A-LIGN

A-LIGN.com

Type 2 SOC 1

Prepared for:
ContinuumCloud

Year:
2025

ContinuumCloud

DATIS

Part of the ContinuumCloud

REPORT ON MANAGEMENT'S DESCRIPTION OF CONTINUUMCLOUD'S SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2

May 1, 2024 To April 30, 2025

Table of Contents

SECTION 1

ASSERTION OF CONTINUUMCLOUD’S MANAGEMENT

ASSERTION OF CONTINUUMCLOUD'S MANAGEMENT

July 17, 2025

We have prepared the description of ContinuumCloud, Inc.'s ('ContinuumCloud' or 'the Company') E3 Human Capital Management and Payroll SaaS System for issuing and maintaining HR software solutions entitled "Description of ContinuumCloud's E3 Human Capital Management and Payroll SaaS System" throughout the period May 1, 2024 to April 30, 2025, (description) for user entities of the system during some or all of the period May 1, 2024 to April 30, 2025, and their user 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 subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

ContinuumCloud uses Amazon Web Services ('AWS' or 'subservice organization') for cloud hosting services. The description includes only the control objectives and related controls of ContinuumCloud and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by ContinuumCloud in the description can be achieved only if complementary subservice organization controls assumed in the design of ContinuumCloud's controls are suitably designed and operating effectively, along with the related controls at ContinuumCloud. 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 ContinuumCloud 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 the E3 Human Capital Management and Payroll SaaS System made available to user entities of the system during some or all of the period May 1, 2024 to April 30, 2025, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      (1) the types of services provided including, as appropriate, the classes of transactions processed.

      (2) the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      (3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      (4) how the system captures significant events and conditions, other than transactions.

      (5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization’s controls.

(8) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. includes relevant details of changes to the service organization’s system during the period covered by the description.

iii. does not omit or distort information relevant to the scope of the E3 Human Capital Management and Payroll SaaS System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the E3 Human Capital Management and Payroll SaaS System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period May 1, 2024 to April 30, 2025, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of ContinuumCloud’s controls throughout the period May 1, 2024 to April 30, 2025. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. 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

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

Bob Bates

Bob Bates
CEO
ContinuumCloud, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ContinuumCloud

Scope

We have examined ContinuumCloud's description of its E3 Human Capital Management and Payroll SaaS System for issuing and maintaining HR software solutions entitled "Description of ContinuumCloud's E3 Human Capital Management and Payroll SaaS System" throughout the period May 1, 2024 to April 30, 2025, (description) and the suitability of the design and operating effectiveness of ContinuumCloud's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of ContinuumCloud's Management" (assertion). The controls and control objectives included in the description are those that management of ContinuumCloud believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the E3 Human Capital Management and Payroll SaaS system that are not likely to be relevant to user entities' internal control over financial reporting.

ContinuumCloud uses Amazon Web Services ('AWS' or 'subservice organization') for cloud hosting services. The description includes only the control objectives and related controls of ContinuumCloud and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by ContinuumCloud can be achieved only if complementary subservice organization controls assumed in the design of ContinuumCloud are suitably designed and operating effectively, along with the related controls at ContinuumCloud. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of ContinuumCloud'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 and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, ContinuumCloud has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ContinuumCloud is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the 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, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

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 to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination 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 stated in the description throughout the period May 1, 2024 to April 30, 2025. We believe that the evidence we 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 those controls to achieve the related control objectives stated in the description, 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 stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 errors or omissions 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 inadequate or fail.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in ContinuumCloud's assertion,

a. the description fairly presents the E3 Human Capital Management and Payroll SaaS System that was designed and implemented throughout the period May 1, 2024 to April 30, 2025.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2024 to April 30, 2025 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of ContinuumCloud's controls throughout the period May 1, 2024 to April 30, 2025.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period May 1, 2024 to April 30, 2025, if complementary subservice organization and user entity controls assume in the design of ContinuumCloud's controls operated effectively throughout the period May 1, 2024 to April 30, 2025.

The information in Section 5 of management's description of ContinuumCloud's system, "Other Information Provided by the Service Organization," that describes management's response to testing exceptions, is presented by management of ContinuumCloud to provide additional information and is not a part of ContinuumCloud's description of its system made available to user entities during the period May 1, 2024 to April 30, 2025. Information about ContinuumCloud's management's response to testing exceptions has not been subjected to the procedures applied in the 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 stated in the description of the system and, accordingly, we express no opinion on it.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of ContinuumCloud, user entities of ContinuumCloud's E3 Human Capital Management and Payroll SaaS System during some or all of the period May 1, 2024 to April 30, 2025, and the independent auditors of such user entities, who 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.

A-LIGN ASSURANCE

Tampa, Florida
July 17, 2025

SECTION 3

DESCRIPTION OF CONTINUUMCLOUD’S E3 HUMAN CAPITAL MANAGEMENT AND PAYROLL SAAS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

ContinuumCloud offers a spectrum of cloud-based software solutions intentionally designed to meet the unique needs of the behavioral health and human services industry. These solutions include a Human Capital Management (HCM), Payroll system (DATIS E3) and an Electronic Health Record (EHR) platform (Welligent). Through these offerings, ContinuumCloud empowers organizations to provide high-quality care and deliver on their mission.

