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

Description of XYZ Company's Payroll Services System for the period January 1, 202X to December 31, 202X

Table of Contents

SECTION ONE

INDEPENDENT SERVICE AUDITOR'S REPORT
PROVIDED BY ERNST & YOUNG

Building a better working world

INDEPENDENT SERVICE AUDITOR'S REPORT

Management of XYZ Company

Scope

We have examined XYZ Company's description entitled "Description of XYZ Company's Payroll Services System for the period January 1, 202X to December 31, 202X" (Description) of its Payroll Services System (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in "XYZ Company Management Assertion" (Assertion). The Control Objectives and controls included in the Description are those that management of XYZ Company believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of XYZ Company'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.

XYZ Company utilizes a subservice organization to provide certain hosting operations, data center management, and network management services to support XYZ Company's Payroll Services System. The Description includes only the Control Objectives and related controls of Payroll Services System and excludes the control objectives and related controls of the subservice organization.

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

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

XYZ Company's responsibilities

XYZ Company has provided the accompanying assertion titled, XYZ Company 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. XYZ Company is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period January 1, 202X to December 31, 202X. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Inherent limitations

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

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

Description of tests of controls

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

Opinion

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

a. The Description fairly presents the System that was designed and implemented throughout the period January 1, 202X to December 31, 202X.
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 January 1, 202X to December 31, 202X and if subservice organizations and user entities applied the complementary controls assumed in the design of XYZ Company's controls throughout the period January 1, 202X to December 31, 202X.
c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period January 1, 202X to December 31, 202X, if complementary subservice organization and user entity controls assumed in the design of XYZ Company's controls operated effectively throughout the period January 1, 202X to December 31, 202X.

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 XYZ Company, user entities of XYZ Company's System during some or all of the period January 1, 202X to December 31, 202X, 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.

Month XX, 20XX

SECTION TWO

MANAGEMENT ASSERTION

XYZ COMPANY MANAGEMENT ASSERTION

Month XX, 202X

We have prepared the description of XYZ Company's Payroll Services System entitled, "Description of XYZ Company's Payroll Services System for the period January 1, 202X to December 31, 202X" (Description) for processing user entities' transactions throughout the period January 1, 202X to December 31, 202X for user entities of the system during some or all of the period January 1, 202X to December 31, 202X, 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.

XYZ Company utilizes a subservice organization to provide certain hosting operations, data center management, and network management services to support its Payroll Services System. The Description includes only the control objectives and related controls of XYZ Company and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of XYZ Company'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 XYZ Company's Payroll Services System (System) made available to user entities of the System during some or all of the period January 1, 202X to December 31, 202X 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 January 1, 202X to December 31, 202X 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 XYZ Company's controls throughout the period January 1, 202X to December 31, 202X. 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.

XYZ Company

SECTION THREE

DESCRIPTION OF XYZ COMPANY'S PAYROLL SERVICES SYSTEM FOR THE PERIOD JANUARY 1, 202X to DECEMBER 31, 202X

OVERVIEW OF OPERATIONS

General

XYZ Company Overview

Business Overview

XYZ Company's Mission

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

CONTROL ENVIRONMENT

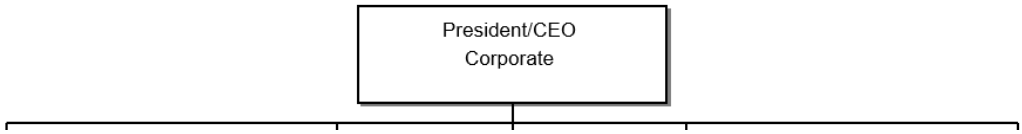
XYZ Company's control environment description….

Oversight by XYZ Company's Board of Directors

XYZ Company's Board of Directors description..

Organizational Structure

Corporate Structure



Other XYZ Company Corporate Supporting Groups

XXXXXX

Human Resources Policies and Practices

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

The HR department is primarily responsible for recruiting and evaluating job applicants. Based on the sensitivity of the underlying job, various levels of background checks are performed on applicants prior to or following their employment. HR policies and procedures are posted on XYZ Company'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 XYZ Company and Third Party Software
- Harassment
- Substance Abuse
- Confidentiality of Information
- Electronic Communication Systems
- Corrective Actions

XYZ Company's core values are posted on XYZ Company'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 XYZ Company's general operating practices, policies and procedures, and assists employees in becoming acclimated to XYZ Company's business philosophy. The orientation activities assist new associates in understanding XYZ Company's overall mission and core values, departmental operation practices, and individual performance objectives.

