System and Organization Controls 2 (SOC 2) Type 2

Report on controls placed in operation at WMBE Payrolling Inc. dba TCWGlobal relevant to Security, Confidentiality, and Processing Integrity and the suitability of the design and operating effectiveness of its controls

For the Period March 1, 2023 to February 29, 2024

TABLE OF CONTENTS

SECTION ONE

Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of WMBE Payrolling Inc. dba TCWGlobal
San Diego, CA

Scope

We have examined WMBE Payrolling Inc. dba TCWGlobal's ("Service Organization" or TCWGlobal") accompanying description of its StaffingNation and Payroll Services System found in Section 3 titled "WMBE Payrolling Inc. dba TCWGlobal's Description of its StaffingNation and Payroll Services System" throughout the period March 1, 2023 to February 29, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that TCWGlobal's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Processing Integrity (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

TCWGlobal uses subservice organizations to supplement its services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TCWGlobal, to achieve TCWGlobal's service commitments and system requirements based on the applicable trust services criteria. The description presents TCWGlobal's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TCWGlobal's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TCWGlobal, to achieve TCWGlobal's service commitments and system requirements based on the applicable trust services criteria. The description presents TCWGlobal's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TCWGlobal's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

TCWGlobal is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TCWGlobal's service commitments and system requirements were achieved. In Section 2, TCWGlobal has provided the accompanying assertion titled, "Assertion of WMBE Payrolling Inc. dba TCWGlobal Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. TCWGlobal is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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 report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects:

a. The description presents TCWGlobal's StaffingNation and Payroll Services System that was designed and implemented throughout the period March 1, 2023 to February 29, 2024 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that TCWGlobal's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of TCWGlobal's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that TCWGlobal's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TCWGlobal's controls operated effectively throughout that period.

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 TCWGlobal, user entities of TCWGlobal's StaffingNation and Payroll Services System during some or all of the period March 1, 2023 to February 29, 2024, business partners of TCWGlobal subject to risks arising from interactions with the StaffingNation and Payroll Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than the specified parties.

CyberGuard Compliance, LLP

Las Vegas, NV

April 15, 2024

SECTION TWO

Assertion of WMBE Payrolling Inc. dba TCWGlobal Management

ASSERTION OF WMBE PAYROLLING INC. DBA TCWGLOBAL MANAGEMENT

April 15, 2024

Scope

We have prepared the accompanying description of WMBE Payrolling Inc. dba TCWGlobal's ("Service Organization" or "TCWGlobal") StaffingNation and Payroll Services System titled "WMBE Payrolling Inc. dba TCWGlobal's Description of its StaffingNation and Payroll Services System" throughout the period March 1, 2023 to February 29, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the StaffingNation and Payroll Services System that may be useful when assessing the risks arising from interactions with TCWGlobal's system, particularly information about system controls that TCWGlobal has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Processing Integrity (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

TCWGlobal uses subservice organizations to supplement its services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TCWGlobal, to achieve TCWGlobal's service commitments and system requirements based on the applicable trust services criteria. The description presents TCWGlobal's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TCWGlobal's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TCWGlobal, to achieve TCWGlobal's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents TCWGlobal's StaffingNation and Payroll Services System that was designed and implemented throughout the period March 1, 2023 to February 29, 2024 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that TCWGlobal's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of TCWGlobal's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that TCWGlobal's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TCWGlobal's controls operated effectively throughout that period.

WMBE Payrolling Inc. dba TCWGlobal

SECTION THREE

WMBE Payrolling Inc. dba TCWGlobal's Description of its StaffingNation and Payroll Services System

WMBE PAYROLLING INC. DBA TCWGLOBAL'S DESCRIPTION OF ITS STAFFINGNATION AND PAYROLL SERVICES SYSTEM

1. Overview of WMBE Payrolling Inc. dba TCWGlobal's Operations

Company Background

WMBE Payrolling Inc. dba TCWGlobal ("TCWGlobal") is a dynamic business with a team of experienced HR professionals offering payrolling, staffing, pre-screening, MSP/VMS, and international HR services for temporary workers and contractors. TCWGlobal's dedication to excellence and focus on client needs enables their clients to effectively achieve their workforce goals.

Description of Services Provided

Global Payrolling

TCWGlobal provides global payrolling (employer of record) services to companies around the world. As the employer of record, TCWGlobal manages and holds the liability for the contingent workforce; workers compensation, unemployment claims, insurance coverage, benefits, timekeeping, tax withholdings, employment contacts and other client specific and tax reporting.

Managed Service Provider (MSP) Services

TCWGlobal offers a variety of MSP services to help companies effectively manage their contingent workforce and staffing vendors. Depending on each company's unique needs, TCWGlobal offers a variety of services to streamline, simplify and manage their contingent workforce lifecycle from requisition to payment, and all processes in between. In addition, as an MSP, TCWGlobal owns the management of all staffing vendors, while remaining vendor neutral to ensure clients receive the best talent. TCWGlobal's MSP services help clients remain compliant with all labor regulations and government requirements.

Contingent Workforce Management Platform/VMS System

TCWGlobal's global enterprise cloud software, StaffingNation, enables companies to oversee and manage their contingent workforce needs with ease, flexibility, and compliance assurance, while automating their workflow.

Pre-Screening

Pre-Employment Screening/Background Checks is another service offered to mitigate risk and exposure to client's information and assets. By utilizing TCWGlobal's in-house pre-screening department, its customers can make fully informed hiring decisions with rapid turn-around time needed when hiring temporary and contract workers. From criminal background checks and drug screening to driving records and credit reports, services can be customized to suit various budgets and hiring requirements.

International Services

TCWGlobal's services for managing its United States contingent workforce are also available overseas and is processed at the global headquarters in San Diego, CA. TCWGlobal provides local customer service to clients while their established partners in various countries provide local customer service to the employees. A dedicated team of international HR professionals and worldwide employment lawyers are available to answer international payrolling questions with an in-depth knowledge of countries' employment laws and standard business practices. As with US payrolling, TCWGlobal or its local partner becomes the legal employer for the overseas workers and manages all hiring, benefits, legal regulations, and employment contracts.

Staffing

TCWGlobal's full-service staffing and recruiting department utilizes innovative strategies to ensure client companies are exposed to top-tier talent. TCWGlobal's recruiters customize a full package to meet client needs for a wide variety of positions. TCWGlobal provides FTE services and contract staffing services.

Principal Service Commitments and System Requirements

TCWGlobal's Security, Confidentiality, and Processing Integrity commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service document published on the TCWGlobal website. The principal security, confidentiality and processing integrity commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the TCWGlobal platform and the customer data in accordance with TCWGlobal's security requirements.
- Perform third-party security and compliance audits of the environment, including, but not limited to:
  - Security penetration testing (pen tests)
  - Internal and external vulnerability scans and related remediations
  - Reporting on Controls at a Service Organization Relevant to Security, Processing Integrity, and Confidentiality (SOC 2) examinations.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of TCWGlobal personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.

- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

TCWGlobal establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in TCWGlobal's policies and procedures, system design documentation, and in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

TCWGlobal regularly reviews the security, confidentiality, and processing integrity performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security, confidentiality, and processing integrity commitments within the agreement, TCWGlobal will notify the customer via the TCWGlobal website or directly via email.

2. Overview of the System and Applications

Scope and System Boundaries

As outlined in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* a system is designed, implemented, and operated to provide reasonable assurance that TCWGlobal's service commitments and system requirements are achieved.

The scope of this examination is limited to TCWGlobal's StaffingNation and Payroll Services System ("StaffingNation") and all onsite hosted systems. The specific criteria and related control activities included in the scope of this engagement can be found in Section 4.

All criteria and controls within the security, confidentiality, and processing integrity categories are applicable to StaffingNation and Payroll Services System.

System Overview

The System is comprised of the following components:

- ***Infrastructure*** – The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** – The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** – The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** – The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** – The automated and manual procedures involved in the operation of a system

Infrastructure

The operations and corporate facilities are located in San Diego, CA. TCWGlobal utilizes a combination local area network (“LAN”) / wide area network ("WAN") to share data among its employees. The IT data center is located at a third-party secure colocation facility in San Diego near headquarters and is accessible 24 hours a day, 7 days a week, and 365 days a year to authorized TCWGlobal personnel. TCWGlobal uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

The StaffingNation Platform is hosted in Amazon Web Services (AWS) across multiple Availability Zones for high availability and disaster recovery purposes. TCWGlobal does not own or maintain any hardware in the AWS data centers. Services operate within a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure, and TCWGlobal is responsible for securing the StaffingNation Platform deployed in AWS (e.g., IAM, S3 bucket policies, Operating System and application security, Security Group configuration, network traffic monitoring).

Production, Staging, QA, and Development environments all reside on separate servers. Access to all instances is restricted to authorized administrators who must authenticate through Secure SSH Keys.

Production instances at AWS are logically and physically separate from TCWGlobal’s internal corporate network. All system hosts run on EC2, and database servers run on RDS instances that are secured via Security Groups. Security Groups monitor incoming network traffic by analyzing data packets and filtering traffic based on a defined ruleset. Access to manage the Security Groups is restricted to authorized DevSecOps personnel, and changes to these rulesets are governed by TCWGlobal’s change management policy, which includes documenting, testing, and approving the change.