Description of Services Provided

The DATIS E3 solution is a configurable platform that fully integrates both human resources and payroll data management functions. DATIS E3 provides comprehensive reporting and auditing capabilities.

DATIS E3 provides solutions for the entire employee lifecycle, including applicant tracking, onboarding, time and attendance and payroll modules.

The following are some of the features that support the human resources and payroll processing services:

- Human Resources
  - Electronics Employee File
  - Employee Portal
  - Company Asset Tracking
  - Compensation Management
  - Document Management
- Position Control
  - Visual Organization Chart
  - Budgeting
  - Position Reporting
- Recruiting
  - Electronic Job Postings and Career portals
  - Electronic Candidate Management
  - Applicant Tracking
- New Hire Onboarding
  - Complete electronic onboarding documentation
  - Paperless Onboarding
- Time and Attendance
  - Configurable Timesheets
  - Attendance Calendar
  - Leave and Absence Management
- Payroll
  - Comprehensive Payroll Processing
  - Direct Deposit
  - Tax Filing Services
  - W-2 Filing
- Benefits Administration
  - Configurable Benefit Enrollment
  - Affordable Care Act (ACA) Management
  - Carrier Feeds Integration for most benefit types
    - Medical, Dental, Vision
    - Flexible Spending Accounts
    - Retirement Savings Plans
    - Life Insurance and Accidental Death and Dismemberment (AD&D)

        - Health Savings Accounts
        - Consolidated Omnibus Budget Reconciliation Act (COBRA) Administrators
    - Employee and Manager Self-service
        - Paystubs and W-2
        - Timesheets
        - Performance Appraisals
        - Direct Deposit and W-4
        - Open Enrollment
    - Talent Management
        - Performance Appraisals
        - Credential Management
        - Learning Management
    - Comprehensive Reporting and Workflows
        - Standard Reports
        - Customer Report Writer
        - Workflow driven business process approvals

Transactions Processing and Reporting

ContinuumCloud has developed the E3 Human Capital Management and Payroll SaaS System to serve its customers. Clients access the application through a web browser to perform various human resource and payroll functions including:

- Applicant Screening
- New Hire Onboarding
- Time and Attendance
- Payroll, Benefits Administration
- Talent Management

Specific transaction processing items include the following:

1. *Payroll Processing* - Clients use E3 software to process payroll. ContinuumCloud's E3 proprietary payroll engine calculates gross wages, benefits, deductions, and taxes for net wages from time sheets electronically submitted by employees to managers and electronically approved by managers. Payroll administrators review and submit processed timesheets to payroll, and the payroll engine completes the gross to net calculation for employees. Client payroll administrators with appropriate security access review and approve payroll. Once approved by the client, payroll is finalized and is automatically processed without manual intervention. ContinuumCloud has established policies, procedures and segregation of duties for the packaging and handling of printed checks that are mailed to the clients. The tax and compliance department are physically segregated from other departments and a separate and secure processing room is access controlled and monitored.

2. *Bank Transaction Processing -* As part of the daily close procedures, ContinuumCloud tax and compliance employees launch an internal service process accessed through a secure internal website requiring login credentials and password to close banking. This is an automated process that allows ContinuumCloud employees to review banking impounds, taxes, liens, garnishments, money transfers and direct deposit transactions. Strict controls are in place to protect bank account information and detailed transaction information. Summary data is reviewed for variations, reasonableness checks and validated against payrolls processed for the day. Once the two-step review and approve procedure is completed, banking is approved through the secure internal website, which launches a second automated process of transmitting the files to the bank for processing. Policies, procedures and internal controls are in place to ensure the integrity and security of the banking process.
3. *Tax Processin*g - Tax Processing involves processing of federal, state and local taxes. When possible, tax payments and filings are completed electronically. Some state and local tax authorities do not have automated systems and may require paper check payments, which are automatically generated based on payment frequency. Tax filings are completed by a team of tax and payroll specialists based on the various local, state and federal requirements. The internal policies and procedures are designed to maintain filing and payment accuracy and timeliness. The team is supervised by the Manager of Tax and Compliance as well as the Chief Executive Officer with an Enrolled Agent certification.
4. *Benefit Carrier Feeds Processing -* As part of the services offered by ContinuumCloud, benefit carrier feeds processing is frequently selected by clients as an optional add-on service. ContinuumCloud offers carrier feeds to more than 80 different benefit carriers covering offerings such as medical, dental, vision, life, AD&D, retirement contribution and feedback files and COBRA notifications. This offering is sometimes subject to minimum plan participants and varies by carrier. File formats can be transmitted in a standard HIPAA 834 file format and non-HIPAA formats. These files are automatically created and transmitted to the carriers on a weekly basis. As part of the internal controls process, there is a schedule monitoring process and file completion audit process.