XYZ Company has a formal "Code of Conduct" that all employees must read and acknowledge as part of their new employee orientation. In addition, associates are required to disclose any previously unreported circumstances or events known by the employee that appear to be in violation of this Code. XYZ Company 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 XYZ Company. 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 XYZ Company. Associates who violate XYZ Company'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.

XYZ Company 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.

RISK ASSESSMENT

XYZ Company's Risk Assessment Process

MONITORING

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

XYZ Company 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.

Internal Audit Monitoring

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

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

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

CONTROL ACTIVITIES

XYZ Company 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

XYZ Company'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.

CONTROL OBJECTIVES AND CONTROLS

The control objectives specified by XYZ Company, 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 PAYROLL SERVICE

Service Overview

XYZ Company's Payroll Services System is comprised of processing that includes:

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

The XYZ Company payroll locations supporting clients throughout the U.S. and Canada are comprised of:

- Service Payroll Centers – Business Functions perform the primary activities for Payroll Services clients, including printing client payrolls, XYZ Company Checks, and distribution of payroll-related documents and files. The Business Function also perform the gross-to-net calculations. Region activities are processed on the mainframe platform hosted at XYZ Company's hosting and data center facility.
- Satellite locations are responsible for selling products to clients, implementing clients on the various XYZ Company platforms, and providing ongoing client support.

IT Applications and Supporting Infrastructure

The Payroll Services System is comprised of the applications depicted below, along with the supporting operating systems and database platforms:

Application Name	Operating System Technology	Database Technology	Description
Payroll Application	XXXX	XXXX	Payroll Application Description
Reporting Application	XXXX	XXXX	Reporting Application Description

Key Organizational Support Structure

XXXXXXXX

Changes to the Control Environment

XXXXXXXX

SCOPE OF THE REPORT

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

This report covers XYZ Company's Payroll Services that comprise the hosting and outsourcing of payroll transaction processing applicable to XYZ Company's Application and the supporting Data Entry Systems described in the prior section (collectively referred to as the "Payroll Services System").

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

TRANSACTION PROCESSING

Overview of Key Transaction Processing/Services

Payroll Services transaction processing encompasses three major components: Payroll Input, Payroll Processing, and Payroll Output. Payroll Input consists of payroll data related to an employee's current period hours and/or earnings and Masterfile maintenance that is collected from the client into XYZ Company provided Input Systems or communicated directly to XYZ Company for input by phone or fax. XYZ Company processes payroll transactions using the client-provided input and generates a variety of standard and optional output reports (e.g., payroll registers, payroll summary), data files. Output reports and files are distributed to clients when produced.

Payroll Input

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

- Automated Input (primary method) – Clients can use one of several XYZ Company-supplied Input Systems. Input Systems can be hosted by XYZ Company or installed at a client site (i.e., premised-based systems). Premised-based systems are optional and not in the scope of this Description.
- Manual Input (secondary method – a small percentage of clients) – Clients communicate payroll data to XYZ Company over the phone or send completed system-generated standard forms that contain payroll data via fax or courier. Once received XYZ Company Data Entry operators manually enter the payroll information into the Application for processing.

Automated Input

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

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

Manual Input

Payroll Services clients can also submit payroll transactions directly to XYZ Company operators by phone. Some Business Functions are able to receive client payroll information by fax.

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

Statutory (STAT) File Maintenance

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

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

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

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

Upon identification of a statutory change, the Statutory Research Shared Services Group creates a Feature tracking item in the change management software. The Feature includes details obtained from the Work in Progress (WIP) item used for monitoring and indicates that an actual statutory change was issued. The Statutory Project Manager then creates a "Development" Feature tracking item in the Change Management Software, which

is assigned to a Business Analyst on the Payroll Statutory change management team. The Business Analyst is responsible for prioritizing, analyzing, and scheduling the statutory item, based upon the effective date of the statutory change. Identifying the Application impacts (e.g., STAT File, quarter, client, region), and creating "User Stories" in the Change Management Software to be used for further research and development of the proposed change, is also the responsibility of the business analyst.

