to the base.
- Developing new clients and delivering new client contracts.

Finance is responsible for:

- Facilities (part of the Finance team) are responsible for formulating and executing the facilities strategy and for daily maintenance including the physical security of ADP's offices.
- Accounting & Reporting includes:
 - External Financial Reporting
 - SOX Controls
 - Accounts Payable
 - Credit Control
- Sales/Revenue Control ensure that ADP's clients are billed accurately.
- Financial Planning prepares management reports and forecasts.

Changes to the Control Environment

The "Calculating Payroll and Output" section of the control framework was split into two separate sections for "Calculating Payroll" and "Payroll Output". Control 3.01 "Payroll Reports" was moved under the "Payroll Output" section of the control framework with number 4.01. Control 4.02 "Tax Declarations" and control 4.03 "Journal Entry Files" were added under the "Payroll Output" section and were implemented since October 1, 2020.

Effective April 1, 2021, the User Access Review and Recertification controls (control number 6.03 & control number 6.04) for the local domain NL.EHC.ADP.COM have been shifted from the ADP NL to ADP GETS EMEA and are now in the scope of the ADP GETS EMEA SOC 1 report.

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



SCOPE OF THE REPORT

This description was prepared in accordance with the criteria set forth for a SOC 1® Type 2 Report in the ADP Management Assertion and the guidance for a description of a service organization's system set forth in the AICPA Attestation Standards AT-C section 320 as clarified and recodified by Statement on Standards for Attestation Engagements (SSAE) No. 18 *Attestation Standards: Clarification and Recodification* and the International Auditing and Assurance Standards Board (IAASB)'s International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*.

This report covers ADP ESI NL Payroll Processing Services (PS) and Payroll Managed Services (MS) including clients contracted through the Streamline service. ADP Streamline® offers Payroll Managed Services (MS) designed for small and medium-size entities of multi-national companies worldwide. The Streamline service is composed of:

- Central Services provided by ADP Streamline Central Services
- Local Services provided in each individual local country by ADP partners on behalf of ADP Streamline (e.g., ADP ESI NL)

The description of the delivery of central services is described in the ADP Streamline SOC 1 Type 2 report. The description of the delivery of local services for Streamline clients in the Netherlands provided by ADP Streamline Partner (e.g., ADP ESI NL) is described in this report.

The scope of the report covers the business processes that ADP determined are significant to its clients from a financial reporting perspective and the applicable information technology processes specific to supporting the services noted above.



TRANSACTION PROCESSING

Overview of Key Transaction Processing/Services

The Payroll Managed Services and Payroll Processing Services include the following business processes to support service delivery:

- Payroll Input
- Payroll Processing
- Payroll Output

Payroll Input (Payroll Processing Services and Payroll Managed Services Clients)

Data Input for Payroll Processing Services Clients

Payroll data can be input through the following means:

- Front-end applications (ADP GETS EMEA organization hosted) – ADP Perman, ADP Workforce, ADP Excasso, and iHCM are web-based front-end applications that enable clients to enter, change, and delete payroll master file data. Data changes are automatically updated into Multipay or Prisal. Clients are responsible for ensuring that the data entered into ADP Perman, ADP Workforce, ADP Excasso, or iHCM is accurate, complete, and valid.
- Front-end applications (non-ADP GETS EMEA organization hosted/client-hosted) – The client-hosted version of ADP Workforce is a non-ADP GETS EMEA hosted front-end application that enables clients to enter, change, and delete payroll master file data. Data changes are automatically updated into Multipay or Prisal. Clients are responsible for ensuring that data entered is accurate, complete, and valid.
- Client's HR dedicated systems – The client can enter, change, and delete payroll master file data from its own HR system. Data changes are automatically updated into Multipay. Clients are responsible for ensuring that data entered is accurate, complete, and valid.



Payroll Data Input for Payroll Managed Services Clients

Clients can provide payroll data to ADP through the following means:

- Upload Data Sheets – Excel spreadsheets are uploaded in an ADP-predetermined format. The upload data sheets are received via Transpay. A confirmation log is created that contains the number of records uploaded and potential process rejections. A checklist is created during each step of the upload process to ensure accuracy. The appropriate payroll specialist liaises with the client about correcting errors or rejections if needed. The client is responsible for ensuring that the payroll data provided to ADP is accurate and valid.
- Front-end applications (ADP GETS EMEA organization hosted) – ADP Perman, ADP Workforce, ADP Excasso and iHCM are web-based, front-end applications that enable clients to provide ADP with payroll data. Clients are responsible for ensuring that the data entered into ADP Perman, ADP Workforce, ADP Excasso or iHCM is accurate, complete, and valid. The payroll specialist checks the input for legal notice compliance and accuracy.
- ADP StreamOnline Payroll Management (SPM) – ADP StreamOnline Payroll Management is based on the SPM, a secure web-based tool under ADP Streamline's supervision, which provides a single channel of communication between ADP ESI NL and clients contracted through ADP Streamline. SPM can be used by clients to upload Excel files with changes. Payroll Managed Services imports these files into the standard front-end systems (Perman or iHCM) to start processing.

For Payroll Managed Services clients, some back-office activities are performed at ADP supervised locations; ADP ESI NL is responsible for the back-office employee activities. At the ADP-supervised back-office locations, employee activities are validated by a second back-office associate. Control reports of these activities are reviewed for accuracy, completeness and validity by payroll specialists from offices located in Capelle aan den IJssel and Amsterdam. These payroll specialists also check for legal notice compliance and accuracy.

Types of Payroll Data Input

Hiring Personnel – When clients hire new employees, they must enter their new hire's personnel, along with other relevant data, into the master file. These entries are traced and agreed to the source document to ensure that all payroll data is accurate and valid. All entries are logged for documentation and audit purposes.

Payroll Data Changes – When clients have payroll data changes for existing employees, they must enter them into the master file. These entries are traced and agreed to the source document to ensure that all payroll data is accurate and valid. All entries are logged for documentation and audit purposes.