Significant Events

ContinuumCloud has implemented automated and manual procedures to capture and address significant events and conditions. The following are examples of the procedures ContinuumCloud has placed into operation:

- Automated alert notifications are utilized to notify operations personnel of file transmission errors
- Data validation checks are configured into the E3 Human Capital Management and Payroll SaaS System to restrict processing errors
- Bank reconciliation procedures are performed on a daily basis by the tax and compliance team. Those reconciliations are reviewed and approved by the Manager of Tax and Compliance
- ContinuumCloud utilizes AWS Infrastructure Security to provide a secure deployment of E3 application in the cloud. This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. AWS ensures that these controls are replicated in every new data center or service
- Enterprise monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations personnel when specific predefined thresholds are met

In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the E3 Human Capital Management and Payroll SaaS System. Please see the monitoring and risk assessment procedures described in the relevant sections of this report for further details.

Functional Areas of Operation

The ContinuumCloud staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specifications
- Quality assurance team - verifies that the system complies with the functional specifications through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Tax and Compliance - performs payroll processing, banking transaction processing, and tax processing to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Boundaries of the System

The scope of this report includes the E3 Human Capital Management and Payroll SaaS System performed in the Tampa, Florida facility.

This report does not include the cloud hosting services provided by AWS at the various facilities.

Subservice Organizations

AWS provides cloud hosting services for ContinuumCloud' E3 Human Capital Management and Payroll SaaS System.

Subservice Description of Services

AWS has provided flexible, scalable and secure IT infrastructure to businesses of any size around the world. With AWS, ContinuumCloud can deploy solutions on a cloud computing environment that provides compute power, storage, and other application services over the Internet. AWS affords the flexibility to employ the operating systems, application programs, and databases such as Amazon Elastic Cloud Compute (EC2) for Microsoft structured query language (SQL) Server, Application Servers and more. ContinuumCloud leverages a number of additional services from AWS including, but not limited to: CloudFront, CloudWatch, Lambda, Redshift, ElastiCache, Simple Storage Service (S3), Route 52, virtual private cloud (VPC). AWS builds a shared responsibility model between customers and AWS. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, ContinuumCloud assumes responsibility and management of the design, implementation and operation of the AWS environment.

Complementary Subservice Organization Controls

ContinuumCloud's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to ContinuumCloud's services to be solely achieved by ContinuumCloud control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of ContinuumCloud.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - AWS	
Control Objective	**Control**
Physical Security	Physical access to data centers is approved by an authorized individual.
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
	Physical access points to server locations are managed by electronic access control devices.
	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Environmental Safeguards	Amazon-owned data centers are protected by fire detection and suppression systems.
	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
	AWS performs reviews of colocation service providers to validate adherence with AWS security and operational standards.
	S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
	When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
	Objects are stored redundantly across multiple fault-isolated facilities.
	The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.

Subservice Organization - AWS	
Control Objective	**Control**
	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
	Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
	Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

ContinuumCloud management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements (SLAs). In addition, ContinuumCloud performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

CONTROL ENVIRONMENT

The control environment at ContinuumCloud is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ContinuumCloud's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ContinuumCloud's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel.
- The employee manual contains organizational policy statements and codes of conduct to which employees are required to adhere.
- Employees are required to sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees are required to complete a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.

- Criminal background checks are performed for employee candidates as a component of the hiring process.

Commitment to Competence

ContinuumCloud's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

ContinuumCloud's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is annually briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

ContinuumCloud's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ContinuumCloud's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

ContinuumCloud's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. ContinuumCloud's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation upon hire.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT

ContinuumCloud's risk assessment process identifies and manages risks that could potentially affect ContinuumCloud's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ContinuumCloud identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Risk Identification

ContinuumCloud has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Key members of the management and operational teams meet on a regular basis to identify and review risks to the system. Management considers risks that can arise from both external and internal factors including:

External Factors:

- Technological dependencies from vendors could become unavailable, resulting in the inability to provide payroll processing services or the need to make changes to the payroll system or application provider
- Changing customer needs or expectations that could affect product development, production process, customer service, or pricing
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in operating policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems and highlight the need for contingency planning
- Economic changes that could have an impact on decisions related to financing, capital expenditures and expansion

Internal Factors:

- A disruption in information systems processing that could adversely affect the entity's operations
- The quality of personnel hired and methods of training and motivation that could influence the level of control consciousness within the entity
- A change in management responsibilities that could affect the way certain controls are affected
- The nature of the entity's activities, and employee accessibility to assets, that could contribute to misappropriation of resources

The ContinuumCloud risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. ContinuumCloud management oversees risk management ownership and accountability as well as risk identification. Management identifies elements of business risk including threats, vulnerabilities, safeguards and the likelihood of a threat, to determine the actions to be taken.

Risks Analysis

ContinuumCloud risk analysis methodology varies due to the wide variety of risks and difficulty in quantifying risks. However, the risk analysis process includes the following:

- Estimating the significance of a risk.
- Assessing the likelihood (or frequency) of the risk occurring.
- Considering how the risk should be managed via risk acceptance or mitigation by implementation of control activities.

