System and Organization Controls (SOC) 2 Type II
Report on Management's Description of its

Time and Attendance, Point of Sale, and Payroll Systems

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to Security, Availability, Confidentiality, and Processing Integrity

For the Period
October 1, 2022, to December 31, 2022

Together with
Independent Service Auditors' Report

Table of Contents

I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of Workwell Technologies Inc (Workwell)

Scope

We have examined Workwell's accompanying description of its Time and Attendance, Point of Sales, and Payroll Systems titled "Description of Workwell's Time and Attendance, Point of Sales, and Payroll Systems" throughout the period October 1, 2022 to December 31, 2022 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2022 to December 31, 2022, to provide reasonable assurance that Workwell's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Processing Integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Workwell 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 Workwell's service commitments and system requirements were achieved. Workwell has provided the accompanying assertion titled "Assertion of Workwell Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Workwell 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 Auditors' 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, 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 the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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.

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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of 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 and 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 IV.

Opinion

In our opinion, in all material respects,

a. the description presents Workwell's Time and Attendance, Point of Sales, and Payroll Systems that was designed and implemented throughout the period October 1, 2022, to December 31, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to December 31, 2022, to provide reasonable assurance that Workwell'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 organization and user entities applied the complementary controls assumed in the design of Workwell's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2022 to December 31, 2022, to provide reasonable assurance that Workwell'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 Workwell's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Workwell, user entities of Workwell's Time and Attendance, Point of Sales, and Payroll Systems during some or all of the period October 1, 2022 to December 31, 2022, business partners of Workwell subject to risks arising from interactions with the Time and Attendance, Point of Sales, and Payroll Systems, 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 these specified parties.

San Jose, California

February 24, 2023

II. Assertion of Workwell Management

Assertion of Workwell Management

We have prepared the accompanying description of Workwell Technologies Inc's (Workwell) Time and Attendance, Point of Sales, and Payroll Systems titled "Description of Workwell's Time and Attendance, Point of Sales, and Payroll Systems" throughout the period October 1, 2022 to December 31, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*. The description is intended to provide report users with information about the Time and Attendance, Point of Sales, and Payroll Systems that may be useful when assessing the risks arising from interactions with Workwell's system, particularly information about system controls that Workwell 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, Availability, Confidentiality, and Processing Integrity (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

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

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

a. the description presents Workwell's Time and Attendance, Point of Sales, and Payroll Systems that was designed and implemented throughout the period October 1, 2022, to December 31, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to December 31, 2022, to provide reasonable assurance that Workwell'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 organization and user entities applied the complementary controls assumed in the design of Workwell's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2022 to December 31, 2022, to provide reasonable assurance that Workwell'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 Workwell's controls operated effectively throughout that period.

Signed by Workwell Management

February 24, 2023

III. Description of Workwell's Time and Attendance, Point of Sales, and Payroll Systems

Description of Workwell's Time and Attendance, Point of Sales, and Payroll Systems

Company Background

Workwell Technologies was founded in 2005 with a vision of providing merchant credit card processing and other business enabling tools for small to mid-size businesses.

Workwell Technologies is the leader in time and attendance solutions built specifically for small and mid-size companies. Their commitment to delivering well designed solutions allows their customers to manage hourly employees with ease and efficiency. They expertly automate vital business tasks, leaving you free to focus on things that matter, like growing your business.

Services Provided

Workwell's cloud based products helps employers capture employee time and attendance for their employees. Our time and attendance products allow for robust rules configuration for configuring time and attendance rules such as overtime, breaks, and lunches. Additionally, our time and attendance systems export time data to hundreds of payroll platforms to facilitate payroll processes.

Principal Service Commitments and System Requirements

Workwell designs its processes and procedures related to meet its objectives for its cloud services. Those objectives are based on the service commitments that Workwell makes to user entities, the laws and regulations that govern the provision of cloud services, and the financial, operational, and compliance requirements that Workwell has established for the cloud services.

Security commitments to user entities are documented and communicated in End User License Agreements (EULAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Customer data is always encrypted at rest and in transit
- The platform is housed in state-of-the-art cloud environments that are SOC 2 Type II compliant.
- The platform is continuously monitored and tested for any security vulnerabilities or unexpected Changes.
- The platform security enables segregation of responsibilities and application functional access.
- Workwell provides access to customer data on a need-to-know basis only. All employee access to the platform is audited to assure access levels are never-out-of-date.
- Workwell employees authorized to work with customers and their data are trained to handle data properly and never expose the data via insecure practices.
- Workwell monitors its cloud services 24/7/365 and routes incidents immediately to all on call resources for immediate resolution.