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

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

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

Updates requiring coding modifications are coded and tested by either the Payroll Statutory change management team or designated Scrum teams. Both teams certify and "accept" changes signifying they are ready for release to the Application production environment. The process and controls for releasing changes follow the Change Management process described in the *General Computer Controls* section of this Description.

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

Payroll Processing

Processing is divided into two phases: EDIT and NET/CALC. XYZ Company uses the Application's PTCS to track, control, and monitor the results of each processing phase. PTCS controls the processing of data from Datapool through NET/CALC processing. Using online screens, individual Business Functions can define processing parameters based on their individual requirements, including the length of time data, can accumulate before being transferred to the next processing phase. PTCS also provides online inquiry to track the status of the

individual payrolls that are being processed by the Application. PTCS also provides online control totals and daily production statistics that are used to track and monitor Application processing activities.

EDIT Processing

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

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

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

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

NET/CALC Processing

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

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

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

Monitoring of Processing Activities

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

Output

WRAP Processing

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

Pay Statements

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

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

Design characteristics in XYZ Company's payroll checks and stubs provide security protection against color copy and scanner duplication systems. The checks include an intricate encoding pattern within high-resolution borders that become distorted when duplicated. In addition, the background of the checks uses a multi-tone shade over a cascading building block design (prismatic printing) that is difficult to accurately reproduce and the shading

accentuates the word “VOID” when the check is copied. On the reverse side of the check, a unique printing pattern of multi-width lines embedded with encoding marks has been added to protect the document from scanner duplication. In addition, XYZ Company’s check design uses a number of sophisticated features that include:

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

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

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

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

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

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

Reports

In each region, the CSSs are responsible for setting up and maintaining clients’ reporting requirements and schedules in MR 2000. MR 2000 enables report customization and generation. Reports can be printed or made available electronically in PDF format through XYZ Company’s system, depending on client requirements. The

following table presents a listing of the standard reports available to clients to support their financial reporting requirements:

Report/File Name(s)	Description	Source and Preparation
Payroll Output Report	XXXXX	XXXX

Delivery of Printed Reports

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

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

Delivery of Electronic Reports and Pay Statements

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

Data Files

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

- Other Payroll Related Files – These output files consist of electronic payroll registers, year-to-date, AMC, and any other custom client reports that are transmitted from to the Input Systems for clients to view, download, and/or print.

Funds Transfer/Direct Deposit Files

The Application produces funds transfer and direct deposit files and transmits them, for clients that have elected FSDD or a regular Direct Deposit option as follows.

Transmission to Financial Institutions or Bank Service Processors

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

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

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

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

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

Data File Transmission Monitoring

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

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

GENERAL COMPUTER CONTROLS

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

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

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 authorized users.

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

Logical Security

Network Access

To access the Application, XYZ Company users must first authenticate to XYZ Company's network. \

Application – Mainframe Access

Once authenticated at the network-level, logical access to the Application is controlled through an external security manager.

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

Information security's primary goal is to help control access to application programs, client data and transactions, and other computing resources as well as restricting access to authorized users.
Management has implemented a formal process to grant logical access privileges based on the user's job responsibilities. Logical access requests are formally approved by management or Human Resources. Access requests are documented in a centralized Service Desk Problem Management System.

Management sends access requests to the Technical Services group who reviews the forms for completeness and assigns a unique user ID and password to the user as well as user ID and password to access the mainframe

production environment. The Technical Services Group then communicates the user IDs and initial passwords to the requester by email or phone. Users are forced to change their mainframe passwords upon initial login.

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

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

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

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

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

XYZ Company’s Hosting Organization is responsible for supporting the OS and database administration at the infrastructure level. In addition, database access for application support purposes is also granted to authorized personnel, the use of application database accounts is managed by the individual application support teams for the environment.

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

Data Entry Systems Application Layer – Security Administration

XYZ Company associates are granted update access to the Data Entry Systems for troubleshooting purposes which permits XYZ Company support personnel to log into a client environment using a valid user name and password. The client is responsible for administering access to Data Entry Systems for its employees.

A valid user ID and password are required to authenticate to the Data Entry Systems. Password controls include expiration after a specific number of days, required minimum length, and password history tracking.