Risk analysis is an essential process to the entity’s success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk.

Necessary actions are taken to reduce the significance or likelihood of the risk occurring and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Control Objectives and Related Control Activities section below.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ContinuumCloud systems; as well as the nature of the components of the system result in risks that the criteria will not be met. ContinuumCloud addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ContinuumCloud’s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which ContinuumCloud strives to achieve its business objectives. ContinuumCloud has applied a risk management approach to the organization in order to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

ContinuumCloud’s control objectives and related control activities are included in Section 4 (the “Testing Matrices”) of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of ContinuumCloud’s description of the E3 Human Capital Management and Payroll SaaS System.

The description of the service auditor’s tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization’s description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to consider whether they are operating as intended and that the controls are modified for changes in conditions. ContinuumCloud management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policy and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Management's close involvement in ContinuumCloud operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any controls weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to help ensure legal compliance and to maximize the performance of ContinuumCloud personnel.

On-Going Monitoring

ContinuumCloud performs ongoing monitor to help ensure that business systems operate effectively on a continuous basis.

Aspects of the ongoing monitoring procedures include the following:

- In carrying out its regular management activities, operations management obtains evidence that the system of internal control continues to function, including error and performance reports.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- The information technology department performs data restorations on a daily basis to help ensure that system components can be recovered from backup media.
- The information technology department utilizes monitoring applications to monitor systems availability and performance metrics.
- The cloud-based hosting and managed services provided by AWS are monitored on a regular basis as part of the day-to-day information technology and business operations.

Vendor Management

ContinuumCloud has defined the following activities to oversee controls performed by vendors that could impact the E3 Human Capital Management and Payroll SaaS System:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Reporting Deficiencies

Deficiencies in an entity's internal control system surface from many sources, including ContinuumCloud's ongoing monitoring procedures. Management has developed protocols to help ensure that findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in ContinuumCloud's procedures or personnel.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

The E3 application provides a web interface for clients to review, approve and submit payroll for processing by the application. Payroll processing rules determine if the submitted files meet client-specific standards for validation. Core functionality of the E3 application provides customers with:

- Flexibility to custom configure their data management
- Constant access to their data
- The ability to update and retrieve historical data and re-run prior feeds
- Comprehensive reporting capabilities
- A user-friendly interface that is intuitive to navigate
- Automated features that reduce keystroke time and errors
- Continuous feature enhancements sent free each month
- Software requiring little or no training to get started
- Responsive and professional service and support

Production systems supporting the E3 application are maintained at the AWS third-party data center facility. Backup and redundant systems are maintained within in the AWS infrastructure. Communications with the E3 web server interface is encrypted using the secure socket layer (SSL) protocol. The E3 application operates on a Windows platform and is supported by a SQL server backend database.

Infrastructure

Primary infrastructure used to provide ContinuumCloud's E3 Human Capital Management and Payroll SaaS System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Third-party Infrastructure Hosting Services	Provides Database, Application Servers, Load Balancing and Storage

Software

Primary software used to provide ContinuumCloud's E3 Human Capital Management and Payroll SaaS System includes the following:

Primary Software	
Software	**Purpose**
Microsoft SQL Server	Provides underlying database for customer tenants
Salesforce Service Cloud	Provides support ticketing functionality to document and track issues and requests for the client environment
Gitlab	Gitlab is a software development life cycle (SDLC) tool for source control, project management, bug tracking, QA, continuous integration and release management
Cloudberry	Performs scheduled backups of client data according to requirements and provides status alerts to operations personnel

Communication Systems

ContinuumCloud utilizes several methods of communication to ensure its employees understand their roles and responsibilities, and to provide management and control over its operations. Communication exists throughout the ContinuumCloud organization via multiple communication paths to help ensure that significant events are communicated and resolved. These include voice-mail, e-mail, and regularly scheduled meetings.

COMPLEMENTARY USER ENTITY CONTROLS

ContinuumCloud's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to ContinuumCloud's services to be solely achieved by ContinuumCloud control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ContinuumCloud's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Control Objective 1

1. User entities are responsible for validating changes that affect payroll calculations.

Control Objective 7

1. User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with ContinuumCloud's systems.
2. User entities are responsible for immediately notifying ContinuumCloud of any actual or suspected information security breaches, including compromised user accounts.
3. User entities are responsible for notifying ContinuumCloud of any changes to user account access.
4. User entities are responsible for safeguarding the security of their systems that could affect the ContinuumCloud's SaaS solution.

Control Objective 9

1. User entities are responsible for ensuring that payroll calculations are accurate prior to signing off on the application setup process.
2. User entities are responsible for understanding and complying with their contractual obligations to ContinuumCloud.