TCWGlobal Company StaffingNation System Portal
The user facing StaffingNation System is a front-end application for customers to access their services. This application content is hosted on EC2, with data being stored in RDS, and customer-uploaded graphics (profile photos, company logos, and any file uploaded in StaffingNation) being loaded from S3 via CloudFront Content Delivery Network (CDN) for increased performance.

Software
The StaffingNation System runs with Ubuntu as the base image based on a generic Amazon Machine Images (AMI). Monthly, the continuous integration platform runs an automated process to update the image. A configuration management tool is used to configure software applications on individual instances using approved scripts.

TCWGlobal uses several software tools and utilities to configure, develop, and support the in-scope infrastructure and applications, including:

- Salt – SaltStack Infrastructure as Code
- GitHub – Online source code control repository
- Jenkins – Continuous integration platform
- Jira – Agile project management

Data
The types of services provided to user entities, including the various types of transactions processed.

The foundation of all the services is TCWGlobal functioning as a global employer of record. Whether clients require TCWGlobal to identify and source talent, or simply requires existing talent payrolled, the core service is TCWGlobal functioning as the employer of that talent. In addition, TCWGlobal offers services for staffing, MSP management of a client's total contingent workforce, classification of ICs, and guidance on navigating the complexities of a global contingent workforce.

The transactions associated with the services include:

- Job description review and the review of exemptions and workers compensation code classification.
- Job order with specific client requirements such as pay rate, bill rate, other client provided criteria.
- Complete on-boarding support, from job offer, onboarding documents, direct deposit or pay card setup, background check and benefits enrollment/administration (if applicable).

- Payroll processing in accordance with established pay frequency and any government requirements, which also includes tax withholding on W-2 eligible wages, and providing end of year tax forms, such as W-2 and 1099s.
- Timekeeping access and/or instruction provided to workers, with approval instruction provided to client contacts as necessary.
- Weekly invoicing based on transactions paid to workers, and any other contractual agreements.
- Off-boarding of the employees once the engagement is completed/ended. This includes termination of benefits, final pay, and unemployment management.
- Management of staffing requisitions and vendor management for clients engaging in MSP/VMS services.
- Sourcing and staffing of candidates in open positions as requested by clients engaged in these services. Candidates are submitted to clients via VMS portal, StaffingNation.
- Independent Contractor review and classification to comply with federal and state requirements.
- Overall customer service to both workers and clients to ensure a positive employment experience.

While TCWGlobal offers a variety of services, the primary day-to-day functions include online timekeeping and payroll processing, customer service, full employee lifecycle support, and compliance management.

Timekeeping and Payroll

Timekeeping is governed by secure username and password for each user, which is created within the payroll software for the purpose of accessing webcenter.tcwglobal.com. Each user has an approver, provided by an authorized user of the client company. The approver may or may not govern the day-to-day work of the worker. The approver is identified by the company and their internal processes. Once an approver has been identified that person receives an invitation to create their username and password for WebCenter (if not already a user). The worker and the approver both use WebCenter for time entry and approval. Workers log into WebCenter and can freely add hours and lunch periods for the entire pay period. Workers can save/edit entries throughout the week. Once worker clicks submit for the week, hours generally cannot be edited, unless the worker unlocks the timecard before it's approved. Once any edits are made, workers should resubmit the timecard for approval. A notification is sent to the approver via email. The approver logs in and can approve or reject entries. Managers may also make the corrections directly, which is logged in the system. Rejected entries send a message to the worker so that they may log back into the portal, make any necessary corrections, and then resubmit for approval. This process repeats. Approved hours go to the account manager to process payroll. All entries are time/date stamped for auditing and tracking purposes. Account managers can edit entries and can impersonate workers and supervisors, but this is logged.

No transfers happen in this process, it is all contained within one software, TempWorks. This timekeeping data is automatically used to process payroll and generate invoices which are sent via email to the approved contact along with a report of the time entries with associated fields. An ACH file containing relevant data for ACH payments is exported from the payroll software once a day and uploaded directly to the secure banking system by the finance team. Any checks mailed are printed and mailed to the mailing address provided by workers. Check/invoice errors are corrections are VERY rare (less than .1% of paycheck/invoice items require correction). Any corrections to paychecks/invoices are requested via a form submission and are then owned solely by the finance team. If a correction is made, TCWGlobal either issues a new invoice, a credit memo, paycheck adjustment etc. Updates are provided to the appropriate recipient and heavily documented.

Onboarding and Employee Relations

TCWGlobal offers full worker lifecycle support, from requirements, onboarding, to offboarding. The full worker lifecycle is supported within the StaffingNation system. Client users of StaffingNation can submit internally sourced candidates quickly. Those candidates are then notified of their offer letter, and if they accept the offer letter, they are taken through the full onboarding process, and are required to create a StaffingNation profile. Once onboarding paperwork is completed, a secure file drop is sent to the payroll/HRIS software to create an employee record. Operations team members then complete the remaining creation and review of the employee and engagement files. Once completed, another team member performs a QC of the entry for accuracy. If a candidate is not already known, client contacts may also submit a staffing request via StaffingNation for TCWGlobal recruiters to submit candidates too. In addition to onboarding and staffing support, client contacts may also communicate changes to engagements within StaffingNation or end of engagements by updating the relevant fields. As updates are made in StaffingNation, TCWGlobal's operations team is notified so they may take the appropriate action necessary.

Customer Service

TCWGlobal provides customer service to both workers and client companies related to contingent workforce or employment with one of the client companies. TCWGlobal strives to provide high levels of customer service, in accordance with established SLAs. The primary avenues through which customer service is provided are email, phone, and website chat.

Compliance Support

While not a standalone service, compliance support is provided as it pertains to workers employed through TCWGlobal. Changes to relevant employment laws are monitored by a compliance team and communicated via Operations and Client Relations teams. Compliance partners closely both with internal team members as well as customers to ensure TCWGlobal is safeguarding all parties and following relevant and required employment laws. Compliance provides guidance as it relates to IC classification as well, and drafts applicable contracts related to any IC relationships established.

People

The overall organization supports the framework for an effective control environment. The organization is comprised of the following functional areas:

- *Executive Management* provides strategic direction and leadership for TCWGlobal. Executive Management oversees and is ultimately responsible for all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to finance, information technology, human resources, legal, facilities, and corporate development.
- *Human Resources* is responsible for managing all functions related to recruiting and hiring, benefits, employee relations, performance management, training, resource management, and career assistance. The department provides administration of employee benefits and prescreening services for both corporate employees (internal) and contingent workers (external). Human Resources also oversees various aspects of employment while maintaining compliance with current labor law and employment standards, organizing employee files with the required documents, and employee offboarding. The department partners with Executive Management and various functional areas to ensure that all initiatives are appropriately aligned with TCWGlobal's mission, vision, and values.
- *Technology Services* management has overall responsibility and accountability for the enterprise computing environment, including computer hardware, operating systems, network systems, and application development. IT personnel work closely with the end users of other functional areas to develop and implement guidelines and procedures to ensure that the enterprise computing environment is functioning both efficiently and effectively with regard to the Company's business objectives and requirements. IT personnel also support the client service business processes, including the administration of systems supporting key business processes as well as maintaining application patch levels in accordance with vendor recommendations.
- *Marketing* is responsible for the strategic deployment of the TCWGlobal brand and for building awareness through multiple media channels including the internet, public relations, advertising, industry associations, and direct mail. Marketing also supports the business development group through action-oriented targeted marketing initiatives that qualify prospects and drive revenue generation.
- *Finance Management* oversees all financial aspects of the company which includes planning, organizing, auditing, accounting for, and reconciliation of all accounts. Additionally, the department provides necessary information to high-level managers to assist them in strategic decision making and is also responsible for the accuracy of financial reporting and related tax compliance. Finance personnel are responsible for corporate treasury matters, client invoicing and payment applications, payroll, and procurement processing. Finance provides support and assistance as needed to client services.

- *Client and Employee Services* are responsible for providing dedicated support for day-to-day questions and issues at the domestic and international level. The department is responsible for processing payroll, providing general support to the organization's workforce in terms of customer service and data entry responsibilities such as unemployment requests. Additionally, the department develops and grows the organization's client base by offering new services while maintaining its client relationships.
- *Legal and Compliance* brings together the organization's policies, procedures, and other compliance efforts. The department is responsible for preventing and detecting violations of laws, regulations, and policies. Legal and Compliance will promote a culture that encourages ethical conduct and commitment to compliance with the law. The department will address the specific risks of an organization with concrete actions to reduce or eliminate those risks. The department will also ensure that employees understand and comply with the laws, regulations, and policies that apply to their daily work.

TCWGlobal is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. TCWGlobal Company endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

TCWGlobal has a Chief Technology Officer (CTO)/ Chief Information Security Officer (CISO) who is responsible for the design and oversight of security and privacy initiatives. The CTO/CISO reports directly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, confidentiality, and processing integrity and operation of the StaffingNation Platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CTO/CISO.

All employees are expected to adhere to TCWGlobal's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect TCWGlobal's service commitments or system requirements.

3. Trust Services Criteria and Related Controls

TCWGlobal's criteria and related control activities are included in Section 4 of this report to eliminate redundancy. The description of the service auditor's tests and the results of those tests are also presented in Section 4, adjacent to the service organization's control activities. The description of the tests and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Control Environment

Management's Philosophy and Operating Style

TCWGlobal'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. Management monthly meetings are held to discuss operational issues.