Application Development and Change Management

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

Application Development and Change Management

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

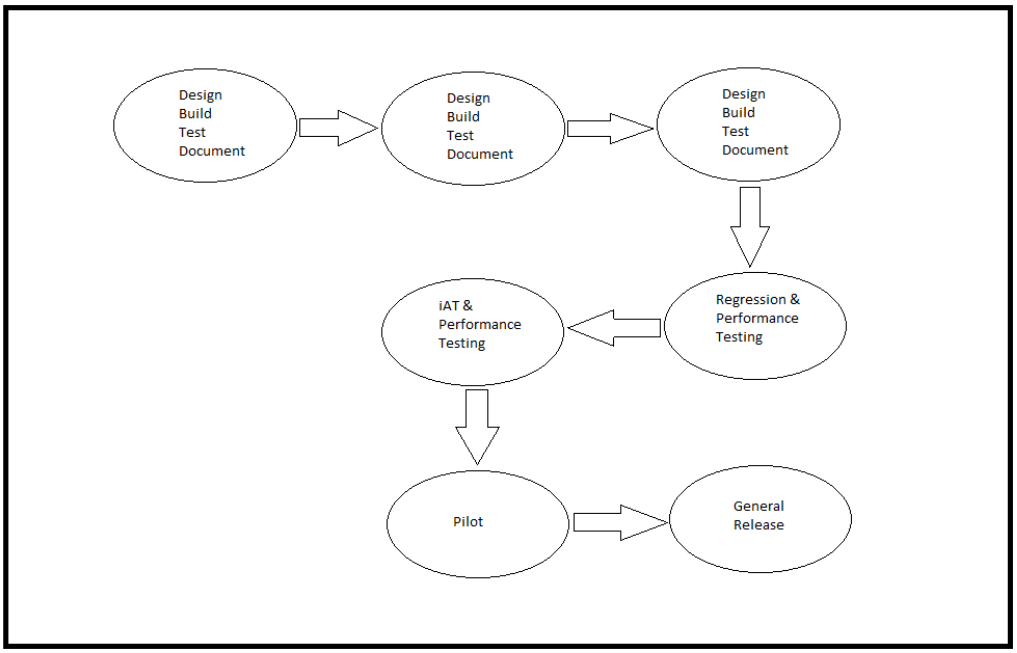
Change Request Management

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

Software Development, Testing and Implementation Procedures

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

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



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

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

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

Development implements Agile Scrum and/or Kanban as a management framework for incremental product development using one or more cross-functional, self-organizing teams of about seven people each. It provides a

structure of roles, meetings, rules, and artifacts. Teams follow best practices defined by XYZ Company management and are responsible for creating and adapting processes within this framework. Scrum uses fixed-length iterations, called Sprints, which are typically three weeks long. Scrum teams attempt to build a potentially shippable (properly tested) product increment in each sprint.

Agile Roles

Product Owner

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

Scrum Master

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

Scrum Development Team

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

Agile Ceremonies

Sprint Planning Meeting

At the beginning of each Sprint, the Product Owner and Scrum Development Team hold a Sprint Planning Meeting to negotiate which Product Backlog Items they will attempt to convert to working product during the Sprint. The Product Owner is responsible for declaring which items are the most important to the business

(Minimum Viable Product – MVP). The Scrum Development Team is responsible for selecting the amount of work to implement without accruing technical debt.

Daily Scrum and Sprint Execution

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

Sprint Review Meeting

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

Sprint Retrospective Meeting

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

Backlog Refinement Meeting

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

<u>Documentation (performed in parallel with Scrum and Kanban)</u>

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

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

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

Release Hardening, iAT, Pilot, General Release:

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

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

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

Pilot Phase
As part of the Pilot Phase, the Application releases/changes are installed and run on one or more LPARs to monitor performance. The Technical Services Group has an Implementation Guide documenting the installation process. Offsite IT personnel from XYZ Company Release Management and development groups provide technical support to the pilot region. Feedback from the pilot LPARs drives modifications to programs, documentation, or training procedures.

General Release Phase
Upon successful completion of the iAT and/or Pilot phases, the Release Management Group sends a written communication authorizing deployment to XYZ Company's production environment. Upon receipt of the

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

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

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

Data Entry Systems Development and Change Management

Changes to the Data Entry Systems, consist of major releases, break fixes, minor enhancements, configuration changes, report changes, or emergency changes. Changes are governed by the respective product owner and/or business unit management responsible for the Data Entry Systems.

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

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

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

Application – Operating System and Database Change Management

Policy and Methodology

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

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

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

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

Testing

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

Deploying the Updates

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

SUBSERVICE ORGANIZATIONS

ABC Company Hosting Services

Overview of Subservice Provider Relationship

The Payroll application and supporting technology infrastructure are hosted and managed by ABC Company Hosting Services.