SECTION 4

DESCRIPTION OF CONTINUUMCLOUD’S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

GUIDANCE REGARDING DESCRIPTION OF CONTINUUMCLOUD'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN ASSURANCE's examination of the controls of ContinuumCloud was limited to the control objectives and related control activities specified by the management of ContinuumCloud and did not encompass all aspects of ContinuumCloud's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions
- Understand the flow of significant transactions through the service organization
- Determine whether the control objectives are relevant to the user organization's financial statement assertions
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented

CONTROL AREA 1 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization

Control activities provide reasonable assurance that new development or changes to existing applications, system software, and infrastructure are authorized, tested, approved, properly implemented, and documented.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes.	Inspected the supporting release tickets for a sample of application releases to determine that a ticketing system was utilized to document the change control procedures for changes in the application and implementation of new changes.	No exceptions noted.
1.2	Changes to the production environment are automatically moved to the staging area to wait for approval prior to migration to the production environment.	Inspected the release documentation for a sample of application releases to determine that changes to the production environment were automatically moved to the staging area to wait for approval prior to migration to the production environment.	No exceptions noted.
1.3	Quality assurance testing and management approvals are required for production releases.	Inspected the release documentation for a sample of application releases to determine that quality assurance testing and management approvals were required for production releases.	No exceptions noted.
1.4	The ability to migrate application changes to the production environment is restricted to authorized personnel.	Inquired of the Senior Applications Development Director regarding users with access to push changes to production to determine that the ability to migrate application changes to the production environment was restricted to authorized personnel.	No exceptions noted.
		Inspected the list of users with the ability to migrate changes to determine that the ability to migrate application changes to the production environment was restricted to authorized personnel.	No exceptions noted.
1.5	The application development, testing, and production environments are logically separated from each other.	Inspected the separate environments to determine that the application development, testing, and production environments were logically separated from each other.	No exceptions noted.

CONTROL AREA 1 **APPLICATION DEVELOPMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development or changes to existing applications, system software, and infrastructure are authorized, tested, approved, properly implemented, and documented.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.6	Users with write access to the version control software, enabling them to make changes to the source code is restricted to authorized members of the development team.	Inquired of the Senior Applications Development Director regarding version control access to determine that users with write access to the version control software, enabling them to make changes to the source code was restricted to authorized members of the development team.	No exceptions noted.
		Inspected the version control system user listing to determine that users with write access to the version control software, enabling them to make changes to the source code was restricted to authorized members of the development team.	No exceptions noted.
1.7	Version control software is used to track changes to the source code resulting in the creation of a new version of source code.	Inquired of the Senior Applications Development Director regarding version control to determine that version control software was used to track changes to the source code resulting in the creation of a new version of source code.	No exceptions noted.
		Inspected the version control software dashboard to determine that version control software was used to track changes to the source code resulting in the creation of a new version of source code.	No exceptions noted.
1.8	Version control software is utilized to track the history of source code being checked in and out.	Inquired of the Senior Applications Development Director regarding version control to determine that version control software was utilized to track the history of source code being checked in and out.	No exceptions noted.
		Inspected the version control software dashboard to determine that version control software was utilized to track the history of source code being checked in and out.	No exceptions noted.

CONTROL AREA 1 **APPLICATION DEVELOPMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development or changes to existing applications, system software, and infrastructure are authorized, tested, approved, properly implemented, and documented.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	A code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that s code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
1.10	The code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
1.11	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
1.12	The change management process has defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	No exceptions noted.
1.13	Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the code repository to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
1.14	Security patches follow the standard change management process.	Inspected the patch management policies and procedures to determine that security patches follow the standard patch management process.	No exceptions noted.

CONTROL AREA 1 **APPLICATION DEVELOPMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development or changes to existing applications, system software, and infrastructure are authorized, tested, approved, properly implemented, and documented.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.15	Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the rollback capabilities to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	No exceptions noted.

CONTROL AREA 2 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that policies and procedures are in place to govern the Human Resource practices of the organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Core values are communicated from executive management to personnel through policies, procedures and the employee handbook including the code of conduct.	Inspected the employee handbook, information security policies and procedures and the entity's SharePoint to determine that core values were communicated from executive management to personnel through policies, procedures and the employee handbook including the code of conduct.	No exceptions noted.
2.2	An employee handbook including the code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook including the code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
2.3	Upon hire, personnel are required to acknowledge the employee handbook including the code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook including the code of conduct.	No exceptions noted.
2.4	Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
2.5	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation tracking spreadsheet for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
2.6	Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
2.7	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

CONTROL AREA 2 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that policies and procedures are in place to govern the Human Resource practices of the organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.8	The organizational chart is updated on a real-time basis via the entity's human resources software, and updates to the organizational structure and lines of reporting are made as necessary.	Inspected the organizational chart to determine that the organizational chart was updated on a real-time basis via the entity's human resources software, and updates to the organizational structure and lines of reporting were made as necessary.	No exceptions noted.
2.9	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
2.10	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
2.11	The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
2.12	The entity provides training programs for employees that relate to job roles and responsibilities, technical competencies, and continuing professional education.	Inspected the training tracker to determine that the entity provided training programs for employees that related to job roles and responsibilities, technical competencies, and continuing professional education.	No exceptions noted.
2.13	Upon hire, personnel are required to complete information security awareness training.	Inquired of the Security and compliance specialist regarding the information security training to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Inspected the security and compliance training policy to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.