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 TCWGlobal's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of TCWGlobal's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices.

Commitment to Competence

TCWGlobal's management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. TCWGlobal has focused on hiring experienced employees for the various positions required for the business along with continued development, training, and upskilling of the current workforce.

Organizational Structure and Assignment of Authority and Responsibility

TCWGlobal's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. TCWGlobal's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. TCWGlobal has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Customer Access Management
TCWGlobal Company provides customers with access to the StaffingNation System to access data and statistics. As part of the new customer onboarding process, the assigned Client Relations Analyst (CRA):

- Provides documented procedures pertaining to use of the portal.
- Facilitates customized training for new customers on the StaffingNation System platform.
- Provisions user accounts based on channels/products in contract. This process triggers emails to the users, in which they are prompted to create their own password based on system-enforced parameters.
- Assigns administrator-level permission to one authorized user account. Once an administrator-level user account has been created for the customer, that administrator can perform user administration activities, including provisioning and revoking access to the StaffingNation System portal.

Internal Access Management
Access to IT resources is granted based on role and business justification. Predefined groups are used to assign role-based access privileges and segregate duties and access to systems and data. TCWGlobal's HR team is responsible for the approval and assignment of access on a need-to-know basis. The granting and removal of access is facilitated via the IT and StaffingNation authorized teams. The IT Security Operations Team is responsible for administering and enforcing access to IT resources, as well as user provisioning and deprovisioning. Third-party partners and contractors are authorized prior to the issuance of credentials to access the IT environment.

User accounts terminations for employees, third-party partners, and contractors are communicated to IT Security Operations and are immediately disabled. In addition, a review of all user accounts and privileges is performed on a quarterly basis. Inappropriate access is immediately modified or removed.

Administrative privileges to IT resources are granted based on role and business justification and require specific authorization by the CTO/CISO. Employees requiring administrative access are assigned privileges through group membership or to their unique user account. Access to any database containing confidential data, including access by applications, administrators, and all other users, is restricted through programmatic methods (application code, system utilities). Application service IDs can only be used by applications and not individual users or processes.

All employees and third parties are assigned a unique user ID and authentication credentials aligned with password configuration requirements defined in the Information Security Policy. Password configuration requirements enforce minimum length, password complexity, password expiration, and password history. Group, shared, and generic accounts are

prohibited unless specifically required and approved by the CTO/CISO. Shared user IDs for system administration activities and other critical functions are not used.

Multi-factor authentication (MFA) is enforced to access production instances through administrative non-console access, remote access, and access to the AWS cloud. MFA requires the use of valid login and time-based token.

Production Access Management

Access to production systems is authenticated using SSH keys and AWS IAM roles, requires MFA, and is restricted to authorized administrators. In the event an employee with access to the production environment is terminated, the corresponding AWS IAM roles and SSH keys are removed as a component of the termination process. Management performs a review of network and application administrator access quarterly to ensure that appropriate privileged access is restricted.

Remote Access

Remote access to the network must be authorized and approved and is strictly controlled using public/private keys to access TCWGlobal systems. A VPN connection and/or firewall rule is required to access internal services. Additionally, the VPN connection is secured with MFA for all connections. For employees, automatic disconnect must be configured for remote access technologies after a specified period of inactivity. Remote access for third-party partners and contractors is granted upon authorization for the period needed and is immediately deactivated after use. TCWGlobal workstations that remotely connect to TCWGlobal's corporate network must have a strong password, an encrypted hard drive, must be a member of the VPN security group and run an antivirus solution.

Physical Security

The StaffingNation and Payroll Services System and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security of the infrastructure hosting the platform.

Physical access to TCWGlobal office locations is restricted by badge access. Badges are approved and removed as part of the new hire/termination process. All visitors must sign in and be escorted to office locations. Data Center requires additional badge + pin access by authorized system administrators only. Annually, owners of sensitive areas of the facilities review a list of the names and roles of those granted physical access to their areas to verify for continued business need.

Third Party Management

TCWGlobal engages with third-party partners to support/extend product offerings. The engagement, management, and monitoring of third-party partners is addressed in the Vendor Management Policy. Prior to engaging with a third-party for the solicitation of services, a signed NDA is received, and due diligence is performed. Annually, vendor risk is

assessed as part of the overall risk management effort to ensure continued compliance with the requirements for safeguarding TCWGlobal's systems and data.

Systems Development

TCWGlobal follows Software Development and Coding Standards that address security throughout the software development life cycle. Products are developed in accordance with the System Development Lifecycle Policy. Software development activities are subject to TCWGlobal's Change Management Policy and tracked using GitHub.

Developers follow secure coding practices, and all code is reviewed prior to implementation. Coding standards ensure that code is developed securely throughout the development life cycle and security vulnerabilities are addressed. Developers are trained on secure coding techniques.

Development, QA, Staging, and production environments are segregated. Virtual sandbox and production environments exist in separate virtual networks. The sandbox environment has virtual servers that are separated from production. Sandbox hosts all the lower-level environments (i.e., development, staging). The development environment is used to test code and conduct quality assurance testing. The staging environment is used for internal user acceptance and overall product evaluation. The production environment is used for live applications and data. Role-based access to all three environments is controlled using SSH keys. Access to the production environment is limited to the StaffingNation DevSecOps team.

Change Management

TCWGlobal has documented SDLC and change management procedures, which govern changes to infrastructure, as well as application and API development. Changes to infrastructure and microservices follow a Continuous Integration / Continuous Delivery (CI/CD) model.

The Change Control Policy includes requirements for authorization, testing, approval, and implementation. All changes are requested, tracked, and closed using Jira and GitHub for product changes, Cayzu and Jira for infrastructure changes, and HubSpot for customer support changes.

All planned and unplanned (emergency) changes must be submitted and approved by the CTO/CISO. Subsequent to approval, changes are scheduled and communicated to affected parties, including the date/time of the change, anticipated impact to users, and length of downtime, if any.

Change requests are assigned to appropriate IT operations team members for execution. Testing must be completed to confirm the requested functionality has been successfully developed. Assigned individuals are responsible for testing the change in a QA environment. Changes may be implemented into the production environment only after testing has been completed by both the developer and QA Engineer.

Final change approval is obtained by the Change Control Board prior to implementation. Segregation of duties is properly enforced to prevent developers from migrating changes to the production environment. Changes are approved, functionally tested, and include back out procedures. Upon completion of a significant change, documentation on all relevant requirements implemented on new and/or changed systems is updated as needed.

Patch Management
IT personnel monitor critical vendor patches and upgrades on an ongoing basis in order to mitigate potential damage to TCWGlobal Company's operations resulting from exploitation of published vulnerabilities. If a patch is deemed necessary, IT personnel document and track the patch installation in a ticket. Critical patches are evaluated and applied within 30 days of release.

Configuration Management
Configuration management tools are used for hardening devices, servers, and databases residing in the cloud infrastructure. These tools enable the automatic configuration of infrastructure devices in accordance with configuration standards. Changes to configurations are logged using Jira. Updates to the configuration management tool are made as needed as new vulnerabilities are identified.

System Monitoring
TCWGlobal Company monitors security and operations using network, infrastructure, and database monitoring tools within the StaffingNation and TCWGlobal System production environments. Agents are installed on all hosts to monitor network security and uptime, disk space, and system resource usage, and alerts are sent to IT personnel for any security events or usage issues. Additionally, audit logs are recorded by the system with a time stamp, are monitored on a regular basis, and are retained according to policy.

Critical events related to the security, confidentiality, and processing integrity of the system are logged and monitored at the infrastructure, application, and data layers. TCWGlobal also uses anomalous behavior detection/exfiltration software at the infrastructure level to identify personal data exfiltration. Logs provide key information, are indicators of potential compromise, and are used for troubleshooting purposes.

AWS CloudWatch, along with third-party tools, are used to monitor the performance and availability of the infrastructure. Microsoft Defender and Cloud App Security are used to collect and analyze the logs of servers and applications. Logs are reviewed periodically based upon the risk associated with the event and retained in accordance with the Data Retention Policy.

Data Asset Classification and Management
An inventory of all hardware and software located at TCW is maintained and updated as needed. The inventory includes a description of the function/use, version number, and location of all infrastructure hardware. Assets are discovered through an automated scanning

process using PDQ for scanning workstation and server nodes and Domotz for network. Scans are run on a periodic basis to detect any unauthorized hardware or software.

Data is classified based on value, sensitivity, and use. All TCWGlobal information and all information entrusted to TCWGlobal from third parties falls into one of four classifications, presented in order of increasing sensitivity. These classifications include Public, Internal, Restricted, Confidential.

Information is retained based upon its sensitivity, value, and legal and regulatory retention requirements. TCWGlobal considers retention requirements based on the classification and risk assigned. The retention of information applies to both electronic and physical information.

Data Security
TLS, PKI, and AES encryption are used to protect data used, transmitted, and stored. Trusted keys and/or certificates are used for security incident reporting, TLS connections, and interconnections between applications and databases.

Electronic hardware previously used to process or store data must be physically destroyed or wiped using a method that overwrites the data.

A Clean Desk Policy in place to ensure that sensitive/confidential information is secured when not in use. All sensitive/confidential information must be removed from an employee's user workspace and locked away when the items are not in use, or an employee leaves his/her workstation.