Complementary Subservice Organization Controls

ABC Company 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 Hosting organization personnel on a regular basis. The Hosting organization has implemented the following key control activities to support the associated control objectives as they related to the scope of this Description:

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

These controls are covered in ABC Company's Hosting Service SOC 1 Report.

COMPLEMENTARY USER ENTITY CONTROLS

XYZ Company 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 XYZ Company'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 XYZ Company's user entities. Other controls may be required by user entities and should therefore be evaluated by the user entity. User entity auditors should consider whether user entities have implemented these controls (as applicable) when understanding and evaluating the internal controls at the respective user entity.

Control Objective #1: Payroll Data Input

Client management is responsible for:

- Notifying XYZ Company of changes in the authorized contacts list
- Validating the accuracy of initial data entry when using the Input Systems
- Reviewing error messages that result from transmitting data, addressing errors and resending data in a timely manner
- The accuracy/completeness and authorization of worksheets and faxes that are sent to XYZ Company
- Setting up a second authentication method (such as the use of a passphrase) for phone or fax payrolls
- Setting up a receipt confirmation method (such as callback or fax) for phone or fax payrolls
- Reviewing Correction Notices received from XYZ Company
- Reviewing the Master Control form, containing the listing of each employee's master record, produced by the Application after initial account set-up, to confirm that employee-level and company-level information was initially recorded completely and accurately

Control Objective #2: Deductions and Tax Withholding Specifications

Client management is responsible for:

- The completeness and accuracy of client-specified deductions
- Submitting client-specified deduction changes to XYZ Company in a timely manner
- Verifying that deduction and tax withholding information is accurate before providing payroll processing approval if client uses Quick View
- Reviewing the Master Control and Personnel Change reports that are distributed upon payroll processing to determine whether deduction and tax withholding information is complete and accurate and notifying XYZ Company if an error is identified or a change needed

Control Objective #3: Payroll Processing

Client management is responsible for:

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

Control Objective #4: Payroll Output

Client management is responsible for:

- Notifying XYZ Company of changes required to their payroll output
- Printing and secure check distribution, if done in-house by client
- Defining the processing schedule and communicating required changes to XYZ Company in a timely manner
- Acknowledging the receipt of payroll output
- Reviewing the payroll output reports and notifying XYZ Company of any discrepancies
- Notifying XYZ Company of any issues with delivery of printed reports

Control Objective #5: Payroll Output – Funds Transfer/Direct Deposit Files

Client management is responsible for:

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

Control Objective #8: Logical Security

Client management is responsible for:

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

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 XYZ Company in this Description, Ernst & Young considered the aspects of XYZ Company'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 XYZ Company and provided to user entities (if relevant and defined as part of the output control objectives), IPE used by XYZ Company management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

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

TRANSACTION PROCESSING CONTROL OBJECTIVES AND CONTROLS

Payroll Data Input

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.01	Client users require a valid user ID and password for authentication to the XYZ Company supplied Data Entry Systems.	Inspected the log in screen for each of the Data Entry Systems to determine whether a valid user ID and password were required for authentication to the systems. Observed an XYZ Company associate attempt to authenticate to a sample Data Entry System to determine whether a valid user ID and password were required to access the system.	No deviations noted No deviations noted
1.02	The XYZ Company Input Systems restrict erroneous data input and incomplete data from being entered through pre-formatted data entry screens.	Observed an XYZ Company associate attempt to submit incorrect/incomplete data (SSN, zip code, employee name, pay frequency) into each of the XYZ Company Input Systems and inspected the related error messages generated to determine whether pre-defined data validation rules are in place to detect and identify erroneous data input and incomplete data.	No deviations noted
1.03	Operators require a valid user ID and password to access the Key-Fast Input System to enter client provided data. In addition, operators authenticate the client contacts prior to inputting the client-provided payroll information into Key-Fast.	For a sample of days and clients, observed operators enter client payroll data into Key-Fast to determine whether they: • Authenticated to the Key-Fast system using a valid user ID and password; • Authenticated the client contact that provided the payroll data according to documented client specifications prior to input.	No deviations noted

