Report on Logicworks Systems Corporation's Description of Its Managed Cloud Operations and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period February 1, 2022 to January 31, 2023

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Logicworks Systems Corporation ("Logicworks")

Scope

We have examined Logicworks' accompanying description in Section 3 titled "Logicworks Systems Corporation's Description of Its Managed Cloud Operations Throughout the Period February 1, 2022 to January 31, 2023" (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022*) (2018 description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Logicworks' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

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

Logicworks uses subservice organizations to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Logicworks, to achieve Logicworks' service commitments and system requirements based on the applicable trust services criteria. The description presents Logicworks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Logicworks' 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.

Service Organization's Responsibilities

Logicworks 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 Logicworks' service commitments and system requirements were achieved. In Section 2, Logicworks has provided the accompanying assertion titled "Assertion of Logicworks Systems Corporation Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Logicworks 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 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.

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

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.

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 Relevant to the Security, Availability, and Confidentiality Categories” of this report.

Opinion

In our opinion, in all material respects—

a. The description presents Logicworks’ Managed Cloud Operations that were designed and implemented throughout the period February 1, 2022 to January 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Logicworks’ 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 Logicworks’ controls throughout that period.

c. The controls stated in the description operated effectively throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Logicworks’ 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 Logicworks’ 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 Logicworks, user entities of Logicworks’ Managed Cloud Operations during some or all of the period February 1, 2022 to January 31, 2023, business partners of Logicworks subject to risks arising from interactions with Logicworks’ Managed Cloud Operations, 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. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Westminster, Colorado
April 12, 2023

Section 2

Assertion of Logicworks Systems Corporation Management

Assertion of Logicworks Systems Corporation ("Logicworks") Management

We have prepared the accompanying description in Section 3 titled "Logicworks Systems Corporation's Description of Its Managed Cloud Operations Throughout the Period February 1, 2022 to January 31, 2023" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (2018 description criteria). The description is intended to provide report users with information about the Managed Cloud Operations that may be useful when assessing the risks arising from interactions with Logicworks' system, particularly information about system controls that Logicworks 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, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

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

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

a. The description presents Logicworks' Managed Cloud Operations that were designed and implemented throughout the period February 1, 2022 to January 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Logicworks' 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 Logicworks' controls throughout that period.

c. The controls stated in the description operated effectively throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Logicworks' 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 Logicworks' controls operated effectively throughout that period.

Logicworks Systems Corporation

Section 3

Logicworks Systems Corporation's Description of Its Managed Cloud Operations Throughout the Period February 1, 2022 to January 31, 2023

Type of Services Provided

Logicworks Systems Corporation ("Logicworks" or "the Company") is a software-enabled provider of Managed Cloud Operations services. Based in New York City, NY, Logicworks is a privately held company that began operations in 1993 as Digital Telemedia and, in 2002, changed its name to reflect its focus on managed dedicated server hosting. Logicworks employs approximately 200 employees, divided among the Executive; Go-to-Market (G2M); Professional Services (PS); Managed Services; People – Finance – Legal (PFL); Information Security (InfoSec); and Product groups.

Logicworks' Managed Cloud Operations comprise a custom solution in which the Company provides public, private, and hybrid cloud services. Customer cloud operations are delivered through a proprietary Cloud Reliability Platform (CRP) that combines world-class engineering talent, policy-as-code, and integrated tooling to enable customers to confidently meet compliance regulations, security requirements, cost control, and high availability.

Customers consume their own designated environments that utilize the Company's servers or public cloud infrastructure provided by Amazon Web Services (AWS) or Microsoft Azure (Azure). Customers select one of three Cloud Operations packages: Essential, Premium, and Complete.

Cloud Operations - Essential -	
Platform	Support
Logicworks Pulse	Dedicated Service Delivery Manager
Monitoring	24x7x365 Network Operations Support
Best Practice Scanners	Remote Hands
Backups	Data Lifecycle Management
Budget Dashboard	Change Management
Essential Services are included for all customers	

Cloud Operations - Premium -
Configuration Management
Designated Engineering Lead
Patching
Cost Management
Receive all Cloud Operations – Essentials features, plus the above Premium Services

Cloud Operations - Complete -
Data Loss Prevention
Quarterly Compliance Assessment
Alert Logic Cloud Defender
Trend Micro Antivirus
Threat Stack
Receive all Cloud Operations – Essentials and Premium Services features, plus the above security services

Figure 1: Logicworks' Cloud Operations Packages

Customers select from a suite of supported public cloud services, as well as physical servers, operating systems (OSs), firewalls, switches, backup and recovery services, and relational database management systems. The Company installs and configures a customer's chosen devices and/or software and manages customer architecture, monitoring, patching, configuration, cost, and security. Customer environments can be solely dedicated infrastructure or a mix of dedicated and shared infrastructure, with dedicated physical

and virtual resources, dedicated or shared enterprise-grade storage, and virtual resources hosted on shared computing resources in the public cloud.

The Company operates a customizable, scalable, network environment. Customers are able to customize their hosted environment (e.g., OS configurations) to meet their needs by installing any applications that do not interfere with the Company's Acceptable Use Policy. All customer environments are co-managed by Logicworks and the customer.

In providing its Managed Cloud Operations, Logicworks provides and takes responsibility for several aspects of a customer's infrastructure and applications, including server hardware; OSs; security; monitoring; issue resolution, recovery, and restoration; and select OS-specific applications.

The system description in this section of the report details Logicworks' Managed Cloud Operations. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the customer level or any subservice organizations (see below for further discussion of the subservice organizations).