Workwell establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Workwell's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Workwell cloud services.

Components of the System

Infrastructure

Workwell is hosted within Amazon Web Services' (AWS) Elastic Compute Cloud (EC2) and consists of a multi-tier virtualized architecture comprised of web and database servers, storage and content delivery systems, and network and application monitoring and logging tools. Workwell does not own or maintain any of the hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations) and Workwell is responsible for securing the platform deployed in AWS (i.e., customer data, applications, identity access management, operating system and network firewall configuration, network traffic, server-side encryption).

The AWS services are replicated across multiple regions and availability zones. In the event of a disaster, the service is able to failover to the secondary site. In addition, regular data backups are performed.
The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below.

Primary Infrastructure		
Hardware	Type	Purpose
AWS	VPC, EC2, RDS, IAM, CloudTrail, Cloudwatch, Config, ALB, GuardDuty, Inspector, Lambda, QuickSight, MQ, SNS, SQS	Used to host all products excluding some Payroll. Payroll in the process of migrating to AWS.
Peak10	Colo	Used to host Payroll.

Software

Workwell utilizes various vendor and internal tools to support the in-scope systems. The following list includes the supporting tools:

Primary Software	
Software	Purpose
Sentry.io	Exception logging
PagerDuty	Alerting/Monitoring
NodePing	Alerting/Monitoring
LastPass	Password vault
Jira	Project management
Confluence	Project management
TrendMicro Cloud One	Cloud security
QADeputy	Test management
Rapid7	Security
DataDog	Alerting/Monitoring
Eset	Security
TrueVault	3rd party PII and sensitive data vault
Arpio	Disaster Recovery
DynaTrace	APM solution

People

Workwell has a staff of approximately 90 employees organized in the following functional areas:

- Executives – responsible for the overall vision and success of the company.
- Engineering – responsible for developing, maintaining, securing, monitoring, and scaling products.
- Product Management – responsible for product roadmaps, product design, product specifications, and product communication.
- Marketing – responsible for marketing of all products.
- Sales – responsible for internal and external sales of all products and services.
- Customer Service – responsible for customer service via chat, phone, and email. Additionally, responsible for product help documentation.
- Finance – responsible for AP, AR, forecasting, and shipping.
- Payroll Operations – Responsible for all operations related to payroll processing and support.
- QC -responsible for QC'ing new hardware inventory, shipping, and RMA's.
- HR - HR
- IT – Responsible for internal IT (not product related).

Data

- Configuration Data: Data used to configure Workwell products
- Application Data: Data collected in Workwell's SaaS applications to facilitate primary functionality of the system.
- Log Data: Logs, traces, and samples produced by Workwell's systems to audit, identify issues, and record system events.

Configuration Data is stored in Workwell's MySQL databases and includes:

- Data related to account level configuration.
- Data related user level configuration.
- Lookup data for common functionality (i.e., State lookup).
- Mapping data for 3rd party integrations.

Application Data is data collected in product, by customers, to achieve core functionality of the product. Customers can invite other people in their company to access their Workwell organization and read and write application data. Workwell operators may access application data to troubleshoot customer issues or to gather feedback for improving the Workwell product.

Log Data is produced by the infrastructure, monitoring tools, and APM tools to make it easier for Workwell engineers to monitor the health and security of the system and track down any issues.

Log data will include snapshots of **Configuration and Application Data**. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include non PII **Application Data** captured by automatic tracers.

Log data may be stored by vendors that Workwell has entrusted for purposes like indexing, monitoring, and trending.

All data types processed by Workwell are encrypted on the wire – no networking connections used by Workwell for any purpose will ever send unencrypted data. In addition, all **Configuration Data** and **Log Data**, as well as samples of **Application Data** stored by Workwell is encrypted at rest, in databases, caches, and cloud storage.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Workwell policies and procedures that define how services should be delivered. These are located on the Company's Drata environment and can be accessed by any Workwell team member.

Physical Security

All Workwell system's centralized data storages are housed in SOC 2 Type II data centers that have extremely high levels of physical security.

These data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Only approved employees with specific roles may enter.

Workwell office locations do not house any computer equipment for central storage of customer or confidential data.

The Workwell main office has a fob controlled entry with each employee receiving their own fob for office access. All visitors to the Workwell office are required to sign in at the main door, which is the only authorized access for all visitors.

Upon an employee's termination, the Workwell IT team ensures the employee's fob is deactivated.