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.04	Key-Fast restricts erroneous and incomplete data from being entered through pre-formatted data entry screens.	Observed an operator attempt to enter erroneous and incomplete data (invalid modifier, missing state tax code, invalid SSN, invalid file number) into the Key-Fast data entry screens on a sample day to determine whether the data was rejected and an error message was presented, and only valid and complete data was accepted.	No deviations noted
1.05	Prior to submitting the phone or fax payroll data entered for processing by the Application, operators compare control totals provided to data entered into the Key-Fast system. Out-of-balance conditions are corrected with the client.	For a sample of days and clients, inspected system records and payroll information provided by the client to determine whether the operator compared the control totals provided by the client to the control totals entered into the Key-Fast system and out-of-balance conditions were corrected with the client.	No deviations noted

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
1.06	Secure Socket Layer (SSL) technology with encryption is used to securely transmit payroll data entered from the Input Systems into the Application.	Observed an XYZ Company associate log into the application site for a sample Input System on a sample day to determine whether the sites use SSL technology with encryption. For a sample file from each of the Input Systems: • Inquired of a Principle Quality Assurance Engineer to determine whether SSL technology with encryption is used to securely transmit payroll data entered from the Input Systems into the Application; • Inspected a data string within the file to determine whether data is not presented in clear text.	No deviations noted No deviations noted
1.07	Data file transmissions between the Input Systems and the Application are monitored and identified issues, if any, are documented, reported, and followed up to resolution.	Observed XYZ Company personnel monitoring data file transmission alerts on a sample day to determine whether automated monitoring tools are used to monitor for issues or exceptions with data file transmissions between the Input Systems and the Application. For a sample of identified file transmission issues between the Input Systems and the Application, inspected the problem resolution record (Service Desk tickets, End of Night checklists, emails) to determine whether reported issues were documented and followed up through resolution in a timely manner.	No deviations noted No deviations noted

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

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

Deductions and Tax Withholdings Specifications

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

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

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
2.03	Statutory changes requiring coding modifications are coded by the appropriate development team and tested and certified for production release by the appropriate testing group. *Upon completion of testing, changes are deployed to production following the change management process outlined in Control Objective 6.*	For a sample of statutory changes that required coding modifications, inspected the testing results within the Change Management ticket to determine whether the change was tested and certified for production release by the appropriate testing group.	No deviations noted
2.04	Statutory changes that do not require coding modifications are applied to the STAT File database by appropriate STAT members.	Inspected the system-generated listing of user IDs with update privileges in the STAT File database and inquired of the Director Applications Development regarding the job responsibilities of the identified users to determine whether accounts were assigned to appropriate STAT members. For a sample of statutory changes applied to the database where no coding was required, inspected the STAT File database records to determine whether an authorized user applied the change.	No deviations noted No deviations noted

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

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

Payroll Processing

Control Objective 3: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored, and deviations are resolved and that payroll data is processed completely and accurately.

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

Control Objective 3: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored, and deviations are resolved and that payroll data is processed completely and accurately.

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

Control Objective 3: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored, and deviations are resolved and that payroll data is processed completely and accurately.

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

Control Objective 3: Controls provide reasonable assurance that processing of payroll information is completed according to schedule, monitored, and deviations are resolved and that payroll data is processed completely and accurately.

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

Payroll Output

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.01	Client output reports and data files are automatically generated from the Application upon completion of each payroll run.	For a sample test client in the Application production environment, executed a sample payroll run and inspected the following reports to determine whether the reports were automatically generated, transmitted and the payroll information (gross pay, net pay, taxes) was accurately and completely produced. Observed the data files being automatically generated from the Application for a sample of each of the following data files for a sample client and selected a transaction from each file and compared the payroll information (net pay amounts, control totals) from the file to amounts in the Application to determine whether the amounts were completely and accurately produced.	No deviations noted No deviations noted
4.02	Client output reports (e.g., payroll register) and other payroll-related data files are automatically transmitted and made available to clients through output reports and Input Systems (data files).	For a sample test client in the Application production environment, executed a sample payroll run and inspected the following output reports to determine whether the reports were automatically transmitted to and made available to clients. For a sample test client in the Application production environment, executed a sample payroll run and inspected the payroll-related data files to determine	No deviations noted No deviations noted