Vulnerability Management
Internal vulnerability scans are performed monthly, and external vulnerability scans are performed quarterly. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements. If a potential or actual security breach is detected, security personnel work to identify the cause and remediate it immediately. Additionally, penetration tests are performed annually to find and address any security weaknesses. Security personnel review the reports and document remediation plans to resolve any potential vulnerabilities, as applicable. Management reviews results of the report and evaluates updates to the Risk Assessment based on findings.

TCWGlobal addresses vulnerabilities potentially affecting the security, confidentiality, and processing integrity of systems and data through the following:

- The implementation of antivirus software on all systems commonly affected by malicious software.
- The application of vendor-supplied security patches as needed. Critical security patches are installed within one month of release.

- Internal vulnerability scans are performed monthly, and external vulnerability scans are performed quarterly. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.
- Penetration tests are performed at least annually, or more frequently as needed due to significant changes to the infrastructure or applications.

Issues identified in vulnerability scans and penetration test results are remediated and repeat scans and testing are performed to ensure that weaknesses have been corrected.

Incident Management

TCWGlobal has incident response and escalation procedures in place to efficiently and effectively manage unexpected incidents that can potentially impact the business. The incident response process defines activities to identify and mitigate security breaches and manage communications with TCWGlobal personnel, as well as customers, legal counsel, or law enforcement as necessary. Actions taken to contain and resolve incidents are documented in a ticketing system. When a security event is detected or reported, IT examines and attempts to resolve the issue, and escalates the incident if necessary. Customers are responsible for reporting any security issues based on the terms of the service agreement with TCWGlobal.

The Incident Response Policy includes procedures for incident preparation, detection and analysis, notification, containment, eradication and recovery, and post incident activity. Security incidents are logged in the TCW Security Incident Log and appropriately followed through the incident response lifecycle. The Incident Response Plan is tested on an annual basis or more frequently as needed. TCWGlobal defines a security incident as any irregular or suspicious event that might affect the security, confidentiality, or processing integrity of systems and data.

The Security Incident Response Team (SIRT) comprises management and employees representing infrastructure and product development and support. The SIRT also seeks support from other departments and external forensic professionals as needed.

Security incidents are detected through network devices, AWS alerts, and logs for suspicious events. Once the security incident is detected, the SIRT works quickly to analyze and validate each incident following a predefined process documenting each step taken. The initial analysis provides information to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. The security incident is logged in the TCW Security Incident Log and followed through the incident response lifecycle.

During/after incident detection and analysis, the SIRT notifies appropriate internal employees and law enforcement as needed. If the incident/breach impacts sensitive or personal data, notice is provided to customers affected.

Post-mortem activities include holding a “lessons learned” meeting with all involved parties after a major incident, and optionally after lesser incidents as deemed necessary. This meeting seeks to review what occurred, what was done to intervene, and how well intervention worked. The Incident Response Policy is updated as needed after each lesson learned session.

Backup and Recovery

TCWGlobal’s backup strategy includes snapshot images, differential and full backups of volumes and databases performed on an hourly and daily basis. TCWGlobal uses differential and full backups for SQL databases. RDS backups are also used to archive and store database backups, which are encrypted during the backup process. In addition, the source code of the configuration management and infrastructure orchestration system is backed up as well as system databases so infrastructure and services can be restored quickly. Scheduled database integrity checks are done daily as well to ensure the health of backups.

The disaster recovery strategy is predicated on a high availability scheme that has been established and configured for the StaffingNation system to reside at AWS in multiple availability zones. As part of the AWS S3 service offering, all data stored within AWS S3 includes cross region replication which automatically replicates data across different AWS regions. In the event one zone is unavailable, complete copies of production systems are available in other AWS zones.

The Disaster Recovery and Business Continuity Policy outlines the disaster recovery and business continuity strategy in place for TCWGlobal operations located onsite in production systems and data located at AWS. Backup data for local production systems are stored locally as well as redundantly on AWS.

The Disaster Recovery and Business Continuity Plan is tested on an annual basis. The test is conducted within a realistic environment that includes simulating conditions that are applicable in an actual emergency. Results of this test are reviewed, and updates are made to the plan/policy as necessary.

Risk Assessment

TCWGlobal recognizes the importance of risk management in properly managing TCWGlobal and customer transactions and providing high-quality, cost-effective services to its customers. The CTO/CISO oversees the assessment of risk with respect to the IT processing environment and related application systems and services provided to users of the company’s application systems.

The CTO/CISO leads risk assessment with the IT and StaffingNation DevSecOps team on a monthly basis. Items discussed each month can include any aspect of the IT department and will always include a security review of the physical facility, software security and appropriate

use. This review happens at least once a month and can happen more frequently if the need arises.

Fraud Risk Assessment
Management considers the potential for fraud, which can occur in both financial and non-financial reporting, when assessing risks to TCWGlobal's business objectives. Non-existent, insufficient, or ineffective controls provide an opportunity for fraud when combined with pressure or an incentive to commit fraud. Therefore, the potential for fraud is assessed on an annual basis as part of the formal Enterprise Risk Assessment.

Vendor Risk Assessment
TCWGlobal has a documented vendor risk management process in place, which includes performing due diligence prior to agreeing to services with new vendors or business partners. As part of this rigorous evaluation process, vendors are provided a compliance questionnaire, which assesses and seeks to identify security risks that may arise from sharing data or otherwise partnering with the organization. Data privacy risks are also evaluated, though the depth of the evaluation is largely dependent on the location of the organization. For example, US-based companies are questioned on where they store data, what compliance laws and regulations they are subject to, in which countries they do business, and their process to obtain explicit consent from data subjects.

On a periodic basis, management assesses the compliance status of critical vendors, subservice organizations, or business partners, communicates security incidents or issues as necessary, and terminates contracts in the event that security commitments are not met. Annually, at minimum, vendor risk is evaluated as a component of the Enterprise Risk Assessment and SOC audit reports of key subservice organizations are reviewed for appropriateness, including complementary user entity controls. Management requires all subservice organizations without a SOC report to fill out a questionnaire to evaluate risk.

Customer Security Risk Evaluation
Once a customer is onboarded, the customer is provided with a compliance questionnaire to assess security risks, including data encryption methods, privileged access management, etc. The Privacy and Security team reviews the responses and reaches out to the customer to request remediation, where necessary. Upon successful remediation of identified gaps, the risk evaluation process is complete, and the customer can be given access to the StaffingNation platform.

Information and Communication

TCWGlobal obtains relevant and quality information from internal and external sources, such as security monitoring tools, data imported via API, and management assessments of risks to the production environment. Additionally, management has implemented various communication methods for employees and external parties to help ensure that communication occurs broadly and in all directions within the organization. These methods

include, but are not limited to, management meetings, documented job descriptions, policy distribution and acknowledgements, change and incident management tickets, company Intranet, Knowledge Base and SOPs, and documented policies and procedures that are formally documented and clearly communicated to all employees.

Internal Communication

TCWGlobal's information security policies are updated annually, at minimum, and are published to all employees internally via SharePoint. The Employee Handbook also contains reference to security responsibilities, as well as disciplinary procedures for not adhering to security protocols within the organization. The Employee Handbook and security policies are acknowledged by all employees upon hire, and the security policies are acknowledged annually thereafter. Additionally, TCWGlobal requires all employees to sign confidentiality and non-solicitation agreements before starting work in the organization.

The security policies and responsibilities are reinforced through security and privacy awareness training, which occurs via SkillSoft through the branded company Learning Management System (LMS) upon hire and annually thereafter. Additionally, event-driven security reminders/notifications are communicated as needed.

External Communication

TCWGlobal Company's security commitments are communicated to customers via an executed agreement or contract. Multiple communication channels are in place to allow customers to report security incidents, failures, concerns, or other complaints, including direct line to customer representatives via phone or email.

In the case of a confirmed data breach, TCWGlobal would notify customers within 48-72 hours. If a breach involves TCWGlobal Company's data, as opposed to customer data, TCWGlobal would notify the regulatory agencies within 72 hours.

Various methods of communication are used to ensure that service commitments and system requirements are communicated and addressed in a timely manner. Email and Teams are used to communicate time sensitive messages. Executive leadership, manager, and staff meetings are held on a periodic basis and as needed. All-hands company meetings, where company objectives and performance are discussed, are held on a quarterly basis with all employees.

Significant System and Control Change

The IT environment has been stable throughout the period and there have been no significant changes to the system. The description does not omit or distort information relevant to TCWGlobal's system. TCWGlobal acknowledges the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

4. Monitoring

The CTO/CISO and DevSecOps team monitors the quality of internal control performance as a normal part of her activities. The CTO/CISO is heavily involved in day-to-day activities and regularly reviews various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. TCWGlobal adopts a proactive approach to the monitoring of application security to ensure that any issues or risks are addressed before becoming significant problems.

Separate Evaluations

Evaluations of internal control vary in scope and frequency, depending on the significance of risks being managed and the importance of the controls in reducing risks. Evaluations often take the form of informal self-assessments, where personnel responsible for a particular function determine the effectiveness of controls for their activities.

Security reviews, vulnerability assessments, and penetration tests are performed or coordinated by Information Security personnel periodically to identify threats and assess their potential impacts to system security. Any detected security vulnerabilities are investigated and documented through remediation.