CONTROL AREA 2 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that policies and procedures are in place to govern the Human Resource practices of the organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security awareness training tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	Testing of the control activity disclosed that information security and awareness training was not completed for three of five new hires sampled. Subsequent testing of the control activity disclosed that information and security and awareness training was completed by the three samples after the deadline.
2.14	Current employees are required to complete information security awareness training annually.	Inquired of the Security and compliance specialist regarding the information security training to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Inspected the security and compliance training policy to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Inspected the information security awareness training tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	Testing of the control activity disclosed that the information security and awareness training was not completed annually for nine of 12 current employees sampled. Subsequent testing of the control activity disclosed that security and awareness training was completed by the nine samples after the deadline.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software settings, the code repository configurations, the WAF configurations, and the production firewall rulesets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
3.2	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery, incident response, and business continuity program to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
3.3	Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
3.4	Web application firewalls (WAFs) are established to monitor and filter HyperText Transfer Protocol (HTTP) traffic between all applications and the Internet to help prevent malicious activities.	Inspected the WAFs configurations to determine that WAFs were established to monitor and filter HTTP traffic between all applications and the Internet to help prevent malicious activities.	No exceptions noted.
3.5	The WAF is configured to monitor and alert on suspicious activity.	Inspected the WAF configurations and the supporting change ticket for an example notification from the WAF to determine that the WAF was configured to monitor and alert on suspicious activity.	No exceptions noted.
3.6	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.7	The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configurations for a sample of workstations and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
3.8	The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus software configurations for a sample of workstations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
3.9	The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the code repository and an example WAF alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
3.10	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
3.11	The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
3.12	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Security and Compliance Specialist regarding their processes for documenting and tracking incidents in the ticketing system to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the disaster recovery, incident response, and business continuity program to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that there were no incidents during the review period.
3.13	A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery, incident response, and business continuity program to determine that a business continuity and disaster recovery plan were documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.

CONTROL AREA 4 COMPUTER OPERATIONS - BACKUP

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that timely system backups of critical files to an off-site location are performed.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Backup policies and procedures are in place to guide personnel in the event of an incident.	Inspected the backup and recovery policy to determine that backup policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
4.2	Restore tests are configured to be performed on backed up data at least daily to test the viability of the backup.	Inquired of the Senior Director, IT and Operations regarding restoration tests to determine that restore tests were configured to be performed on backed up data on a daily basis to test the viability of the backup.	No exceptions noted.
		Inspected the backup restoration configurations and daily system restoration logs and the restoration test results to determine that restore tests were configured to be performed on backed up data on a daily basis to test the viability of the backup.	No exceptions noted.
4.3	The backup software system is configured to perform daily and weekly backups of critical systems and files.	Inquired of the Senior Director, IT and Operations regarding backups of critical systems and files to determine that the backup software system was configured to perform daily and weekly backups of critical systems and files.	No exceptions noted.
		Inspected the backup configuration schedule and an example backup log to determine that the backup software system was configured to perform daily and weekly backups of critical systems and files.	No exceptions noted.
4.4	Access to modify backups is restricted to appropriate personnel.	Inquired of the Senior Director, IT and Operations regarding access to modify backups to determine that access to modify backups was restricted to appropriate personnel.	No exceptions noted.
		Inspected the backup access user listing to determine that access to modify backups was restricted to appropriate personnel.	No exceptions noted.
4.5	System data is encrypted during the replication process between cloud environments.	Inspected the backup replication configurations to determine that system data was encrypted during the replication process between cloud environments.	No exceptions noted.

CONTROL AREA 4 **COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that timely system backups of critical files to an off-site location are performed.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.6	The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding recalling backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		Inspected the listing of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
4.7	Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
4.8	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
4.9	When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inquired of the Security and compliance specialist regarding backup failures to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Inspected the backup policies to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	Testing of the control activity disclosed that there were no failed backups during the review period.

CONTROL AREA 4 **COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that timely system backups of critical files to an off-site location are performed.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.10	Production data is backed up and replicated to an offsite facility daily.	Inspected the backup replication configurations to determine that production data was backed up and replicated to an offsite facility daily.	No exceptions noted.

CONTROL AREA 5 COMPUTER OPERATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that application and data files for the payroll processing systems are backed up in a timely manner and securely stored.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	A centralized ticketing system is utilized to document and manage client support requests.	Inspected the ticket system dashboard to determine that a centralized ticketing system was utilized to document and manage client support requests.	No exceptions noted.
5.2	A disk space monitoring application is utilized to notify personnel via onscreen and e-mail alerts when disk space metrics reach a pre-defined threshold.	Inquired of the Senior Director, IT and Operations regarding monitoring notifications to determine that a disk space monitoring application was utilized to notify personnel via onscreen and e-mail alerts when disk space metrics reached a pre-defined threshold.	No exceptions noted.
		Inspected the server alert configurations and an example disk space alert to determine that a disk space monitoring application was utilized to notify personnel via onscreen and e-mail alerts when disk space metrics reached a pre-defined threshold.	No exceptions noted.
5.3	Application and data files for the payroll processing systems are backed up in a timely manner and securely stored.	Inquired of the Senior Director, IT and Operations regarding rollback functionality to determine that application and data files for the payroll processing systems were backed up in a timely manner and securely stored.	No exceptions noted.
		Inspected the client backup guide, the backup configuration schedule and an example completed backup log to determine that application and data files for the payroll processing systems were backed up in a timely manner and securely stored.	No exceptions noted.
5.4	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus scan configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.