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
		whether the data files are automatically transmitted to the in-scope Input Systems.	
4.03	Data files and output report files are made available to clients and other XYZ Company systems using Secure Socket Layer (SSL) technology encryption to secure the transmission of payroll data.	Inspected a sample data file and output report file made available to clients and/or other XYZ Company systems to determine whether Secure Socket Layer (SSL) technology encryption was used during transmission. Inspected the XYZ Company Internet-based products to determine whether a valid password and ID was required for successful authentication and whether SSL technology encryption was in place to secure transmission of payroll data.	No deviations noted No deviations noted

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

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
4.04	The Corporate Systems Engineering group monitors the results of data files and output report file transmissions and is alerted of any identified issues or exceptions. Issues are documented, reported, and followed to resolution.	Observed a member of the Corporate Systems Engineering group monitoring data file transmission alerts on a sample day to determine whether automated monitoring tools are used to monitor for issues or exceptions with data file transmissions between the Input Systems and the Application. For a sample of identified transmission issues, inspected the related problem resolution tickets to determine whether monitoring was performed and identified transmission problems were documented and followed to resolution.	No deviations noted No deviations noted
4.05	For client output reports printed by XYZ Company, the Operations group monitors the transmissions of the output print files from the Application to the XYZ Company printers and is alerted of any identified issues or exceptions and those exceptions are followed up to resolution.	For a sample Region, observed a member of the Operations group monitoring the transmissions of output print files on a sample day to determine whether issues were documented and followed up to resolution.	No deviations noted
4.06	Production Support and Quality Control personnel review printed client-output reports and electronic media for defects.	For a sample Region, observed a Production Support and Quality Control associate review client-output reports and electronic media on a sample day to determine whether printing defects were identified and resolved.	No deviations noted
4.07	Print Operations Quality Control personnel are restricted from	Inspected the access rights screen within the Application for the Operations Quality	No deviations noted

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

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

Payroll Output – Funds Transfer/Direct Deposit Files

Control Objective 5: Controls provide reasonable assurance that transmissions of Funds Transfer files/direct deposit files from the Application to the XYZ Company systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

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

Control Objective 5: Controls provide reasonable assurance that transmissions of Funds Transfer files/direct deposit files from the Application to the XYZ Company systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

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

Control Objective 5: Controls provide reasonable assurance that transmissions of Funds Transfer files/direct deposit files from the Application to the XYZ Company systems or the clients' banks are authorized, completed according to schedule and deviations are identified and resolved.

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

GENERAL COMPUTER CONTROL OBJECTIVES AND CONTROLS

Application Development and Program Change Management

Control Objective 6: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Application (Mainframe)			
6.01	A formal and documented application development and change management policy has been developed for mainframe application development projects to guide the Development group.	Inspected the application development and change management policy documentation to determine whether development requirements were documented for mainframe application development projects to guide the Development group.	No deviations noted
6.02	Application change requests are formally documented and authorized by appropriate XYZ Company management personnel.	For a sample of months, inspected the Release Coordination Schedule for the major releases to the Application to determine whether the change request was documented and authorized by appropriate XYZ Company management. For a sample of minor changes made to the Application, inspected the Change Management ticket to determine whether the change request was documented and authorized by appropriate XYZ Company management.	No deviations noted No deviations noted

Control Objective 6: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
6.03	Changes to the Application are tested (unit, regression, and functional testing) in a segregated test environment and the results are approved by XYZ Company management prior to deployment.	For a sample of months, inspected test documentation for the major releases to the Application to determine whether testing was executed, and the test results were documented and approved by XYZ Company management prior to deployment. For a sample of minor changes made to the Application, inspected test documentation to determine whether testing was executed, and test results were documented and approved by XYZ Company management prior to deployment. Inspected the relevant application system configurations to determine whether separate development, test and production environments were established.	No deviations noted No deviations noted No deviations noted

Control Objective 6: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

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

Control Objective 6: Controls provide reasonable assurance that the implementation of and changes to application programs are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
Data Entry Systems			
6.06	Change requests to the Data Entry Systems are documented and authorized by appropriate product owners or business unit management personnel.	For a sample of changes made to the Data Entry Systems, inspected change documentation (emails, meeting minutes) to determine whether the change was authorized by appropriate XYZ Company management personnel.	No deviations noted
6.07	Changes to the Data Entry Systems are tested in a non-production environment by the development testers and iAT groups and approved by XYZ Company management prior to deployment.	For a sample of changes made to the Data Entry Systems, inspected change documentation (emails) to determine whether testing was performed by the development testers and iAT groups in a non-production environment and results are approved by XYZ Company management prior to deployment to production.	No deviations noted
6.08	Changes to the Data Entry Systems are approved for migration to the production environment by the project manager prior to deployment.	For a sample of changes made to the Data Entry Systems, inspected the change order to determine whether the change was approved by the project manager prior to deployment to production.	No deviations noted
6.09	Access to deploy changes to the Data Entry System production environment is restricted to properly authorized personnel based on job function.	Inspected the user access listings from each of the Data Entry Systems, inspected job titles, and inquired of the IT Compliance Manager to determine whether the assigned access to deploy changes to the production environment was restricted to appropriate personnel based upon job responsibilities.	No deviations noted