Subservice Organizations

Subservice organizations are used to deliver products and services that TCWGlobal relies on to serve its customers and clients.

Amazon Web Services (AWS)
TCWGlobal uses **Amazon Web Services (AWS**) as the cloud hosting provider for the StaffingNation application. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at AWS, alone or in combination with controls at TCWGlobal, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Control
6.4	AWS is partially responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.

TCWGlobal Management receives and reviews the AWS SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 2 report are analyzed for relevance to and effect on TCWGlobal's organization and its users. As part of the review:

- Management confirms that the CSOCs listed above are covered within the scope of AWS' SOC 2 Type 2 report and are found to be operating effectively during the audit period.
- Management determines that the Complementary User Entity Controls (CUECs) identified in AWS' SOC 2 Type 2 report are included in the scope of this SOC 2 report as controls that are tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by AWS to ensure that operations and controls expected to be implemented are functioning effectively.

Arctic Wolf

TCWGlobal uses **Arctic Wolf** as the security monitoring provider for the StaffingNation application. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Arctic Wolf, alone or in combination with controls at TCWGlobal, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Control
7.2, 7.3	Arctic Wolf is partially responsible for detecting and reporting security events.

TCWGlobal Management receives and reviews the Arctic Wolf SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 2 report are analyzed for relevance to and effect on TCWGlobal's organization and its users. As part of the review:

- Management confirms that the CSOCs listed above are covered within the scope of Arctic Wolf's SOC 2 Type 2 report and are found to be operating effectively during the audit period.
- Management determines that the Complementary User Entity Controls (CUECs) identified in Arctic Wolf's SOC 2 Type 2 report are included in the scope of this SOC 2 report as controls that are tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by Arctic Wolf to ensure that operations and controls expected to be implemented are functioning effectively.

5. Complementary User Entity Controls and Responsibilities

The control activities performed by TCWGlobal were designed with the understanding that certain user organization controls would be implemented by each customer. Each customer's internal control structure must be evaluated in conjunction with TCWGlobal's controls, policies and procedures described in this report. The Complementary User Entity Controls (CUECs) below are the minimum controls that customers must have in operation to complement the controls of the StaffingNation system and should not be regarded as a comprehensive list of all controls that should be employed by customers.

Complementary User Entity Controls	Related Applicable Criteria
Users are responsible for the safekeeping of their credentials to the StaffingNation system.	6.1, 6.3
Users are responsible for reviewing the accuracy of the data that is input into the system.	PI 1.2
Supervisors are responsible for contacting TCWGlobal in a timely manner to ensure terminated employee account access is removed.	6.1, 6.3
Clients are responsible for the accuracy, completeness, and authorization of pay rate changes of their users.	PI 1.2, PI 1.3
Clients and users are responsible for the accuracy and completeness of changes to benefit information.	PI 1.2, PI 1.3
Clients are responsible for the review and approval of all user payroll information for each period.	PI 1.2, PI 1.3
Clients are responsible for the reconciliation of payroll reports generated by TCWGlobal to what they entered into the system (output to input) to ensure accuracy and completeness.	PI 1.2
Users are responsible for adhering to all regulatory compliance issues when they are associated with TCWGlobal in a service agreement.	2.3, C 1.1, PI 1.2
Users are responsible for reviewing and approving the terms and conditions stated in service agreements with TCWGlobal.	2.3, C 1.1

6. Non-Applicable Trust Services Criteria

All criteria within the Security, Confidentiality, and Processing Integrity categories are applicable to the StaffingNation and Payroll Services System.

SECTION FOUR

Trust Services Criteria, Related Controls, and Tests of Controls

TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

1 Scope, Purpose, and Objectives of the Report

The scope of CyberGuard Compliance, LLP's procedures was based on the AICPA and trust services criteria relevant to Security, Confidentiality, and Processing Integrity as they relate to the system and the design and operating effectiveness of the applicable controls. This report, when combined with an understanding and assessment of the internal controls at user organizations, is intended to meet the needs of a broad range of users that need information and assurance about the controls at TCWGlobal that affect the Security, Confidentiality, and Processing Integrity criteria of the system. Stakeholders who may need this report are: management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls.

APPLICABLE TRUST SERVICES CRITERIA

The applicable trust services criteria and related controls presented in Section 4, "Trust Services Criteria, Related Controls, and Tests of Controls," are an integral part of TCWGlobal's system description throughout the period March 1, 2023 to February 29, 2024.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

i. information during its collection or creation, use processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of TCWGlobal service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements. Confidentiality addresses TCWGlobal's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from TCWGlobal's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Processing Integrity

The trust services criteria relevant to processing integrity address the need for system processing to be complete, valid, accurate, timely, and authorized to achieve the service organization's service commitments and system requirements.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Our examination was restricted to the Trust Services Criteria specified above and related control procedures specified in Section 4. It is the stakeholders' responsibility to evaluate this information in relation to the controls in place at each user organization.

2 Tests of Operating Effectiveness

Our tests of the operating effectiveness of controls were designed to cover a representative number of transactions for the period March 1, 2023 to February 29, 2024 for each of the trust services criteria listed in Section 4, which are designed to achieve the specific criteria. Tests of design and operating effectiveness were based off the criteria and illustrative controls within each trust services criteria.

Type of Test	General Description of Test
Inquiry or corroborative inquiry	Inquired of appropriate personnel to ascertain compliance with controls.
Observation	Observed application of specific controls.
Inspection	Obtained and examined documents and reports indicating performance of the controls.
Re-Performed	Re-performed application of the controls.

In addition, as required by paragraph .35 of ATC Section 205, Assertion-Based Examination Engagements (AICPA, *Professional Standards*), and paragraph .30 of ATC Section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

This assessment was performed virtually using Information and Communication Technology (ICT).

3 Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), CGC performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1) Inspect the source of the IPE.
2) Inspect the query, script, or parameters used to generate the IPE.
3) Tie data between the IPE and the source.
4) Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above, procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), CGC inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria for Security