Logical Access

AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Workwell applications reside.

Workwell has implemented role-based security to limit and control access within the Workwell instances or any system that houses customer or confidential data. Employees are granted logical access to these

systems based on documented approvals by appropriate management personnel. User access is reviewed biannually both via the review of the access list and audits of existing system access control list ("ACL").

Unique usernames and passwords are required to authenticate all users to Workwell systems, infrastructure, and business systems. Passwords have complexity requirements and have expiration settings that fit the classification of data contained within the system.

When an employee is terminated, HR team notifies the IT team through initiation of the offboarding process. Offboarding steps include revocation of all system access. Offboarding forms are signed off by HR and IT.

Computer Operations – Backups

Workwell has multiple redundant backup strategies in place for the production environments. These include database backups 1 hour that are encrypted and transferred (over encrypted transport) to AWS DR environments.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Peak10 infrastructure is backed up daily via BackupMyPC.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Workwell monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches expectations. Workwell evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Application Servers
- Database Servers
- Disk Storage
- I/O Capacity
- Network bandwidth

Workwell has implemented an automated patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Workwell system owners review proposed operating system patches to determine whether the

patches are applied. Workwell systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Workwell staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Workwell has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed.

The engineering team meets as needed to review and schedule changes to the IT environment. Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, only key developers have the ability to migrate changes into production environments.

Workwell has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

Workwell uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with Workwell's patch management process.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. Rapid 7's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a

disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, Rapid7 attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by Rapid 7 on a monthly basis. Rapid 7 uses industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Services performed by Workwell. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. 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.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). 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. For example, the information may be proprietary, intended only for entity personnel. 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
Processing integrity provides assurance that data in the audited system is complete, valid, accurate, timely and authorized to fully satisfy the entity's objectives. The processing integrity criteria tests that there are no errors in processing, and if there are, errors are corrected appropriately. Processing integrity criteria also focuses on inputs and outputs to the system, ensuring they are accurate throughout the processing of any actions within the system. Finally, the criteria involved with processing integrity ensure that the data is stored and maintained appropriately while under the service organization's care and responsibility.

Control Environment

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 Workwell's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Workwell's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.

- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

The Workwell management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Workwell can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Workwell to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

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

Organizational Structure and Assignment of Authority and Responsibility

Workwell's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and

responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

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

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

Human Resource Policies and Practices

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

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

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

Risk Assessment Process

Workwell maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information and data assets are subject to the data classification policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security and disposal of information system assets.

On an annual basis, the information security team performs a risk assessment that identifies internal and external threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners with consideration for the cyber threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by relevant management against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

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

Information and Communications Systems

Information and communication are an integral component of Workwell's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Workwell uses several information and communication channels internally to share information with management, employees, contractors, and customers. Workwell uses chat systems (Slack and MS Teams) and email as the primary internal and external communications channels. In addition, Workwell communicates with customers via the ZenDesk customer support application.

Structured data is communicated internally via our SaaS applications (finance information in NetSuite) and our project management tools (Jira). Finally, Workwell uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

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

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Workwell's Time and Attendance, Point of Sales, and Payroll Systems.

Subservice Organizations

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

The following subservice organization controls should be implemented by AWS and Peak10 to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - 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.	The subservice organization is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Workwell's system resides.
CC6.2 - 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.	
CC6.3 - 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.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.5 - 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.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - 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.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	The subservice organization is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where Workwell's system resides.
Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The subservice organization is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where Workwell's system resides.

Workwell Technologies Inc management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Workwell Technologies Inc performs monitoring of the subservice organization controls, including the following procedures:

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

Complementary User Entity Controls

Workwell's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Workwell's services to be solely achieved by Workwell's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Workwell's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Workwell.
2. User entities are responsible for notifying Workwell of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Workwell services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Workwell services.
6. User entities are responsible for providing Workwell with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Workwell of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Criteria, Controls, Tests and Results of Tests

Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Workwell related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Workwell's controls were suitably designed and operating effectively to achieve the specified criteria for the Security, Availability, Processing Integrity, and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period October 1, 2022 to December 31, 2022.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Workwell activities and operations and inspection of Workwell documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Workwell controls, this test was not listed individually for every control in the tables below.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
The entity has a documented code of conduct that includes its commitments to integrity and ethical values.	CC1.1.1	Inspected the entity's code of conduct to determine that it included its commitments to integrity and ethical values.	No exceptions noted
Personnel are required to read and accept the code of conduct upon being hired.	CC1.1.2	Inspected signed acknowledgements to determine that the code of conduct was acknowledged by new hires upon being hired.	No exceptions noted
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.1.3	Inspected background checks for a sample of new hires to determine that background checks were completed for all new hires as a condition of their employment, as permitted by local laws.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	CC1.2.1	Inspected the Code of Conduct, Information Security Policy, and evidence of management's review of the policies, to determine that the company demonstrates a commitment to integrity and ethical values.	No exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC1.3.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
An organizational chart has been defined to appropriately document reporting lines in terms of information security.	CC1.3.2	Inspected the organizational chart to determine that reporting lines had been appropriately defined for information security.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
Job requirements and responsibilities are documented in job descriptions.	CC1.4.1	Inspected a job description to determine that job requirements and responsibilities were documented.	No exceptions noted
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.4.2	Inspected background checks for a sample of new hires to determine that background checks were completed for all new hires as a condition of their employment, as permitted by local laws.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
Security awareness training is provided to all employees on an annual basis.	CC1.5.1	Inspected security awareness training confirmation for a sample of employees to determine that security awareness training was provided.	No exceptions noted
All employees are required to agree to the security policies upon hire. Management also ensures that security policies are accessible to all employees and contractors.	CC1.5.2	Inspected the security policy acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
The company uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	CC2.1.1	Inspected the Drata tool configurations to determine that the company uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	No exceptions noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Personnel are required to read and accept the code of conduct upon being hired.	CC2.2.1	Inspected signed acknowledgements to determine that the code of conduct was acknowledged by new hires upon being hired.	No exceptions noted
Personnel are required to read and accept an acceptable use agreement upon being hired.	CC2.2.2	Inspected signed acceptable use agreements to determine that new hires were required to read and accept acceptable use agreements.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Privacy policies are posted on the entity's website to communicate the entity's privacy practices.	CC2.3.1	Inspected the entity's website to determine that the entity's privacy policies were posted.	No exceptions noted
The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	CC2.3.2	Inspected the company's Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC3.1.1	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
CC3.2 - 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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.2.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC3.2 - 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.			
When identifying risks to include in the risk assessment, the entity considers relevant laws and regulations specific to the types of data they possess (i.e. Protected Health Information, Personally Identifiable Information, etc.).	CC3.2.2	Inspected the completed risk assessment to determine that the entity considered relevant laws and regulations specific to the types of data they possess, when identifying risks to include in the risk assessment.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.3.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC3.4.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.4.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC4.0 - Monitoring Activities			
CC4.1 - 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.			
Cloud infrastructure is monitored through AWS monitoring that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	CC4.1.1	Inspected cloud infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted
Monitoring configured to identify suspicious activity. When anomalous traffic activity is identified, the web application firewall appropriately blocks malicious traffic.	CC4.1.2	Inspected AWS monitoring logs to determine that monitoring was configured to identify suspicious activity and when anomalous traffic activity is identified, the web application firewall appropriately blocks malicious traffic.	No exceptions noted
CC4.2 - 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.			
The entity has incident response policies and procedures in place that includes plans for escalating to internal personnel.	CC4.2.1	Inspected the entity's incident response policies and procedures to determine that the incident response policies and procedures included plans for escalating to internal personnel.	No exceptions noted
The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	CC4.2.2	Inspected the support page to determine that the company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.0 - Control Activities			
CC5.1 - 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.			
As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	CC5.1.1	Inspected the risk assessment that was completed within the year to determine that risks were linked to controls and that new controls were considered for any risks not adequately addressed by existing controls.	No exceptions noted
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC5.1.2	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC5.2.1	Inspected the scan results to determine that vulnerability scans were performed to identify security issues.	No exceptions noted
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC5.2.2	Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
IT and security policies are defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems. IT and security policies are reviewed by appropriate members of management on an annual basis.	CC5.3.1	Inspected the IT and security policies to determine that IT and security policies were defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems.	No exceptions noted