Operating Systems (OS) and Database Change Management

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

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

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

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

Logical Security

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.01	XYZ Company associates accessing the Data Entry Systems and Application are required to authenticate using a valid user ID and password compliant with XYZ Company's security policies and standards.	Inspected the relevant password configuration settings governing access to each of the Data Entry Systems, the Application and the documented Information Security Standards to determine whether password settings (history, length, expiration, complexity) comply with XYZ Company's security policies and standards. Observed an XYZ Company associate attempt to authenticate to a sample Data Entry System and the Application to determine whether a valid user ID and password was required to access the systems.	No deviations noted No deviations noted

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.02	Only appropriate IT personnel have access to the administrative functionality for the Data Entry Systems and Application and key mainframe datasets (specific to the Application).	Inspected the system-generated listings of users with access to the key mainframe datasets in the Application and inquired of Corporate Mainframe Security management regarding job responsibilities to determine whether access was restricted to authorized personnel. For a sample of users granted administrative level privileges to the Data Entry Systems, inspected job titles and inquired of XYZ Company management regarding the job responsibilities to determine whether access was restricted to authorized personnel.	No deviations noted No deviations noted

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.03	User access additions and modifications to the Data Entry Systems require authorization from appropriate XYZ Company management. Changes are documented and executed.	For a sample of user access additions and modifications: • Inspected the ticket to determine whether the request to grant access to the Data Entry Systems was documented and authorized by appropriate XYZ Company management. • Inspected system-generated user access listings from the Data Entry Systems to determine whether access was granted as requested.	No deviations noted

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.04	User access additions and modifications to the Application requires authorization from appropriate XYZ Company management. Changes are documented and executed.	For a sample of user access additions and modifications: • Inspected the ticket to determine whether the request to grant access to the Application was documented and authorized by appropriate XYZ Company management. • Inspected system-generated user access listings from the Application to determine whether access was granted as requested.	No deviations noted
8.05	User access deletions to the Data Entry Systems require authorization from appropriate XYZ Company management. Changes are documented and executed.	Inspected a screenshot of the configured job schedule and a sample termination email notification to determine whether a nightly job is scheduled to run automatically to remove terminated Active Directory users from the Data Entry Systems. For a sample of user terminations, inspected system-generated user access listings from the Data Entry Systems to determine whether access was revoked as requested.	No deviations noted No deviations noted

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

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

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

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

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

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

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

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

Control Objective 8: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Ref	*Description of Control Activity*	*Test of Controls*	*Results*
8.10	Auditing has been enabled at the application level for the in-scope Data Entry Systems. Transactional data is logged with the user ID of the person who initiated the transaction and is available for review.	Inspected the relevant configuration settings within the in-scope Data Entry Systems to determine whether auditing was enabled and transactional data was being logged and made available for review. Observed a Technical Services Manager log into a sample Data Entry System and make changes to a sample employee's compensation rate and effective date, and inspected the Employment Actions Audit Report and modification history screen within the Data Entry system to determine whether the employee compensation changes and the user ID of the operator who made the change were logged and available for review.	No deviations noted No deviations noted
8.11	Data Entry Systems provide the ability for clients to restrict user access based on roles and functions.	Inspected the relevant security screens for the in-scope Data Entry systems to determine whether the applications provide the ability for clients to manage user access based on roles and functions.	No deviations noted
8.12	Only authorized individuals have update access to the Data Entry systems production databases.	For a sample of production databases supporting the in-scope Data Entry Systems, inspected the system-generated listing of users with update access and inquired of XYZ Company Management to determine whether access was limited to authorized individuals based on job responsibilities.	No deviations noted

SECTION FIVE

OTHER INFORMATION PROVIDED BY XYZ COMPANY