Terminating Personnel – To remove terminated-employee access, clients must provide an authorized source document stating the employee's termination date and special arrangements, if any. ADP generates the final pay slip and reviews the payroll data to ensure it is accurate, complete, valid, and compliant with legal requirements.

Maintain Payroll Master Files

Data additions, changes, or deletions are traced to authorized client contact and agreed to authorized and approved source documents to confirm accuracy, completeness, and compliance with client requirements.

Recorded changes are compared to authorized source documents and reviewed with automatically generated reports and verified with client policies and procedures if applicable. A checklist is used by the payroll specialist or back-office associate to ensure the completeness of the request before processing.

Recorded changes to the payroll master files are checked by the payroll specialist or back-office associate for compliance with client-employee policies and procedures including compliance with statutory regulation and union requirements, by the payroll reports and checklists, if applicable.

Recorded changes to the payroll master files input by a back-office associate are validated by a second back-office associate to verify their accuracy and completeness. Identified errors are corrected promptly.

The activities performed by ADP supervised locations are reviewed, (on the basis of payroll reports and checklists) by the front-office employee (ADP ESI NL) to ensure changes to the payroll master files, provided to the ADP supervised locations, are processed completely and initiate corrective actions if needed.

The payroll master file changes are reviewed monthly by a payroll specialist for accuracy and completeness based on automatically generated change reports and source documentation.

The ability to view, modify, or transfer payroll master file information is restricted to authorized ADP personnel.

For clients contracted through ADP Streamline, monthly payroll data and related payroll instructions can be submitted through the ADP StreamOnline Payroll Management (SPM) system.

Clients have the ability via this platform to send e-mails and utilize specific payroll production control folders to upload input data sheets, add comments, and retrieve system reports (i.e., payroll reports and data output files).



Maintain Payroll Tables and Rules

Payroll Tables

Payroll tables contain parameters resulting from legal rulings (Government), collective labor agreements (Unions) or customer rulings (Customer) that have an impact on the payroll calculations.

Changes to payroll tables are based on reference data from Government, Unions or Customer and are registered in Rally or JIRA (change request management system) by the product owner/scrumb master. Making changes to the payroll table is restricted to authorized personnel (developers), approved by management (product owner/scrumb master), and reviewed by management (product owner). Payroll table changes are verified to source documents by the product owner and are imported into the payroll engines. As part of the payroll table change process, the accuracy and relevance of payroll table changes are formally reviewed for compliance with statutory requirements. Therefore, the changes are verified to source documents of the rulings (Government, Unions or Customer).

Payroll Rules

The Application Development and Change Management process is followed for changes to the payroll rules. Refer to the “General Computer Controls” paragraph within this section for details on the controls currently in place.

Compliance with Statutory Requirements

The Legal Watch Team monitors legal and regulatory requirement changes by maintaining regular, close contact with regulatory authorities. In the case of changes needed to payroll tables or rules (i.e., social deductions tax, representation allowances, legal reports, etc.), the change management process as described above is applied.

The changes are reviewed before implementation by the Legal Watch Team to verify compliance with statutory requirements. The Legal Watch Team signs off on the release reports to document that the changes were reviewed for compliance with the statutory requirements and approved.

Payroll Processing (Payroll Processing Services and Payroll Managed Services Clients)

Simulation

A Payroll Simulation, performed to start a payroll process, produces a simulation log and payslips. This is a test run and does not update the Results Tables. The Payroll Specialist reviews the clients’ payroll logs and payslips for errors. Inaccurate payslips are corrected. The payroll specialist signs off on the corrections.



Payroll Run

Payroll Processing Services: The client performs a ‘start payroll’ that creates employee results in that specific payroll.

Payroll Managed Services: The Payroll Specialist performs a ‘start payroll’ for Payroll Managed Services clients and it creates employee results for all employees in that particular payroll. This enables the Payroll Specialist to produce a number of key reports including the Wage Type Statement, Payroll Register, Bank Summary, EFT file, and the payslips. The Payroll Specialist also checks the log statistics to ensure that the number of payslips match the number of employees in the pay run.

As part of the ‘start payroll’ process, clients can perform the following reconciliations:

- The wage bank transfer matches the net pay.
- The net pay total in the Payroll Register spreadsheet matches the net pay total in the Wage Type Statement Report and the Bank Summary Report. All three must agree.
- The value date in the payment file matches the payroll schedule as agreed with the client (for Payroll Managed Services Clients only).
- The Control Spreadsheet headcount matches the successfully processed employees in the Payroll Log, and that the number of terminations and new hires in the Control Spreadsheet matches the Starters & Leavers Report.

For Streamline clients, the ADP StreamOnline Payroll Management (SPM) platform is used to log the completion of all payroll milestones. ADP ESI NL will upload a ‘return’ file once payroll has been approved by the client. ADP ESI NL relies on these platforms to validate with the client that all payroll data is accurate, complete, timely, and valid before the delivery of payroll outputs.

Payroll Output (Payroll Processing Services and Payroll Managed Services Clients)

Payroll Reports

Payroll calculation reports are automatically generated by running the payroll calculation process.

Tax Declarations (Payroll Managed Services Clients)

The payroll expert verifies the timely production of the Wage Tax Declarations for the Tax Authorities.



Journal Entry Files (Payroll Managed Services Clients)

The payroll expert verifies the timely production of the Journal Entry Files for the client. The payroll expert verifies that the generated Payroll Journal Entry Files are identical to the approved Payroll Journal Entry Files generated in the pre-check run.

Standard Reports

The in-scope payroll applications produce standard reports as part of each payroll run. These reports are made available to clients via Multidocuments, Voorcheck Web, or as hardcopy documentation.

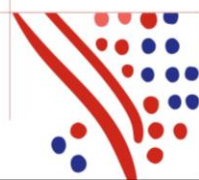
For Streamline clients, payroll files and reports are made available on the ADP StreamOnline Payroll Management (SPM) platform.

The following table presents a list of the most common reports used by clients that could impact their financial statement accounts.