CONTROL AREA 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that application and data files for the payroll processing systems are backed up in a timely manner and securely stored.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.5	The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
5.6	The antivirus software is configured to scan workstations weekly.	Inspected the centralized antivirus software configurations to determine that the antivirus software was configured to scan workstations weekly.	No exceptions noted.

CONTROL AREA 6 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Customer web sessions are encrypted using SSL.	Inspected the SSL certificates to determine that customer web sessions were encrypted using SSL.	No exceptions noted.
6.2	Inbound internet traffic terminates at a host in the demilitarized zone (DMZ) that is separate from the internal network.	Inquired of the Senior Director, IT and Operations regarding network isolation to determine that inbound internet traffic terminated at a host in the DMZ that was separate from the internal network.	No exceptions noted.
		Inspected the network diagram, the DMZ, and the server security group rules to determine that inbound internet traffic terminated at a host in the DMZ that was separate from the internal network.	No exceptions noted.
6.3	The ability to administer the firewall system is restricted to user accounts accessible by the authorized personnel.	Inquired of the Senior Director, IT and Operations regarding firewall administration access to determine that the ability to administer the firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the firewall administrator listing to determine that the ability to administer the firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
6.4	The firewall system requires administrators to authenticate with a user account, password, and multi-factor authentication (MFA) before being granted access to the firewall system.	Inquired of the Senior Director, IT and Operations regarding firewall authentication to determine that the firewall system required administrators to authenticate with a user account, password, and MFA before being granted access to the firewall system.	No exceptions noted.
		Observed the firewall authentication process to determine that the firewall system required administrators to authenticate with a user account, password, and MFA before being granted access to the firewall system.	No exceptions noted.

CONTROL AREA 6 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the firewall system authentication configurations to determine that the firewall system required administrators to authenticate with a user account, password, and MFA before being granted access to the firewall system.	No exceptions noted.
6.5	Vulnerability scans are performed weekly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results for a sample of weeks and the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans to determine that vulnerability scans were performed weekly and remedial actions were taken where necessary.	No exceptions noted.
6.6	The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the network diagram, the production firewall rulesets, the Network Address Translation (NAT) configurations and the DMZ configurations to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
6.7	Server certificate-based authentication is used as part of the SSL / Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
6.8	Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Senior Director, IT and Operations regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.

CONTROL AREA 6 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.9	NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
6.10	Virtual private network (VPN), SSL/TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL/TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
6.11	Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
6.12	Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
6.13	A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and the firewall rulesets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
6.14	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and the firewall rulesets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

CONTROL AREA 6 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization

Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.15	WAFs are established to monitor and filter HTTP traffic between all applications and the Internet to help prevent malicious activities.	Inspected the WAFs configurations to determine that WAFs were established to monitor and filter HTTP traffic between all applications and the Internet to help prevent malicious activities.	No exceptions noted.
6.16	The WAF is configured to monitor and alert on suspicious activity.	Inspected the WAF configurations and the supporting change ticket for an example notification from the WAF to determine that the WAF was configured to monitor and alert on suspicious activity.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	Administrator rights within the E3 application are restricted to authorized users.	Inquired of the Senior Director, IT and Operations regarding application administrative privileges to determine that admin rights within the E3 application were restricted to authorized users.	No exceptions noted.
		Inspected the E3 administrator listing to determine that administrator rights within the E3 application were restricted to authorized users.	No exceptions noted.
7.2	Database passwords are encrypted and the login flow restricts customers to their information only.	Inquired of the Senior Director, IT and Operations regarding database authentication encryption to determine that database passwords were encrypted and the login flow restricted customers to their information only.	No exceptions noted.
		Inspected the database password configuration to determine that database passwords were encrypted and the login flow restricted customers to their information only.	No exceptions noted.
7.3	The application is configured to authenticate users via user account and password before granting access to the application and the password must meet the following requirements: • Minimum length • Maximum length • Special characters • Numbers	Inspected the application password configurations to determine that the application was configured to authenticate users via user account and password before granting access to the application and the password must meet the following requirements: • Minimum length • Maximum length • Special characters • Numbers	No exceptions noted.
7.4	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.5	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
7.6	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
7.7	Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
7.8	Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director, IT and Operations regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
7.9	Network administrative access is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding administrative access to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.10	Network users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the network to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Inspected the network user listing and password configurations to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
7.11	The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
7.12	Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.13	Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
7.14	Network audit logs are maintained for review when needed.	Inquired of the Senior Director, IT and Operations regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
7.15	Production server user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director, IT and Operations regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the production server user listing and access roles for a sample of production servers to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