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
1.1.1	The Company has a formalized Code of Conduct, which demonstrates the importance of integrity and ethical values. The Code of Conduct is included in the Employee Handbook, which is available to employees via the Company's SharePoint.	**Inspection:** Obtained and reviewed the Code of Conduct Policy and Employee Handbook. Verified the Company had a formalized Code of Conduct, which demonstrated the importance of integrity and ethical values. The Code of Conduct was included in the Employee Handbook, which was available to employees via the Company's SharePoint.	No exceptions noted.
1.1.2	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the acknowledgements for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understand and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
1.1.3	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1.4	The Company has established disciplinary policies for employees who violate security policies/acceptable use policies/company policies.	**Inspection:** Obtained and reviewed the Employee Handbook. Verified the Company had established disciplinary policies for employees who violate security policies/acceptable use policies/company policies.	No exceptions noted.
1.2	COSO Principle 2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
1.2.1	The Board of Directors operates independently and provides oversight on the system of internal control.	**Inspection:** Obtained and reviewed the Board meeting minutes. Verified the Board of Directors operated independently and provided oversight on the system of internal control.	No exceptions noted.
1.3	COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
1.3.1	Reporting relationships and organizational structures are reviewed annually by senior management as part of organizational planning, and are adjusted as needed based on changing Company commitments and requirements.	**Inspection:** Obtained and reviewed the organizational chart and review. Verified reporting relationships and organizational structures were reviewed annually by senior management as part of organizational planning, and were adjusted as needed based on changing Company commitments and requirements.	No exceptions noted.
1.3.2	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the job descriptions for the sampled active employees during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
1.4.1	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.
1.4.2	Personnel must pass a criminal background check before they may be hired by the Company.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the background check reports for the sampled employees hired during the audit period. Verified personnel passed a criminal background check before they were hired by the Company.	No exceptions noted.
1.4.3	The experience and training of candidates for employment are verified before they assume the responsibilities of their position.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the background check reports for the sampled employees hired during the audit period. Verified the experience and training of candidates for employment was verified before they assumed the responsibilities of their position.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.4.4	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the job descriptions for the sampled active employees during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.
1.4.5	Personnel are required to attend annual security awareness training.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the training logs for the sampled active employees during the audit period. Verified personnel were required to attend annual security awareness training.	No exceptions noted.
1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
1.5.1	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
1.5.2	The Chief Technology Officer (CTO)/Chief Information Security Officer (CISO) is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the CTO/CISO's job description. Verified the CTO/CISO was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.5.3	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the control review and communication. Verified the list of internal controls were communicated to process owners, reviewed, and updated annually.	No exceptions noted.
1.5.4	Personnel are required to attend annual security awareness training.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the training logs for the sampled active employees during the audit period. Verified personnel were required to attend annual security awareness training.	No exceptions noted.
1.5.5	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
2.1.1	The Company reviews its data flow diagram annually.	**Inspection:** Obtained and reviewed the data flow diagram. Verified the Company reviewed its data flow diagram annually.	No exceptions noted.
2.1.2	The Data Classification Policy details roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	**Inspection:** Obtained and reviewed the Data Classification Policy. Verified the Data Classification Policy detailed roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	No exceptions noted.
2.1.3	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
2.2.1	The Chief Technology Officer (CTO)/Chief Information Security Officer (CISO) is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the CTO/CISO's job descriptions. Verified the CTO and CISO was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.2.2	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
2.2.3	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the control review and communication. Verified the list of internal controls were communicated to process owners, reviewed, and updated annually.	No exceptions noted.
2.2.4	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Plan and training. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
2.2.5	Changes made to systems are communicated to appropriate users.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified changes made to systems were communicated to appropriate users.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
2.3.1	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Plan and training. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
2.3.2	Relevant updates and changes to agreements, policies, and privacy policies are pushed to external parties via the internal portal.	**Inspection:** Obtained and reviewed the privacy policy and screenshot of the policy on the Company portal. Verified relevant updates and changes to agreements, policies, and privacy policies were pushed to external parties via the internal portal.	No exceptions noted.
2.3.3	Company policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it is encrypted.	**Inspection:** Obtained and reviewed the Data Encryption Policy. Verified Company policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
2.3.4	Applicable Company security, processing integrity, and confidentiality commitments regarding the system are included in the Master Service Agreement and/or customer-specific Service Level Agreements.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the Master Service Agreements for the sampled customers during the audit period. Verified applicable Company security, processing integrity, and confidentiality commitments regarding the system were included in the Master Service Agreement and/or customer-specific Service Level Agreements.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.3.5	Customer responsibilities, which may include the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints, are described in the Master Service Agreements, Statements of Work, or Service Level Agreements.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the Master Service Agreements for the sampled customers during the audit period. Verified customer responsibilities, which may include the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints, were described in the Master Service Agreements, Statements of Work, or Service Level Agreements.	No exceptions noted.
2.3.6	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the control review and communication. Verified the list of internal controls were communicated to process owners, reviewed, and updated annually.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
3.1.1	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Assessment Program. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
3.1.2	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.1.3	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.1.4	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
3.2.1	Business Continuity and Disaster Recovery Plans are in place to identify the criticality of information assets.	**Inspection:** Obtained and reviewed the Business Continuity and Disaster Recovery Plan. Verified Business Continuity and Disaster Recovery Plans were in place to identify the criticality of information assets.	No exceptions noted.
3.2.2	Internal vulnerability scans are performed monthly, and external vulnerability scans are performed quarterly. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scans. Verified internal vulnerability scans were performed monthly, and external vulnerability scans were performed quarterly. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
3.2.3	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
3.2.4	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy and vendor risk assessments. Verified the Company maintained a formal Vendor Risk Management process that assessed the potential threats and vulnerabilities from vendors providing goods and services. The Company assessed, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2.5	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.2.6	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.
3.2.7	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.2.8	Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes and the risk assessment. Verified unremediated risks were assessed by Management as needed. Remediation activities were documented and resolved in a timely manner.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
3.3.1	An enterprise risk assessment is performed annually and considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified an enterprise risk assessment was performed annually and considered fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	No exceptions noted.
3.3.2	The enterprise risk assessment considers how management and other personnel might engage in or justify inappropriate actions.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the enterprise risk assessment considered how management and other personnel might engage in or justify inappropriate actions.	No exceptions noted.
3.3.3	The enterprise risk assessment considers threats and vulnerabilities that arise specifically from the use of IT and access to information.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the enterprise risk assessment considered threats and vulnerabilities that arise specifically from the use of IT and access to information.	No exceptions noted.
3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
3.4.1	The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.
3.4.2	The risk identification process considers changes in the Company's systems and in the technology environment.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes in the Company's systems and in the technology environment.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.4.3	The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes in vendor and business partner relationships.	No exceptions noted.
3.4.4	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.4.5	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.
3.4.6	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.

4.0 MONITORING ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
4.1.1	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
4.1.2	Internal vulnerability scans are performed monthly, and external vulnerability scans are performed quarterly. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scans. Verified internal vulnerability scans were performed monthly, and external vulnerability scans were performed quarterly. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
4.1.3	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the configuration review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks were performed annually, at minimum.	No exceptions noted.
4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.		
4.2.1	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the control review and communication. Verified the list of internal controls were communicated to process owners, reviewed, and updated annually.	No exceptions noted.