Report Name(s)	Description	Source and Preparation
Actueel salarisoverzicht	This report displays all monthly/4-weekly payments, deductions, and net result.	Multipay in the monthly final payroll run
Borderel loonaangifte	This report displays the amount to be paid to the Inland Revenue Service (De Belastingdienst).	Multipay in the monthly final payroll run
Periodieke en cumulatieve loonlijst	This report specifies the salary costs and social taxes for the clients' departments.	Multipay in the monthly final payroll run
Complete journaalposten	This report shows the debtor's and creditor's postings.	Multipay in the monthly final payroll run
Premielonen SV & Fiscus	This report identifies the employers' and employees' national insurance contributions.	Multipay in the monthly final payroll run
Borderel Betalings- en annuleringsopdracht en kasbetalingen	This report displays the amounts that are to be paid to the employees, health insurance carriers, pension companies, or both.	Multipay in the monthly final payroll run
Overzicht betalingen	This report displays the periodic calculations and the payroll's total amount broken out by employee.	Prisal in the monthly final payroll run
Overzicht Loonaangifte t.b.v. Belastingdienst	This report displays the amount to be paid to the Inland Revenue Service (De Belastingdienst).	Prisal in the monthly final payroll run
Overzicht Journaalposten	This report shows the debtor's and creditor's postings.	Prisal in the monthly final payroll run
Overzicht afdracht premies en loonbelasting totaal	This report displays the employers' and employees' national insurance contributions.	Prisal in the monthly final payroll run



Report Name(s)	Description	Source and Preparation
Overzicht Betalingen	This report displays the amount to be paid to each employee.	Prisal in the monthly payroll run
Verslag IZA/IZR/ZKA/ ABP verwerking	This report displays the amounts to be paid to the health insurance carriers.	Prisal in the monthly final payroll run



GENERAL COMPUTER CONTROLS

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

- Information Security
- Application Change Management
- Logical Security
- Payroll Job Management

Information Security

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

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

Application Change Management

ADP has implemented procedures for maintaining payroll applications. Program changes must be accepted and formally released by product owners or management. Formal acceptance by product owners or management includes verification that changes are properly tested and matched with the Customer Service Department teams or other stakeholders. Only after formal acceptance, the ADP ESI NL releases changes into production. The production environment is maintained strictly separate from the Development and Test environments.

The structure and operations of the database management systems are defined during application development. Database changes are documented, and administrative responsibilities and database component definitions are assigned to appropriate personnel. Infrastructure management and product development staff possess the necessary skills and experience to perform their job responsibilities and all functions are accurately described.

The Product Development department team members develop, test, and deploy application changes into the Production environment. The product owner and the delivery manager approve the changes as part of the deployment process.



Logical Security

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

Management has implemented procedures to ensure that user accounts are added, modified, and deleted to reduce the risk of unauthorized and inappropriate system access. Only ADP employees are permitted to initiate access requests before they are routed to the appropriate ADP team for processing. Password standards include mandatory, periodic password changes, password complexity, and password history.

ADP ESI NL manages authorization requests for:

- Mainframe accounts (operating system and file system) for the Multipay application
- Local domain (NL.EHC.ADP.COM) containing the accounts that grant access to the production servers that host in-scope applications
- Application access rights for ADP ESI NL associates for all in-scope applications

For ADP associate accounts, including contractors, requests to create or modify access are recorded. Once approved by appropriate management, they are processed by the ADP GETS EMEA team.

Upon formal notification from ADP management or an automated revocation request, user accounts are removed or disabled timely.

Additions, modifications, and deletion of ADP associate accounts and access rights are managed through the ADAPT application. This application incorporates a workflow management tool that ensures proper approval of all requests by appropriate management.

Role-based access controls are implemented to restrict access to approved business needs. An ADP internal user recertification process verifies that all accounts in the system are linked to employees that are still employed by ADP and that the account is still needed by the employee in his or her current role and that all accounts from employees who have left ADP are disabled or removed. Also, ADP ESI NL manages user access on the local domain that contains the accounts that grant access to the production servers that host the in-scope applications.

Application access rights for client employees are managed by the clients themselves, using the appropriate self-service tools provided by ADP. Application access rights for client employees is the sole responsibility of the client.



Mainframe Access (Multipay Application only)

Password settings comply with corporate standards or adapted local standards (system specific to Mainframe) except in case of technical limitations.

ADP GETS EMEA organization Hosted Applications (ADP Perman, ADP Workforce, ADP Excasso, and iHCM Applications only)

ADP ESI NL is responsible for application logical access controls for ADP Perman, ADP Workforce, ADP Excasso, and iHCM (ADP GETS EMEA hosted). Password settings comply with corporate standards or adapted local standards, except in case of technical limitations.

Payroll Job Management (Prisal and Multipay Applications)

ADP management has implemented a daily process of handling payroll job exceptions. Exceptions are detected by e-mail alerts. Exceptions can be application/user-related. Application errors are managed by the ADP ESI NL R&D organization and user errors are managed by the ADP GETS EMEA Payroll Production (Production Control) department. Payroll Production handles the day-by-day payroll processing operations to ensure successful and timely completion.

ADP management has implemented controls to ensure access to payroll run submitting tools is limited to appropriate personnel.

For Multipay, a payroll job can be started with a specific JCL script procedure if one has also access to input and output datasets and dataset locations for the payroll run.

For Prisal, a payroll run in Prisal can be started from the “Prisal Menu” dashboard.