		Inspected management's review of IT and security policies to determine that IT and security policies were reviewed by appropriate members of management on an annual basis.	No exceptions noted
Management has approved the company's security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC5.3.2	Inspected the company's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted
		Inspected the security policy acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
CC6.0 - Logical and Physical Access Controls			
CC6.1 - 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.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.1	Inspected the infrastructure configurations to determine that unique infrastructure accounts were required.	No exceptions noted
No public SSH is allowed.	CC6.1.2	Inspected SSH configurations to determine that no public SSH is allowed.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.2 - 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.			
Prior to granting new hires access to system resources, HR must submit a completed access request form.	CC6.2.1	Inspected the access request form for a sample of new hires to determine that HR must submit a completed access request form prior to granting new hires access to system resources.	No exceptions noted
A termination checklist is completed to ensure that system access, including physical access, for terminated employees has been removed within one business day.	CC6.2.2	Inspected the termination checklist for a sample of terminated employees to determine that employee access to infrastructure is removed as a component of the termination process.	No exceptions noted
CC6.3 - 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.			
The company's access reviews are performed on an annual basis.	CC6.3.1	Inspected the access review to determine that an access review was completed for the company on an annual basis.	No exceptions noted
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	CC6.4.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.5 - 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.			
Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	CC6.5.1	Inspected the Data Deletion Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Inbound and outbound traffic to in-scope systems and environment is appropriately restricted and allowed by exception.	CC6.6.1	Inspected firewall rules to determine that inbound and outbound traffic to in-scope systems and environment was appropriately restricted.	No exceptions noted
Cloud Provider IDS/IPS are in place to detect or prevent malicious traffic.	CC6.6.2	Inspected the AWS cloud firewalls configurations to determine it was appropriately deployed and was configured to appropriately block malicious traffic.	No exceptions noted
Multi-factor authentication (MFA) is required to access the AWS Management Console.	CC6.6.3	Inspected AWS Management Console configurations to determine that MFA was required in order to access the infrastructure.	No exceptions noted
CC6.7 - 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.			
The company uses appropriate encryption standards to ensure confidential information is encrypted in transit.	CC6.7.1	Inspected the company's login page and obtained the website certificate to determine that a valid certificate was in place.	No exceptions noted
Customer data at rest is encrypted.	CC6.7.2	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.7 - 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.			
Full-disk encryption is implemented for all workstations and laptops.	CC6.7.3	Inspected workstation and laptop encryption settings to determine that full-disk encryption was implemented for all workstations and laptops.	No exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Antivirus software is installed on workstations to protect the network against malware.	CC6.8.1	Inspected antivirus configurations to determine that antivirus software was installed on workstations and servers to protect the network against malware.	No exceptions noted
CC7.0 - System Operations			
CC7.1 - 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.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC7.1.1	Inspected the scan results to determine that vulnerability scans were performed to identify security issues.	No exceptions noted
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC7.1.2	Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.2 - 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.			
Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	CC7.2.1	Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	No exceptions noted
Access to the cloud source code version control system is restricted to appropriate personnel.	CC7.2.2	Inspected the version control tool configurations to determine that access was restricted to appropriate personnel.	No exceptions noted
CC7.3 - 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.			
The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.3.1	Inspected the Incident Response Policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted
The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	CC7.3.2	Inspected the Incident Response Plan to determine that the company has policies and procedures that are documented and communicated to authorized users.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.3 - 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.			
The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	CC7.3.3	Inspected the incident ticket for a sample of security and privacy incidents to determine that incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	N/A - A security incident did not occur during October 1, 2022-December 31, 2022 so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed Risk Management Policy and security incident tracking tool to confirm the control was appropriately designed.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.4.1	Inspected the Incident Response Policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted
The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	CC7.4.2	Inspected the Incident Response Plan to determine that the company has policies and procedures that are documented and communicated to authorized users.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	CC7.4.3	Inspected the incident ticket for a sample of security and privacy incidents to determine that incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	N/A - A security incident did not occur during October 1, 2022-December 31, 2022 so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed Risk Management Policy and security incident tracking tool to confirm the control was appropriately designed.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
Business and system recovery plans are documented, which provide roles and responsibilities and detailed procedures for recovery of systems.	CC7.5.1	Inspected Business Continuity Plan to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
A software development life cycle policy is defined to ensure that appropriate controls are in place over the acquisition, development, and maintenance of technology and its infrastructure.	CC8.1.1	Inspected the software development life cycle policy to determine that a software development life cycle policy was defined to ensure that appropriate controls were in place over the acquisition, development, and maintenance of technology and its infrastructure.	No exceptions noted
Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	CC8.1.2	Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	No exceptions noted