4.0 MONITORING ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.2.2	Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes and the risk assessment. Verified unremediated risks were assessed by Management as needed. Remediation activities were documented and resolved in a timely manner.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
5.1.1	The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.
5.1.2	The risk identification process considers changes in the Company's systems and in the technology environment.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes in the Company's systems and in the technology environment.	No exceptions noted.
5.1.3	The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified the risk identification process considered changes in vendor and business partner relationships.	No exceptions noted.
5.1.4	Control activities are mapped to the Company's risk assessment to ensure that risk responses address and mitigate risks.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified control activities were mapped to the Company's risk assessment to ensure that risk responses address and mitigate risks.	No exceptions noted.
5.1.5	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the enterprise risk assessment. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1.6	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.
5.2	COSO Principle 11: The entity selects and develops general control activities over technology to support the achievement of objectives.		
5.2.1	Documented configuration standards are reviewed annually, at minimum, and when significant changes are made or integral system components are added.	**Inspection:** Obtained and reviewed the configuration standards. Verified documented configuration standards were reviewed annually, at minimum, and when significant changes were made or integral system components were added.	No exceptions noted.
5.2.2	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Rights Management Policy. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.
5.2.3	The Company maintains recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	**Inspection:** Obtained and reviewed the Backup Policy. Verified the Company maintained recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
5.3.1	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
5.3.2	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Rights Management Policy. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.
5.3.3	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Management Procedure. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.3.4	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the acknowledgements for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understand and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
5.3.5	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the control review and communication. Verified the list of internal controls were communicated to process owners, reviewed, and updated annually.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
6.1.1	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.1.2	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over a VPN for authorized employees, contractors, and third parties.	No exceptions noted.
6.1.3	Users are required to authenticate via unique user account ID and password before being granted access to in-scope networks, systems, and applications.	**Inspection:** Obtained and reviewed the user listing and screenshots of the login portal. Verified users were required to authenticate via unique user account ID and password before being granted access to in-scope networks, systems, and applications.	No exceptions noted.
6.1.4	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the administrator listing and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.5	Administrators must authenticate via unique ID and password before being granted access to in-scope networks, systems, and applications.	**Inspection:** Obtained and reviewed the administrator listing and reconciled with the employee listing. Verified administrators authenticated via unique ID and password before being granted access to in-scope networks, systems, and applications.	No exceptions noted.
6.1.6	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified New user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.1.7	Modified user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the access request tickets for the sampled access modifications during the audit period. Verified modified user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. RBAC was used to support segregation of incompatible functions.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.8	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Data Encryption Policy. Verified the Company had documented policies and procedures on the use of cryptographic controls for protection of information.	No exceptions noted.
6.1.9	Key management is in place to support cryptographic techniques established by the Company.	**Inspection:** Obtained and reviewed the key rotation configuration. Verified key management was in place to support cryptographic techniques established by the Company.	No exceptions noted.
6.1.10	The production network domain is configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	**Inspection:** Obtained and reviewed the domain password configuration. Verified the production network domain was configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.11	In-scope applications are configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	**Inspection:** Obtained and reviewed the application password configuration. Verified in-scope applications were configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	No exceptions noted.
6.1.12	The system automatically logs out users after a defined period of inactivity.	**Inspection:** Obtained and reviewed the domain and application timeout configuration. Verified the system automatically logged out users after a defined period of inactivity.	No exceptions noted.
6.1.13	Separate environments are used for development, testing, and production. Changes require independent review and approval before they can be merged to production.	**Inspection:** Obtained and reviewed the network diagrams and the code repository configuration and access listing. Verified separate environments were used for development, testing, and production. Changes required independent review and approval before they could be merged to production.	No exceptions noted.
6.1.14	Confidential data files are encrypted prior to backup.	**Inspection:** Obtained and reviewed the backup encryption configuration. Verified confidential data files were encrypted prior to backup	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
6.2.1	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Rights Management Policy. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.
6.2.2	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified New user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.2.3	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified Human Resources was responsible for notifying IT of terminated employees and contractors. IT terminated logical access within 24 hours of notification.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.2.4	Terminated employee and contractor access to Company facilities is removed upon termination and Company assets returned.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and Company assets returned.	No exceptions noted.
6.2.5	A user access review of network and application accounts, and associated permissions, is performed semi-annually to ensure appropriate logical access is maintained.	**Inspection:** Obtained and reviewed the user access reviews. Verified a user access review of network and application accounts, and associated permissions, was performed semi-annually to ensure appropriate logical access was maintained.	No exceptions noted.
6.2.6	Management performs a review of network and application administrator access quarterly to ensure that appropriate privileged access is restricted.	**Inspection:** Obtained and reviewed the user access reviews for the sampled quarters during the audit period. Verified management performed a review of network and application administrator access quarterly to ensure that appropriate privileged access was restricted.	No exceptions noted.
6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
6.3.1	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Rights Management Policy. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.3.2	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified New user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.3.3	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified Human Resources was responsible for notifying IT of terminated employees and contractors. IT terminated logical access within 24 hours of notification.	No exceptions noted.
6.3.4	Terminated employee and contractor access to Company facilities is removed upon termination and Company assets returned.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and Company assets returned.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
6.4.1	Physical access to facilities is controlled with the use of electronic locks using access cards.	**Inspection:** Obtained and reviewed photos of the access device, access configuration and physical access listing. Verified physical access to facilities was controlled with the use of electronic locks using access cards.	No exceptions noted.
6.4.2	Physical access to sensitive areas is restricted to authorized personnel.	**Inspection:** Obtained and reviewed the physical access listing and reconciled with the employee listing. Verified physical access to sensitive areas was restricted to authorized personnel.	No exceptions noted.
6.4.3	Procedures are implemented to enforce controls around the management of removable media. The use of removable media is limited to those with a valid business need.	**Inspection:** Obtained and reviewed the domain removable media configuration. Verified procedures were implemented to enforce controls around the management of removable media. The use of removable media was limited to those with a valid business need.	No exceptions noted.
6.4.4	Terminated employee and contractor access to Company facilities is removed upon termination and Company assets returned.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and Company assets returned.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.4.5	Annually, owners of sensitive areas of the facilities review a list of the names and roles of those granted physical access to their areas to verify for continued business need.	**Inspection:** Obtained and reviewed the physical access review. Verified owners of sensitive areas of the facilities reviewed a list of the names and roles of those granted physical access to their areas to verify for continued business need annually.	No exceptions noted.
AWS is partially responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.			
6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
6.5.1	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.5.2	Formal data retention and disposal procedures are in place to guide the secure disposal of data that has been identified for destruction in a manner that prevents loss, theft, misuse, or unauthorized access.	**Inspection:** Obtained and reviewed the Document Retention and Disposal Policy. Verified formal data retention and disposal procedures were in place to guide the secure disposal of data that had been identified for destruction in a manner that prevented loss, theft, misuse, or unauthorized access.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.5.3	Prior to disposal, all electronic media is securely wiped and sanitized to removal all data and software.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of disposals during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Document Retention and Disposal Policy, and verified all electronic media is securely wiped and sanitized to removal all data and software prior to disposal.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
6.5.4	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the encryption configuration and device listing. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.
6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
6.6.1	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the administrator listing and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.
6.6.2	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over a VPN for authorized employees, contractors, and third parties.	No exceptions noted.
6.6.3	SSH keys are used to access all storage nodes.	**Inspection:** Obtained and reviewed the SSH configuration. Verified SSH keys were used to access all storage nodes.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.6.4	Firewalls are in place to protect production systems and are configured to restrict unnecessary ports, protocols, and services. Logs are monitored to detect any potential security vulnerabilities or unauthorized access attempts.	**Inspection:** Obtained and reviewed the firewall configuration, firewall logs, and network diagram. Verified firewalls were in place to protect production systems and were configured to restrict unnecessary ports, protocols, and services. Logs were monitored to detect any potential security vulnerabilities or unauthorized access attempts.	No exceptions noted.
6.6.5	The Company uses Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the SSL configuration. Verified the Company used Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	No exceptions noted.
6.6.6	An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention system configuration and alert log. Verified an Intrusion Detection and Prevention System was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity. This control is also the responsibility of Arctic Wolf.	No exceptions noted.
6.6.7	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the encryption configuration and device listing. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
6.7.1	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Data Encryption Policy. Verified the Company had documented policies and procedures on the use of cryptographic controls for protection of information.	No exceptions noted.
6.7.2	Key management is in place to support cryptographic techniques established by the Company.	**Inspection:** Obtained and reviewed the key rotation configuration. Verified key management was in place to support cryptographic techniques established by the Company.	No exceptions noted.
6.7.3	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over a VPN for authorized employees, contractors, and third parties.	No exceptions noted.
6.7.4	The Company uses Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the SSL configuration. Verified the Company used Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	No exceptions noted.
6.7.5	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the encryption configuration and device listing. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.7.6	Procedures are implemented to enforce controls around the management of removable media. The use of removable media is limited to those with a valid business need.	**Inspection:** Obtained and reviewed the domain removable media configuration. Verified procedures were implemented to enforce controls around the management of removable media. The use of removable media was limited to those with a valid business need.	No exceptions noted.
6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
6.8.1	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the Company had a documented Change Management Policy that addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.
6.8.2	System and configuration management tools are used to maintain an inventory of installed applications and software and to monitor patch status. These tools log and alert IT of software installation or attempted software installation.	**Inspection:** Obtained and reviewed the application inventory, system log file and installation alert. Verified system and configuration management tools were used to maintain an inventory of installed applications and software and to monitor patch status. These tools logged and alerted IT of software installation or attempted software installation.	No exceptions noted.
6.8.3	Anti-virus software is installed on all servers and workstations. Updates are pushed to the nodes as new updates and signatures become available.	**Inspection:** Obtained and reviewed the antivirus installation report and update configuration. Verified anti-virus software was installed on all servers and workstations. Updates were pushed to the nodes as new updates and signatures became available.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.8.4	Procedures are in place to wipe information assets that have been transferred or returned to the entity's custody prior to its implementation on the network.	**Inspection:** Obtained and reviewed the Termination Procedure. Verified procedures were in place to wipe information assets that had been transferred or returned to the entity's custody prior to its implementation on the network.	No exceptions noted.
6.8.5	Separate environments are used for development, testing, and production. Changes require independent review and approval before they can be merged to production.	**Inspection:** Obtained and reviewed the network diagrams and the code repository configuration and access listing. Verified separate environments were used for development, testing, and production. Changes required independent review and approval before they could be merged to production.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
7.1.1	An enterprise monitoring tool is in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts are sent to security personnel.	**Inspection:** Obtained and reviewed the monitoring dashboard and alert reports. Verified an enterprise monitoring tool was in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts were sent to security personnel.	No exceptions noted.
7.1.2	Internal vulnerability scans are performed monthly, and external vulnerability scans are performed quarterly. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scans. Verified internal vulnerability scans were performed monthly, and external vulnerability scans were performed quarterly. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
7.1.3	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
7.1.4	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the configuration review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks were performed annually, at minimum.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
7.2.1	The Customer Portal is configured to require all relevant parties to accept the terms, which include the organization's services and client responsibilities.	**Inspection:** Obtained and reviewed the Customer Portal terms acknowledgement and the Terms of Use. Verified the Customer Portal was configured to require all relevant parties to accept the terms, which include the organization's services and client responsibilities.	No exceptions noted.
7.2.2	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the configuration review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems. These compliance checks were performed annually, at minimum.	No exceptions noted.
7.2.3	An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention system configuration and alert log. Verified an Intrusion Detection and Prevention System was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	No exceptions noted.
		This control is also the responsibility of Arctic Wolf.	

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.2.4	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the event tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution.	No exceptions noted.
		This control is also the responsibility of Arctic Wolf.	
7.2.5	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Management Procedure. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
Arctic Wolf is partially responsible for detecting and reporting security events.			

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
7.3.1	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Management Procedure. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.3.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Plan and training. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
7.3.3	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the event tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution. This control is also the responsibility of Arctic Wolf.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.3.4	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, observed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Incident Management Procedure, and verified management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
7.3.5	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inspection:** Obtained and reviewed the Business Continuity test reports. Verified the Business Continuity and Disaster Recovery Plan was tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan was updated based on the test results.	No exceptions noted.
Arctic Wolf is partially responsible for detecting and reporting security events.			

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
7.4.1	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Management Procedure. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.4.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Plan and training. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
7.4.3	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, observed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Incident Management Procedure, and verified management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
7.5.1	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inspection:** Obtained and reviewed the Business Continuity test reports. Verified the Business Continuity and Disaster Recovery Plan was tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan was updated based on the test results.	No exceptions noted.
7.5.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Plan and training. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
7.5.3	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, observed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Incident Management Procedure, and verified management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

8.0 CHANGE MANAGEMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
8.1.1	The Company has adopted a formal Systems Development Life Cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC takes into account Security requirements.	**Inspection:** Obtained and reviewed the Software Development Life Cycle Policy. Verified the Company had adopted a formal Systems Development Life Cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC took into account Security requirements.	No exceptions noted.
8.1.2	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the Company had a documented Change Management Policy that addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.
8.1.3	System changes are documented, tested, and approved prior to migrating the change to production as part of the change management process.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified system changes were documented, tested, and approved prior to migrating the change to production as part of the change management process.	No exceptions noted.

8.0 CHANGE MANAGEMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1.4	Emergency changes are documented, authorized, tested, and approved following the Change Management Policy.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the emergency change requests for the sampled emergency changes during the audit period. Verified emergency changes were documented, authorized, tested, and approved following the Change Management Policy.	No exceptions noted.
8.1.5	Changes made to systems are communicated to appropriate users.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified changes made to systems were communicated to appropriate users.	No exceptions noted.
8.1.6	Vendor security patches are evaluated, and critical patches are applied to key systems and applications.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the patch history for the sampled production servers utilized during the audit period. Verified vendor security patches were evaluated, and critical patches applied to key systems and applications.	No exceptions noted.
8.1.7	Separate environments are used for development, testing, and production. Changes require independent review and approval before they can be merged to production.	**Inspection:** Obtained and reviewed the network diagrams and the code repository configuration and access listing. Verified separate environments were used for development, testing, and production. Changes required independent review and approval before they could be merged to production.	No exceptions noted.