SUBSERVICE ORGANIZATIONS

ADP GETS EMEA Organization

Overview of Subservice Provider Relationship

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

ADP Perman, ADP Workforce, ADP Excasso, and iHCM Input Applications & Prisal Payroll Application

The table below outlines the control process areas applicable to the ADP Perman, ADP Workforce, ADP Excasso, and iHCM input applications & Prisal Payroll application that are covered in the scope of this report (Description of ADP's Netherlands Payroll Managed Services and Payroll Processing Services System SOC 1 Report) and those that are covered in the scope of ADP's GETS EMEA Organization SOC 1 Report:

Control Process Name	ADP's GETS EMEA Organization SOC 1 Report	ADP ESI NL Payroll MS and Payroll PS System SOC 1 Report
Application Change Management		
a. ADP Perman application		✓
b. ADP Workforce and ADP Excasso applications		✓
c. iHCM application		✓
d. Prisal application		✓
Operating System (OS) Software, Hardware, and Infrastructure Change Management		
a. Patch management	✓	
b. OS software, hardware, and infrastructure change management	✓	
c. Emergency changes	✓	
d. Server build guidelines	✓	



Control Process Name	ADP's GETS EMEA Organization SOC 1 Report	ADP ESI NL Payroll MS and Payroll PS System SOC 1 Report
e. Policies	✓	
Physical Security		
a. Datacenter access	✓	
b. Environmental safeguards	✓	
Network Monitoring		
a. Network monitoring and security mechanisms	✓	
Logical Security		
a. Network access	✓	
b. Operating System access	✓*	
c. Application access		✓**
d. Database access	✓	
Operational Monitoring and Incident Management		
a. Incidents raised by users	✓	
b. Incidents raised by monitoring tools	✓	
Payroll Job Management		
a. Payroll job monitoring		✓
b. Payroll job incident resolution		✓
System Backup		
a. Backup scheduling and monitoring	✓	
b. Onsite backup storage	✓	
c. Offsite backup replication	✓	

* except for user access management (access creation, modification and revocation) for the local domain NL.EHC.ADP.COM that is covered in this SOC 1 report. User access review and recertification of the local domain NL.EHC.ADP.COM are covered in ADP's GETS EMEA Organization SOC 1 Report.

** except for user access management (user access review and recertification) for Prisal application that is covered in ADP's GETS EMEA Organization SOC 1 Report. Access management (access creation, modification and revocation) for Prisal application is covered in this SOC 1 report.



Multipay Payroll Application

The table below outlines the control process areas applicable to the Multipay application that are covered in the scope of this report (Description of ADP's Netherlands Payroll Managed Services and Payroll Processing Services Systems SOC 1 Report) and those that are covered in the scope of ADP's GETS EMEA Organization SOC 1 Report:

Control Process Name	ADP's GETS EMEA Organization SOC 1 Report	ADP ESI NL Payroll MS and Payroll PS Systems SOC 1 Report
Application Change Management		
a. Multipay application		✓
Operating System (OS) Software, Hardware, and Infrastructure Change Management		
a. Patch management	✓	
b. OS software, hardware, and infrastructure change management	✓	
c. Emergency changes	✓	
d. Policies	✓	
Physical Security		
a. Datacenter access	✓	
b. Environmental safeguards	✓	
Network Monitoring		
a. Network monitoring and security mechanisms	✓	
Logical Security: User Access Management		
a. Network access	✓	
b. Operating System and File System access (Mainframe)		✓*
c. Application access (Multipay)		✓
Operational Monitoring and Incident Management		
a. Incidents raised by users	✓	
b. Incidents raised by monitoring tools	✓	
Payroll Job Management		
a. Payroll job monitoring		✓
b. Payroll job incident resolution		✓
System Backup		



Control Process Name	ADP's GETS EMEA Organization SOC 1 Report	ADP ESI NL Payroll MS and Payroll PS Systems SOC 1 Report
a. Backup scheduling and monitoring	✓	
b. Onsite backup storage	✓	
c. Offsite backup replication	✓	

* except for the user access review and recertification that are covered in ADP's GETS EMEA Organization SOC 1 Report (control 5.03).

Complementary Subservice Organization Controls

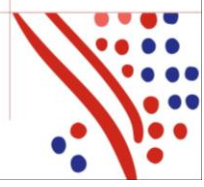
ADP's GETS EMEA organization is subject to the same oversight and governance as outlined in the "Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Control Activities, and Information and Communication" section previously described. Additionally, various business unit personnel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

Control Process Area	Subservice Organization Controls
Operating System (OS) Software, Hardware, and Infrastructure Change Management	Controls to address the implementation of and changes to operating system software, hardware, and infrastructure to confirm changes are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.
Physical Security	Controls to address physical access to computers and other resources to confirm it is restricted to authorized and appropriate personnel.
Environmental Safeguards	Controls to confirm operational procedures are in place within the hosting and data center facilities over physical assets to prevent processing errors and/or unexpected interruptions and support the complete, accurate, and timely processing and reporting of transactions and balances.
Network Monitoring	Controls to address ADP's network monitoring and security mechanisms for protection from external threats and interruptions.
Logical Security	Controls to address logical access to programs, data, and computer resources to confirm it is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.
Operational Monitoring and Incident Management	Controls to address operational problems identification and resolution in a timely manner.



Control Process Area	Subservice Organization Controls
System Backup	Controls to address regular data and applications backups and availability for restoration in the event of processing errors or unexpected processing interruptions.

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



COMPLEMENTARY USER ENTITY CONTROLS

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

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

Payroll Managed Services Clients Only

Control Objective 1: Payroll Input - Maintaining Payroll Master Files

Client management is responsible for:

- Verifying that the procedures agreed between ADP and the client are effectively applied and adjustments are discussed and approved by authorized client and ADP associates before implementation
- Appropriately and timely communicating client-specific or statutory changes affect the client's organization
- Communicating significant payroll or organizational changes that could affect the payroll operations to ADP timely and in compliance with the agreed procedures
- Verifying that the payroll master files are correct and payroll master file changes are communicated timely to ADP
- Using the appropriate means (Upload Data Sheets, front-end applications or SPM) to provide payroll data to ADP
- Verifying the accuracy, authorization, completeness, and clarity of the information and data sent to ADP
- Verifying that the payroll master file change requests are only made by an authorized client employee
- Verifying the data resulting from non-ADP software by authorized client employees, before sending to ADP (particularly time management data)
- Regularly verifying their employees' personnel data to ensure that it is accurate

For ADP's Payroll Managed Services clients contracted through the separate ADP Streamline service, control 1.02 is not applicable and this specific activity is the responsibility of the client.