Access to the cloud source code version control system is restricted to appropriate personnel.	CC8.1.3	Inspected the list of users with access to the cloud source code version control system to determine that access was restricted to appropriate personnel.	No exceptions noted
Code changes to the company are tested prior to implementation.	CC8.1.4	Inspected test results to determine that code changes were tested prior to implementation.	No exceptions noted
The company's releases are approved by appropriate personnel prior to the release being implemented in production.	CC8.1.5	Inspected a change ticket for a sample of changes to determine that releases were approved by appropriate personnel prior to the release being implemented in production.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC9.1.1	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC9.1.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
The company has created a business continuity plan to define the criteria for continuing business operations for the organization in the event of a disruption.	CC9.1.3	Inspected the Business Continuity Plan to determine that it defined an operational and organizational strategy in the event of a disruption and has been updated in the past year.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company's team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	CC9.2.1	Inspected the written policy governing the use of external service providers to determine that the sub-service organization approval process includes collecting and reviewing the provider's SOC report(s).	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	CC9.2.2	Inspected the vendor review to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	N/A - No vendors were reviewed over the audit period, so auditor was unable to conclude on the operating effectiveness of the control. Auditor examined the vendor management policy to determine that the control was appropriately designed.
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
Cloud infrastructure is monitored through AWS monitoring that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	A1.1.1	Inspected cloud infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	A1.2.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	A1.3.1	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
The entity has documented a disaster recovery plan that is tested annually to ensure that recovery procedures are complete and accurate.	A1.3.2	Inspected the annual disaster recovery exercise to determine that the Company's disaster recovery plan is tested annually to ensure that recovery procedures are complete and accurate.	No exceptions noted
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
The entity establishes written policies related to retention periods for the confidential information it maintains.	C1.1.1	Inspected the Data Protection Policy to determine that the entity established written policies related to retention periods for the confidential information it maintains.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
The entity has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.	C1.1.2	Inspected the Data Classification Policy to determine that the entity had established a Data Classification Policy in order to identify the types of confidential information possessed by the entity and types of protection that were required.	No exceptions noted
Customer data at rest is encrypted.	C1.1.3	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted
Full-disk encryption is implemented for all workstations and laptops.	C1.1.4	Inspected workstation and laptop encryption settings to determine that full-disk encryption was implemented for all workstations and laptops.	No exceptions noted
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	C1.1.5	Inspected the infrastructure configurations to determine that unique infrastructure accounts were required.	No exceptions noted
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Formal policies and procedures are in place to guide personnel in the disposal of any sensitive data.	C1.2.1	Inspected the Data Deletion Policy to determine that formal policies and procedures were in place to guide personnel in the disposal of paper documents and hardware containing sensitive data.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
PI1.0 - Additional Criteria for Processing Integrity (over the provision of services or the production, manufacturing, or distribution of goods)			
PI1.1 - 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.			
The entity's application edits limit input to acceptable value ranges	PI1.1.1	Inspected the application requiring limit to input to acceptable value ranges to determine only acceptable value ranges.	No exceptions noted
The entity's system edits require mandatory fields to be complete before record entry is accepted.	PI1.1.2	Observed the application requiring mandatory fields to be completed before record entry is accepted to determine that the application required mandatory fields to be completed before record entry was accepted.	No exceptions noted
PI1.2 - 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.			
The entity's application edits limit input to acceptable value ranges	PI1.2.1	Inspected the application requiring limit to input to acceptable value ranges to determine only acceptable value ranges.	No exceptions noted
The entity's system edits require mandatory fields to be complete before record entry is accepted.	PI1.2.2	Observed the application requiring mandatory fields to be completed before record entry is accepted to determine that the application required mandatory fields to be completed before record entry was accepted.	No exceptions noted
PI1.3 - The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
The entity does application regression testing to validate key processing for the application during the change management process.	PI1.3.1	Inspected the change tickets for an example software changes to determine that application regression testing is performed to validate key processing for the application during the change management process.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
PI1.4 - 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.			
The entity does application regression testing to validate key processing for the application during the change management process.	PI1.4.1	Inspected the change tickets for an example software changes to determine that application regression testing is performed to validate key processing for the application during the change management process.	No exceptions noted
Role-based security is in place for internal and external users, including super admin users.	PI1.4.2	Inspected user groups and federated roles to determine that role-based security is implemented for accessing systems and resources.	No exceptions noted
PI1.5 - 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.			
Customer data at rest is encrypted.	PI1.5.1	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted
The entity utilizes multiple availability zones to replicate production data across different zones.	PI1.5.2	Inspected availability zone configurations to determine that the company utilizes multiple availability zones to replicate production data across different zones.	No exceptions noted
Prior to granting new hires access to system resources, HR must submit a completed access request form.	PI1.5.3	Inspected the access request form for a sample of new hires to determine that HR must submit a completed access request form prior to granting new hires access to system resources.	No exceptions noted