9.0 RISK MITIGATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
9.1.1	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Assessment Program. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
9.1.2	Risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	**Inspection:** Obtained and reviewed the insurance policy. Verified risk management activities considered the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	No exceptions noted.
9.2	The entity assesses and manages risks associated with vendors and business partners.		
9.2.1	The Company has a Vendor Management Policy, which provides guidance regarding the identification and management of critical vendors and business partners.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified the Company had a Vendor Management Policy, which provided guidance regarding the identification and management of critical vendors and business partners.	No exceptions noted.
9.2.2	Executed agreements are maintained for vendors and business partners. These agreements define the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	**Inspection:** Obtained and reviewed the vendor agreements for the sub-service organizations utilized during the audit period. Verified executed agreements were maintained for vendors and business partners. These agreements defined the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	No exceptions noted.

9.0 RISK MITIGATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.2.3	SOC audit reports of key sub-service organizations are reviewed for appropriateness, including complementary user entity controls. Management requires all critical vendors without a SOC report to fill out a questionnaire to evaluate risk.	**Inspection:** Obtained and reviewed the SOC audit report and review. Verified SOC audit reports of key sub-service organizations were reviewed for appropriateness, including complementary user entity controls.	No exceptions noted.
9.2.4	Management requires all critical vendors without a SOC report to fill out a questionnaire to evaluate risk.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of vendors without a SOC report during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Vendor Management Policy, and verified management required all critical vendors without a SOC report to fill out a questionnaire to evaluate risk.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
9.2.5	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy and vendor risk assessments. Verified the Company maintained a formal Vendor Risk Management process that assessed the potential threats and vulnerabilities from vendors providing goods and services. The Company assessed, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	No exceptions noted.

CONFIDENTIALITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C 1.1.1	Procedures are in place to identify and designate confidential information when it is received or created, and to determine the period over which the confidential information is to be retained.	**Inspection:** Obtained and reviewed the Data Classification and Retention Policies. Verified procedures were in place to identify and designate confidential information when it was received or created, and to determine the period over which the confidential information is to be retained.	No exceptions noted.
C 1.1.2	Procedures are in place to protect confidential information from erasure or destruction during the specified retention period.	**Inspection:** Obtained and reviewed the Data Classification and retention policies. Verified procedures were in place to protect confidential information from erasure or destruction during the specified retention period.	No exceptions noted.
C 1.1.3	Executed agreements are maintained for vendors and business partners. These agreements define the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	**Inspection:** Obtained and reviewed the vendor agreements for the sub-service organizations utilized during the audit period. Verified executed agreements were maintained for vendors and business partners. These agreements defined the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	No exceptions noted.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C 1.2.1	Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	**Inspection:** Obtained and reviewed the Data Classification and Retention Policies. Verified procedures were in place to identify confidential information requiring destruction when the end of the retention period was reached.	No exceptions noted.

CONFIDENTIALITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
C 1.2.2	Formal data retention and disposal procedures are in place to guide the secure disposal of data that has been identified for destruction in a manner that prevents loss, theft, misuse, or unauthorized access.	**Inspection:** Obtained and reviewed the Document Retention and Disposal Policy. Verified formal data retention and disposal procedures were in place to guide the secure disposal of data that had been identified for destruction in a manner that prevented loss, theft, misuse, or unauthorized access.	No exceptions noted.
C 1.2.3	On an as-needed basis, confidential information is identified either through data retention requirements, contractual obligations, or customer requests, and the data is securely sanitized, wiped, or destroyed.	**Inspection:** Obtained and reviewed the deletion request communication for the sampled deletion requests during the audit period. Verified on an as-needed basis, confidential information was identified either through data retention requirements, contractual obligations, or customer requests, and the data was securely sanitized, wiped, or destroyed.	No exceptions noted.
C 1.2.4	Prior to disposal, all electronic media is securely wiped and sanitized to removal all data and software.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of disposals during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Document Retention and Disposal Policy, and verified all electronic media is securely wiped and sanitized to removal all data and software prior to disposal.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
PI 1.1.1	Information specifications are defined with each customer, including the scope of services, data definitions, Service Level Agreements, system architecture, and other deliverables.	**Inspection:** Obtained and reviewed the Master Service Agreement and Data Processing Agreement. Verified information specifications were defined with each customer, including the scope of services, data definitions, Service Level Agreements, system architecture, and other deliverables.	No exceptions noted.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.1.2	Definitions of data are available to authorized users and include: • The population of events or instances included in the data • The nature of each element (e.g., field) of the data (that is, the event or instance to which the data element relates) • Source(s) of the data • The unit(s) of measure of data elements (e.g., fields) • The accuracy/precision of measurement • The uncertainty or confidence interval inherent in each data element and in the population of those elements • The date the data was observed or the period of time during which the events relevant to the data occurred • The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements and population	**Inspection:** Obtained and reviewed the data dictionary. Verified definitions of data were available to authorized users and included: • The population of events or instances included in the data • The nature of each element (e.g., field) of the data (that is, the event or instance to which the data element relates) • Source(s) of the data • The unit(s) of measure of data elements (e.g., fields) • The accuracy/precision of measurement • The uncertainty or confidence interval inherent in each data element and in the population of those elements • The date the data was observed or the period of time during which the events relevant to the data occurred • The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements and population	No exceptions noted.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
PI 1.2.1	Processing characteristics are defined as part of the system architecture.	**Inspection:** Obtained and reviewed the Data Flow Diagram and Data Classification Policy. Verified processing characteristics were defined as part of the system architecture.	No exceptions noted.
PI 1.2.2	The Company logs and monitors data to ensure that services are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed the import exception report and communication. Verified the Company logged and monitored data to ensure that services were provided in accordance with contractual obligations.	No exceptions noted.
PI 1.2.3	Employment eligibility and direct deposit verification are performed automatically by the system upon data entry of payment details for onboarding workers.	**Inspection:** Obtained and reviewed the employment and direct deposit verification. Verified employment eligibility and direct deposit verification were performed automatically by the system upon data entry of payment details for onboarding workers.	No exceptions noted.
PI 1.2.4	Account Manager reviews onboarding paperwork and confirms that the paperwork is complete.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the onboarding reviews for the sampled employee deployments during the audit period. Verified the account Manager reviewed onboarding paperwork and confirmed that the paperwork was complete.	No exceptions noted.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.2.5	Account Manager completes a quality check of the data entered and exported to the payroll system.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the quality control status for the sampled employee placements during the audit period. Verified Account Manager completed a quality check of the data entered and exported to the payroll system.	No exceptions noted.
PI 1.2.6	Timecards are approved by Supervisor.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the timecard approval for the sampled deployed employees during the audit period. Verified timecards were approved by Supervisor.	No exceptions noted.
PI 1.2.7	System checks are in place to ensure accuracy of timecards and paychecks.	**Inspection:** Obtained and reviewed the Payroll and Proofing error scripts. Verified system checks were in place to ensure accuracy of timecards and paychecks.	No exceptions noted.
PI 1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
PI 1.3.1	Processing characteristics are defined as part of the system architecture.	**Inspection:** Obtained and reviewed the Data Flow Diagram and Data Classification Policy. Verified processing characteristics were defined as part of the system architecture.	No exceptions noted.
PI 1.3.2	The Company logs and monitors data to ensure that services are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed the import exception report and communication. Verified the Company logged and monitored data to ensure that services were provided in accordance with contractual obligations.	No exceptions noted.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.3.3	The Company's services are monitored to ensure that they are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed screenshots of the processing monitoring and the import exception report and communication. Verified the Company's services were monitored to ensure that they are provided in accordance with contractual obligations.	No exceptions noted.
PI 1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.		
PI 1.4.1	The Company protects data as appropriate according to legal, industry, client specifications.	**Inspection:** Obtained and reviewed the privacy notices. Verified the Company protected data as appropriate according to legal, industry, client specifications.	No exceptions noted.
PI 1.4.2	The Company's services are monitored to ensure that they are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed screenshots of the processing monitoring and the import exception report and communication. Verified the Company's services were monitored to ensure that they are provided in accordance with contractual obligations.	No exceptions noted.
PI 1.4.3	The Company logs and monitors data to ensure that services are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed the import exception report and communication. Verified the Company logged and monitored data to ensure that services were provided in accordance with contractual obligations.	No exceptions noted.
PI 1.4.4	The payroll week requires transactions have been posted and invoiced.	**Inspection:** Obtained and reviewed the payroll invoice log for the sampled weeks during the audit period. Verified the payroll week required transactions had been posted and invoiced.	No exceptions noted.

PROCESSING INTEGRITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
PI 1.4.5	Invoices are delivered electronically in accordance with contractual obligations.	**Inspection:** Obtained and reviewed the email invoicing configuration. Verified Invoices were delivered electronically in accordance with contractual obligations.	No exceptions noted.
PI 1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.		
PI 1.5.1	The Company protects data as appropriate according to legal, industry, client specifications.	**Inspection:** Obtained and reviewed the privacy notices. Verified the Company protected data as appropriate according to legal, industry, client specifications.	No exceptions noted.
PI 1.5.2	The Company's services are monitored to ensure that they are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed screenshots of the processing monitoring and the import exception report and communication. Verified the Company's services were monitored to ensure that they are provided in accordance with contractual obligations.	No exceptions noted.
PI 1.5.3	The Company logs and monitors data to ensure that services are provided in accordance with contractual obligations.	**Inspection:** Obtained and reviewed the import exception report and communication. Verified the Company logged and monitored data to ensure that services were provided in accordance with contractual obligations.	No exceptions noted.