Control Objective 2: Payroll Input - Maintaining Payroll Tables

Client management is responsible for:

- Verifying the accuracy, completeness, and clarity of the data delivered or transmitted to ADP
- Verifying the change requests and that changes are only made by an authorized client employee

Control Objective 3: Payroll Processing - Calculating Payroll

Client management is responsible for:

- Communicating discrepancies/errors to ADP in a timely manner
- Disbursing the payroll

Control Objective 4: Payroll Output

Client management is responsible for:

- Validating the completeness and accuracy of customized reports and data file outputs during the implementation process
- Notifying ADP of required changes to output reports or data files
- Testing and approving changes to output reports and data files
- Reviewing system reports and data file outputs for completeness and accuracy
- Reviewing Wage Tax declarations for completeness and accuracy
- Notifying ADP of errors identified in data outputs

Control Objective 5: Application Change Management

Client management is responsible for:

- Ensuring that their technical environment meets ADP's minimum specifications
- Verifying that the change implementation procedures that were defined in conjunction with ADP are effectively applied
- Verifying the accuracy, completeness, and clarity of the data delivered or transmitted to ADP
- Verifying change requests and that changes are only made by an authorized client employee

Control Objective 6: Logical Security: User Access Management

Client management is responsible for:

- Ensuring that user access is controlled by effective password security, access rights management, and complies with the client's requirements
- Implementing and maintaining appropriate security settings if the client has chosen to use established ADP security settings, including session time-out and expiration



- Implementing access rights management procedures for its client employees
- Ensuring access is limited to appropriate and authorized client personnel only
- Determining how the users are granted access and regularly reviewing their access rights
- Managing access rights for its client employees using the appropriate ADP self-service access management tools

Payroll Processing Services Clients Only

Control Objective 1: Payroll Input - Maintaining Payroll Master Files

Client management is responsible for:

- Verifying that the procedures agreed between ADP and the client are effectively applied and adjustments are discussed and approved by authorized client personnel and ADP associates before implementation
- The accuracy, authorization, completeness, and compliance with policies and procedures of payroll master file data input and deletions
- Verifying that the payroll master file changes are only made by an authorized client employee
- Verifying the data resulting from non-ADP software by authorized client employees, before sending to ADP (particularly time management data)
- Regularly verifying their employees' personnel data to ensure that it is accurate

Control Objective 2: Payroll Input - Maintaining Payroll Tables

Client management is responsible for:

- Verifying the accuracy, completeness, and clarity of the data delivered or transmitted to ADP
- Verifying that changes are only made by an authorized client employee

Control Objective 3: Payroll Processing - Calculating Payroll

Client management is responsible for:

- Validating the payroll reports (e.g., pay slips, collective reports, and error logs) before the final payroll run
- Validating the accuracy of the payroll calculations with self-selected sources and methods in case the client requested ADP not to provide the automatically generated payroll calculation reports
- Correcting and recalculating inaccurate pay slips before the final payroll run
- Disbursing the payroll



Control Objective 4: Payroll Output

Client management is responsible for:

- Validating the completeness and accuracy of customized reports and data file outputs during the implementation process
- Notifying ADP of required changes to output reports or data files
- Testing and approving changes to output reports and data files
- Reviewing system reports and data file outputs for completeness and accuracy
- Reviewing Wage Tax declarations for completeness and accuracy
- Notifying ADP of errors identified in data outputs

Control Objective 5: Application Change Management

Client management is responsible for:

- Ensuring that their technical environment meets ADP's minimum specifications
- Verifying that the change implementation procedures that were defined in conjunction with ADP are effectively applied
- Verifying the accuracy, completeness, and clarity of the data delivered or transmitted to ADP
- Verifying change requests and that changes are only made by an authorized client employee

Control Objective 6: Logical Security: User Access Management

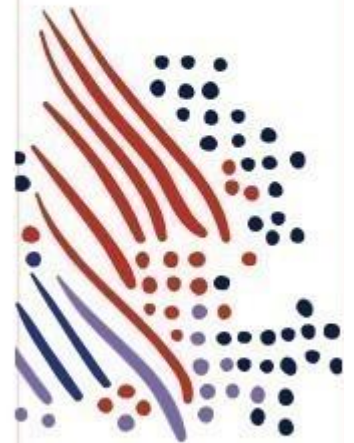
Client management is responsible for:

- Ensuring that user access is controlled by effective password security, access rights management, and complies with the client's requirements
- Implementing and maintaining appropriate security settings if the client has chosen to use established ADP security settings, including session time-out and expiration
- Implementing access rights management procedures for its client employees
- Ensuring access is limited to appropriate and authorized client personnel only
- Determining how the users are granted access and regularly reviewing their access rights
- Managing access rights for its client employees using the appropriate ADP self-service access management tools



SECTION FOUR

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



TESTING PERFORMED AND RESULTS OF TESTS OF ENTITY-LEVEL CONTROLS

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

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

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

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



TRANSACTION PROCESSING CONTROL OBJECTIVES AND CONTROLS

Payroll Input - Maintain Payroll Master Files

Control Objective 1: Controls provide reasonable assurance that additions, changes, and deletions to the payroll master file are authorized, complete, and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.01	<i>Access to Payroll Master Files</i> The ability to view, modify, or transfer payroll master file information is restricted to authorized ADP personnel.	Inspected the listing of users with the ability to view, modify, or transfer the payroll master file information and inquired of management regarding their job responsibilities to determine whether access was restricted to authorized ADP personnel only.	No deviations noted
1.02	<i>Authorized Change Requests</i> Requested changes (additions, changes, and deletions) to the payroll master files are inspected to determine that the request was received by an authorized client contact. (MS clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the change request to determine whether the request was received by an authorized client contact.	No deviations noted
1.03	<i>Complete Change Requests</i> Requested changes (additions, changes, and deletions) to the payroll master files are inspected to determine the completeness of the requests received from the clients. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the checklists to determine whether the completeness of the change request received from the client was verified.	No deviations noted