CONTROL AREA 7	**INFORMATION SECURITY**
Control Objective Specified by the Service Organization	Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.16	Production server administrative access is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding administrative access to determine that production server administrative access was restricted to authorized personnel.	No exceptions noted.
		Inspected the production server administrator listing and access roles for a sample of production servers to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.
7.17	Production server users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the production servers to determine that production server users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Inspected the production server user listings and password configurations for a sample of production servers to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
7.18	Production servers are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the password configurations for a sample of production servers to determine that the production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.19	Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the account lockout configurations for a sample of production servers to determine that production server account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
7.20	Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the audit logging configurations for a sample of production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
7.21	Production server audit logs are maintained for review when needed.	Inquired of the Senior Director, IT and Operations regarding production server audit logs to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Inspected the example production server audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.22	Production database user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director, IT and Operations regarding production database access to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the user listing and access roles for a sample of production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
7.23	Production database administrative access is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding administrative access to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
		Inspected the production database administrator listing and access roles for a sample of production databases to determine that production databases administrative access was restricted to authorized personnel.	No exceptions noted.
7.24	Production database users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the production databases to determine that production database users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Inspected the production database user listings and password configurations for a sample of production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

CONTROL AREA 7 INFORMATION SECURITY

Control Objective Specified by the Service Organization

Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.25	Production databases are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the password configurations for a sample of production databases to determine that production databases were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
7.26	Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the account lockout configurations for a sample of production databases to determine that operating system account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
7.27	Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
7.28	Production database audit logs are maintained for review when needed.	Inquired of the Senior Director, IT and Operations regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed.	No exceptions noted.
		Inspected an example production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.29	Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director, IT and Operations regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
7.30	Production application administrative access is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding administrative access to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
		Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
7.31	Production application users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the production application to determine that production application users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
7.32	Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.33	Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
7.34	Production application audit logs are maintained for review when needed.	Inquired of the Senior Director, IT and Operations regarding application audit logs to determine that application audit logs were maintained for review when needed.	No exceptions noted.
		Inspected the example production application audit log extract to determine that production application audit logs were maintained for review when needed.	No exceptions noted.
7.35	VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director, IT and Operations regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
7.36	The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
7.37	Users are authenticated via MFA prior to being granted remote access to the environment.	Observed a user access the in-scope environment remotely to determine that users authenticated via MFA prior to being granted remote access to the environment.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the VPN authentication settings to determine that users authenticated via MFA prior to being granted remote access to the environment.	No exceptions noted.
7.38	Passwords and production data is stored in an encrypted format using software supporting the Advanced Encryption Standard (AES).	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
7.39	Logical access reviews are performed quarterly.	Inquired of the Security and Compliance Specialist regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
		Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.
7.40	Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Security and Compliance specialist regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
7.41	Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Security and Compliance Specialist regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the termination procedures, the in-scope user listings, and the supporting user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
7.42	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
7.43	Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Director, IT and Operations regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

CONTROL AREA 8 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	This control objective is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

CONTROL AREA 9 **NEW CUSTOMER SETUP**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new clients are set up in an accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Contracts are in place with customers that define the terms of services provided. The contracts include, but are not limited to, the following: • Nature, timing, and extent of services provided • Customer support and training • Roles and responsibilities • SLAs	Inspected the executed contracts for a sample of customers to determine that contracts were in place with customers that defined the terms of services provided and that the contracts included, but were not limited to, the following: • Nature, timing, and extent of services provided • Customer support and training • Roles and responsibilities • SLAs	No exceptions noted.
9.2	Documented project plans are in place to guide the setup and installation of new customer implementations.	Inquired of the Billing Analyst regarding documented project plans for new customers to determine that documented project plans were in place to guide the setup and installation of new customer implementations.	No exceptions noted.
		Inspected the documented project plans for a sample of customers to determine that documented project plans were in place to guide the setup and installation of new customer implementations.	No exceptions noted.
9.3	New customer invoices for the final build are required before implementation.	Inquired of the Billing Analyst regarding new customer invoices for the final build to determine that new customer invoices for the final build were required before implementation.	No exceptions noted.
		Inspected the new customer invoice for a sample of customers to determine that new customer invoices for the final build were required before implementation.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT’S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management’s Response
2.13	Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	Testing of the control activity disclosed that information security and awareness training was not completed for three of five new hires sampled. Subsequent testing of the control activity disclosed that information and security and awareness training was completed by the three samples after the deadline.	We acknowledge that we did not consistently repeat the training annually as outlined in our policy. We have identified this as a compliance gap and are implementing a formal, recurring training program with system-generated reminders and tracking to ensure annual completion going forward. It's important to note that during the period in which annual training was not repeated, we did not experience any security incidents or breaches related to employee behavior. Nonetheless, we recognize the importance of ongoing training and are taking proactive steps to prevent future gaps.
2.14	Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	Testing of the control activity disclosed that the information security and awareness training was not completed annually for nine of 12 current employees sampled. Subsequent testing of the control activity disclosed that security and awareness training was completed by the nine samples after the deadline.	