Control Objective 1: Controls provide reasonable assurance that additions, changes, and deletions to the payroll master file are authorized, complete, and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.04	<i>Authorized Source Documentation</i> Recorded changes (additions, changes, and deletions) to the payroll master files are compared to authorized source documents, by the payroll specialist or back-office, to help ensure the changes were input accurately. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the checklists to determine whether payroll master file changes were compared to authorized source documents by the payroll specialist or back-office to help ensure that the changes were input accurately.	No deviations noted
1.05	<i>Compliance Policies and Procedures</i> Recorded changes (additions, changes, and deletions) to the payroll master files are checked by the payroll specialist or back-office associate for compliance with client-employee policies and procedures including compliance with statutory regulation and union requirements, if applicable. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the payroll reports and checklists to determine whether compliance with client-employee policies and procedures including compliance with statutory regulation and union requirements, where applicable, were checked by the payroll specialist or back-office associate.	Deviation noted For one (1) out of twenty-five (25) payrolls with changes to the payroll master files, supporting evidence of the compliance review could not be provided due to the use of an incorrect checklist by the payroll specialist. <i>Refer to the end of this Control Objective section for additional procedures performed by Ernst & Young and Management's Response.</i>



Control Objective 1: Controls provide reasonable assurance that additions, changes, and deletions to the payroll master file are authorized, complete, and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.06	<i>Validation Recorded Changes</i> Recorded changes to the payroll master files input by a back-office associate are validated by a second back-office associate to verify their accuracy and completeness. Identified errors are corrected immediately. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the checklists to determine whether the changes that were input by a back-office associate were validated by a second back-office associate to verify their accuracy and completeness and, in addition, any identified errors were corrected immediately.	No deviations noted
1.07	<i>Completeness Review Supervised Locations</i> The activities performed by ADP-supervised locations are reviewed by the front-office employee (ADP ES NL) to help ensure changes to the payroll master files, provided to the ADP-supervised locations, are processed completely, and initiate corrective actions if needed. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the checklists to determine whether the activities performed by ADP-supervised locations were reviewed by the front-office employee (ADP ES NL) to help ensure changes to the payroll master files, provided to the ADP-supervised locations, were processed completely and corrective actions were initiated if needed.	No deviations noted



Control Objective 1: Controls provide reasonable assurance that additions, changes, and deletions to the payroll master file are authorized, complete, and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
1.08	<i>Accuracy Review Recorded Changes</i> Recorded payroll master file changes are reviewed monthly by a payroll specialist for accuracy and completeness based on automatically generated change reports and source documentation. (MS & Streamline clients only)	For a sample of payrolls with changes to the payroll master files (additions, changes, and deletions), inspected the automatically generated change reports source documentation and the checklists to determine whether payroll master file data changes were reviewed monthly for accuracy and completeness by a payroll specialist.	No deviations noted
1.09	<i>Payroll Master Files Input and Changes</i> Clients can enter payroll master file data into the front-end systems. Once entered, the Prisal or Multipay application payroll master files are automatically updated. (PS clients only)	Inspected the payroll calculation reports and system records to determine whether, for adding or changing payroll master file data in the front-end applications, the data input was completely and accurately recorded in Prisal or Multipay application automatically.	No deviations noted
1.10	<i>Payroll Master Files Data Deletions</i> Clients can remove or delete payroll master file data from the front-end systems. Deleted data is recorded automatically in the Prisal or Multipay application. (PS clients only)	Inspected the payroll calculation reports and system records to determine whether, for deleting payroll master file data in the front-end applications, the data deletion was completely and accurately recorded in Prisal or Multipay application automatically.	No deviations noted



Management Response to Testing Deviations:

Control 1.05 – Management agrees that for one (1) payroll, an incorrect procedures checklist was used for an additional payroll run. As a result, Management performed a retrospective review of the one (1) identified payroll. From this review, Management confirmed that all mandatory steps were performed correctly, and that the final checks, performed at the time of the payroll run processing, already confirmed the payroll was run correctly. Management also confirmed that upon further inspection, no other incorrect checklists were used for additional payroll runs during the examination period. There was no impact to client data.

Additional Procedures Performed by Ernst & Young:

Control 1.05 – EY inspected the supporting documentation provided by ADP to verify that the final validations for the payroll run were completed by two front office ADP NL associates, indicating that the recorded changes (additions, changes, and deletions) to the payroll master files were checked by the payroll specialists for compliance with client-employee policies and procedures including compliance with statutory regulation and union requirements, if applicable. Additionally, EY inspected the review performed by Management in May 2021 and the written confirmation to gain comfort that the control exception was an isolated case.



Payroll Input - Maintain Payroll Tables

Control Objective 2: Controls provide reasonable assurance that changes to the payroll tables are authorized, complete and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
2.01	<i>Access to Payroll Tables</i> Access to payroll tables is restricted to authorized ADP personnel.	Inspected the listing of ADP users with the ability to access the payroll tables and inspected the user access review document (controls 6.03 & 6.04) to determine whether access was restricted to authorized ADP personnel only.	No deviations noted
2.02	<i>Change Requests</i> Requests to change the payroll tables are recorded and entered by authorized ADP personnel.	For a sample of changes to the payroll tables, inspected the change requests to determine whether requests to change the payroll table data were recorded and entered by authorized ADP personnel.	No deviations noted
2.03	<i>Change Authorization and Validation</i> Changes to the payroll tables are compared to authorized source documents to help ensure that they were entered accurately, completely, and are validated by appropriate personnel (test engineer from the development team) and identified errors are corrected promptly.	For a sample of changes to the payroll tables, inspected the source documents and the activity transition logs (JIRA) to determine whether the changes were compared to authorized source documents to help ensure that they were input accurately, completely, and were validated by appropriate personnel (test engineer from the development team) and identified errors were corrected promptly.	No deviations noted
2.04	<i>Approved Changes</i> Changes to the payroll tables are approved by ADP management.	For a sample of changes to the payroll tables, inspected the change requests (user stories) to determine whether changes to the payroll tables were approved by ADP management.	No deviations noted



Control Objective 2: Controls provide reasonable assurance that changes to the payroll tables are authorized, complete and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
2.05	<i>Accuracy and Ongoing Pertinence</i> Payroll table changes are reviewed by authorized associates for accuracy and ongoing pertinence before released into the production environment.	For a sample of changes to the payroll tables, inspected the release reports to determine whether payroll table changes were reviewed by authorized associates for accuracy and ongoing pertinence before release into the production environment.	No deviations noted
2.06	<i>Compliance with Statutory Requirements</i> Payroll table changes are reviewed by the Legal Watch Team for compliance with the statutory requirements before release into the production environment.	For a sample of changes to the payroll tables, inspected the release reports to determine whether payroll table changes were reviewed by the Legal Watch Teams for compliance with the statutory requirements before release into the production environment.	No deviations noted



Payroll Processing - Calculating Payroll

Control Objective 3: Controls provide reasonable assurance that payroll calculations (including compensation and withholdings) are accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
3.01	<i>Validation Payroll Reports</i> Payroll calculations are checked for consistency by the payroll specialists using the payroll calculation reports. Identified discrepancies are resolved by the payroll specialist. (MS & Streamline clients only)	For a sample of payrolls, inspected the payroll calculation reports to determine whether: - the payroll calculations and error reports were checked for consistency by the payroll specialist - the discrepancies identified were resolved by the payroll specialist	No deviations noted
3.02	<i>Validation Payroll Run</i> Payroll reports (i.e., payslips, collective reports, and error logs) are validated by the payroll specialist before the final payroll run. (MS & Streamline clients only)	For a sample of payrolls, inspected the payroll reports to determine whether they were validated by the payroll specialist before the final payroll run.	No deviations noted
3.03	<i>Follow-Up Inaccurate Payslips</i> Inaccurate payslips are corrected and recalculated by the payroll specialist before the final payroll run. (MS & Streamline clients only)	For a sample of payrolls, inspected the payslips to determine whether inaccurate pay slips were corrected and recalculated by the payroll specialist before the final payroll run.	No deviations noted



Payroll Processing - Payroll Output

Control Objective 4: Controls provide reasonable assurance that the payroll products are complete and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
4.01	<i>Payroll Reports</i> Payroll calculation reports are automatically generated by running the payroll calculation process.	Inspected the program codes for the Prisal and Multipay payroll engines to determine whether the payroll calculation reports (including the Wage Type Statement, Payroll Register, Bank Summary, EFT file and the payslips) were automatically generated by running the payroll calculation process.	No deviations noted
4.02	<i>Tax Declarations</i> The payroll specialist verifies the generation of the Wage Tax Declarations as a result of the final payroll run. (MS & Streamline clients only)	For a sample of payrolls, inspected the checklists to determine whether the generation of the Wage Tax Declarations as a result of the final payroll run was validated by the payroll specialist.	No deviations noted



Control Objective 4: Controls provide reasonable assurance that the payroll products are complete and accurate.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
4.03	<i>Journal Entry files</i> The payroll specialist verifies the generation of the Journal Entry Files as a result of the final payroll run. The payroll specialist verifies that the Journal Entries of the final payroll run are identical to the journal entries generated in the preliminary payroll runs in the payroll calculation phase, thus ensuring the final payslips are identical to the trial payslips. (MS & Streamline clients only)	For a sample of payrolls, inspected the checklists to determine whether the payroll specialist: • validated the generation of the journal entry files as a result of the final payroll run • verified that the journal entries of the final payroll run were identical to the journal entries generated in the preliminary payroll runs in the payroll calculation phase, to help ensure that the final payslips were identical to the trial payslips	No deviations noted



GENERAL COMPUTER CONTROL OBJECTIVES AND CONTROLS

Application Change Management

Control Objective 5: Controls provide reasonable assurance that the implementation of and changes to application programs (incl. payroll rules) 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
5.01	<i>Documentation and Authorization of a Change Request</i> Change requests are documented, reviewed, and authorized by appropriate personnel.	For a sample of changes to payroll applications (front-end and Prisal & Multipay payroll engines), inspected the change requests (user stories) to determine whether change requests were documented, reviewed, and authorized by appropriate personnel.	No deviations noted
5.02	<i>Testing Procedures</i> Changes are tested in a dedicated testing environment according to a defined testing strategy.	For a sample of changes to payroll applications (front-end and Prisal & Multipay payroll engines), inspected the ticket documentation to determine whether changes were tested in a dedicated testing environment according to the defined testing strategy.	No deviations noted
5.03	<i>Deployment Authorization</i> Management approval is obtained prior to the deployment of changes to production. This approval confirms that change has been authorized, testing has been performed and that supporting documentation is available.	For a sample of changes to payroll applications (front-end and Prisal & Multipay payroll engines), inspected the change requests (user stories) to determine whether the changes were approved by management prior to deployment, confirming that the change was authorized, tested, and supporting documentation was available.	No deviations noted
	Deployment is communicated to the relevant internal and external users.	For a sample of changes to payroll applications (front-end and Prisal & Multipay payroll engines), inspected the change requests (user stories) to determine	No deviations noted



Control Objective 5: Controls provide reasonable assurance that the implementation of and changes to application programs (incl. payroll rules) are authorized, tested, documented, approved and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
		whether the deployment of changes was communicated to the relevant internal and external users.	
5.04	<i>Deployment Privileges</i> Only authorized personnel can move program code to the production environment.	Inspected the listing of users with the ability to move program code to the production environment and inquired of ADP management regarding the job responsibilities to determine whether access was restricted to authorized personnel only.	No deviations noted
5.05	<i>Compliance Review</i> Changes to the application programs (incl. payroll rules) are reviewed for compliance with statutory requirements.	For a sample of changes to payroll applications (front-end and Prisal & Multipay payroll engines), inspected the user stories to determine whether the changes were reviewed for compliance with statutory requirements.	No deviations noted



Logical Security: User Access Management

Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
6.01	<i>Access Creation or Modification (ADP users)</i> For ADP associates, including contractors, requests for the creation or modification of user access are formally recorded and approved by appropriate management.	For a sample of ADP access creations or modifications (local domain, Multipay operating system and applications), inspected the access requests and the supporting documentation (i.e., emails, tickets, etc.) to determine whether requests were recorded, approved by appropriate management and the access assigned was in accordance with the access requested.	No deviations noted
6.02	<i>Access Revocation (ADP users)</i> User accounts are timely disabled upon request from appropriate ADP management or upon employee termination.	For a sample of employees who left during the examination period, inspected the request for revocation of user access (local domain, Multipay operating system and applications), the HR listing and system records to determine whether access was disabled timely.	Deviation noted For one (1) out of six (6) terminated employees tested, the user was not disabled in a timely manner. <i>Refer to the end of this Control Objective section for additional procedures performed by Ernst & Young and Management's Response.</i>



Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
6.03	<i>User Access Review</i> Reviews are performed yearly to help ensure that: - ADP associate access that is no longer required is disabled or deleted in a timely manner - Accounts are assigned to a physical person and that non-personal accounts are justified and assigned to an account owner Discrepancies are analyzed, documented, and reported to management.	Inspected the user access review documents to determine whether an annual user access review was performed to help ensure that: - ADP associate access to the in-scope applications (except Prisal) that were no longer required, were disabled or deleted in a timely manner - Accounts were assigned to a physical person and that non-personal accounts are justified and assigned to an account owner	No deviations noted
		Inspected the user access review documents to determine whether discrepancies identified during the account reviews were analyzed, documented, reported to management and resolved.	No deviations noted
6.04	<i>User Access Recertification</i> User access permissions assigned to ADP associates' accounts on applications are reviewed yearly to help ensure that they are in alignment with their job roles. Discrepancies are analyzed, documented, and reported to management.	Inspected the user access review documents to determine whether a user access recertification (for in-scope applications except Prisal) was performed yearly to help ensure that user permissions assigned to ADP associate application accounts were aligned with their job roles.	No deviations noted
		Inspected the user access review documents to determine whether discrepancies identified during the account reviews were analyzed, documented, reported to management and resolved.	No deviations noted



Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
6.05	<i>Authentication Mechanisms</i> Password rules/restrictions are enforced according to policy. Any exceptions to policy are documented and reported to management.	For in-scope production systems (Multipay operating system and applications), inspected the password configuration settings for end-user access to determine whether password policies were enforced and, in case of any exceptions to the policy, inspected ticket documentation to determine whether these exceptions were documented and reported to management.	No deviations noted



Management Response to Testing Deviations:

Control 6.02 – Management agrees that one (1) associate (contractor) had a different end date in the HR registration system (GlobalView) than shown in the access Management system (ADAPT) and was not disabled in a timely manner. Contractors have a mandatory end date of no more than six (6) months into the future, so each contractor needs to be extended at least every six (6) months. During the last extension for this associate, the manager requested of the General Manager (GM) an extension of two (2) additional weeks to obtain the financial commitment. Unfortunately, the GM's approval was not sent to the HR department.

The leaving date in GlobalView remained at the old value and ADAPT was updated manually with the new end date. For ADP associates with a contract, this situation cannot occur as for those accounts a synchronization between GlobalView and ADAPT is in place. For contractors, this synchronization is not implemented due to technical constraints. Management considers the risk of unauthorized access to be minimal, as the associate did not have access rights to any customer data. Management also determined that the associate's account was not used during the requested two (2) week extension. Moreover, Management performed a retrospective review of the 56 employees who left ADP during the examination period. From this review, Management identified three (3) contractors (in addition to the instance identified above) and compared the termination dates recorded in GlobalView and ADAPT respectively to confirm that user accounts were timely disabled upon employee termination.

Mitigating actions (HR approval on extensions for contractors) have been implemented to prevent this from happening again in the future.

Additional Procedures Performed by Ernst & Young:

Control 6.02 – EY reviewed the account details for this associate to confirm the user account had no access to in-scope applications but only to the local domain NL.EHC.ADP.COM. EY also reviewed the last logon details at the network layer for this associate to confirm the user account was not used after the termination date.

Additionally, EY inspected the review performed by Management to confirm the completeness and precision of the review, resulting in no additional identified instances and providing comfort that the control exception was an isolated case.



Payroll Job Management

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

<i>Ref</i>	<i>Description of Control Activity</i>	<i>Test of Controls</i>	<i>Results</i>
7.01	<i>Payroll Job Monitoring</i> Payroll system operations processing is monitored to help ensure successful and timely completion.	Inspected the configuration settings of the monitoring tool to determine whether payroll system operations processing was monitored to help ensure successful and timely completion.	No deviations noted
7.02	<i>Payroll Job Incident Resolution</i> Exceptions to normal processing are reviewed on a daily basis and investigated by management to help ensure their resolution.	For a sample of payroll processing exceptions, inspected the exception logs and resolution documentation to determine whether errors were recorded, analyzed, and resolved timely.	No deviations noted
7.03	<i>Payroll Job Scheduling</i> Access to the payroll run submitting tools is limited to appropriate personnel.	Inspected the listing of users with access to the payroll run submitting tools and inquired of management regarding their job responsibilities to determine whether access was restricted to appropriate personnel only.	No deviations noted



SECTION FIVE

OTHER INFORMATION PROVIDED BY ADP

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



ADP GLOBAL BUSINESS RESILIENCY PROGRAM

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

Disaster Recovery Planning

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

Disaster Recovery plans have been developed to:

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

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

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

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

Business Continuity Planning

Business Continuity plans 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:

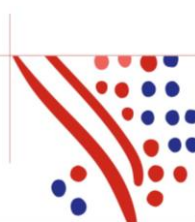
- Crisis Management/Emergency Response
- Incident Detection/First Alert Notification
- Plan Activation
- Recovery Strategies/Recovery Recommendations
- Recovery Procedures, Tasks and Resource Requirements
- Minimum Recovery Configurations
- Plan Administration
- Reports/Forms

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

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 with 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 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.