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Managed Cloud Operations. Commitments are communicated in Master Service Agreements. The Company's principal service commitments related to the Managed Cloud Operations include the following:

- The Company guarantees that each high-availability application that has been successfully configured and tested for failover will be available to perform its required function 100 percent of the time.
- The Company will operate and maintain security measures designed to prevent unauthorized access.
- The Company will use the same degree of care to protect customer information that the Company uses to protect its own information from unauthorized disclosure, and in no event will the Company use less than a commercially reasonable degree of care.

As part of the Company's information security policy, the health and availability of the platform are monitored and communicated. Internal processes and Service Level Objectives (SLOs) between teams are in place to carry out the intent of the policy. Customers of the Company work with their Company representative to receive information.

System requirements are specifications regarding how the Managed Cloud Operations should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to employees at any time. The Company's system requirements related to the Managed Cloud Operations include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls, such as the use of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls

- Logging and monitoring controls
- System hardening standards
- Intrusion detection system

The Components of the System Used to Provide the Services

The boundaries of the Managed Cloud Operations are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Managed Cloud Operations.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Logicworks' Managed Cloud Operations are provided within Equinix data centers. Managed Cloud Operations for AWS and Azure are provided by utilizing resources within facilities run by AWS and Azure.

The Company replaces the hardware it owns and rents to its customers, such as general-purpose servers and special-purpose servers. Also, the Company replaces its dedicated firewalls, dedicated load balancers, and storage devices, appliances, and other on-premises hardware.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
VMware Hypervisor	Virtualization Layer for Private Cloud	VMware ESXi	On-premises
Linux Servers	Kubernetes Cluster, Bastion Hosts, AWS Platform Tools, Load Balancers, Domain Name System (DNS), Linux Firewalls	CentOS, Ubuntu	AWS, On-premises
Windows Servers	Domain Controllers, Authentication, Group Policy Objects (GPOs), Windows Service Update Services (WSUS), Bastion Hosts	Windows	AWS, On-premises
Networking Gear	Switches, Routers, Firewalls	PAN, JunOS, Extreme, Hewlett Packard (HP), Cisco, Cloud Native	AWS, On-premises
VNX	Storage	VNX OS	On-premises

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
Serverless Services on AWS	AWS Lambda, AWS Fargate, Amazon Event Bridge, AWS Step Functions, Amazon Simple Queue Service (SQS), Amazon Application Programming Interface (API) Gateway	Miscellaneous compute, application integration, data stores	AWS
Azure Serverless	Azure Kubernetes Serves, Azure Functions	Miscellaneous compute, database, storage	Azure

Software

Software consists of the programs and software that support the Managed Cloud Operations (OSs, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Logicworks' Managed Cloud Operations, excluding the AWS and Azure native services, include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Threat Stack	Security information and event management (SIEM), logging system, file integrity monitoring, intrusion detection and prevention
Logicworks Pulse	Application monitoring, reporting on service delivery and agent coverage
Sentry	Serverless error monitoring
Datadog	Application performance monitoring
Rubrik	Backup and replication
Sumo Logic	SIEM, logging system
CloudWatch Logs	Infrastructure monitoring
Packery, Package Managers, Custom Internal / Manual Processes	Patch management
Trend Micro	File integrity monitoring, antivirus, intrusion detection and prevention
Alert Logic	Intrusion detection and prevention
Jira Information Technology (IT) Service Desk	Help desk, ticketing system (hosted on-premises)
Confluence	Web-based collaboration workspace (hosted on-premises)
Tenable.io	Vulnerability management
NopSec	Unified vulnerability risk management

Software	
Production Application	**Business Function**
Okta	Cloud Single Sign-On (SSO), multi-factor authentication (MFA), credential store, and identity
Duo	Cloud SSO, MFA, credential store, and identity
HashiCorp Vault	Cloud SSO, MFA, credential store, and identity
Salesforce	Cloud SSO, MFA, credential store, and identity
ObserveIT	Session recording on bastion hosts
GitLab	Web-based DevOps lifecycle tool providing Git-based source code management for Infrastructure as Code (IaC)
PowerBI	Reporting on service delivery and agent coverage
Really Awesome New Cisco conflg Differ (RANCID)	Network monitoring and configuration file integrity
Axonius	Cybersecurity asset management
CyberArk	Endpoint privilege management

People

The Company develops, manages, and secures Logicworks' Managed Cloud Operations via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Information Security (InfoSec)	Responsible for ensuring the successful governance, risk, and compliance of Logicworks' Managed Cloud Operations, for producing policy and standards, and for evaluating adherence to standards. Includes the Risk Analysis team.
Product	Responsible for developing the platform tooling and CMP that Logicworks makes available to internal stakeholders and clients in the course of delivering Logicworks' Managed Cloud Operations.
Product Support (PS)	Responsible for the initial assessment, design, and implementation of cloud environments for customers migrating to the cloud, enhancing existing cloud operations, or adopting Logicworks' Managed Cloud Operations.
Go to Market (G2M)	Responsible for cultivating, developing, and prosecuting sales opportunities in the market. The Marketing team focuses on brand and content, demand generation, and partner marketing. The Alliances team focuses on developing partner relationships. The Sales team matures the input from Marketing and Alliances to help drive bookings and, eventually, revenue.

People	
Group/Role Name	**Function**
People, Finance and Legal (PFL)	Responsible for the Human Resources (People), Finance, and Legal operations supporting Logicworks' Managed Cloud Operations.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

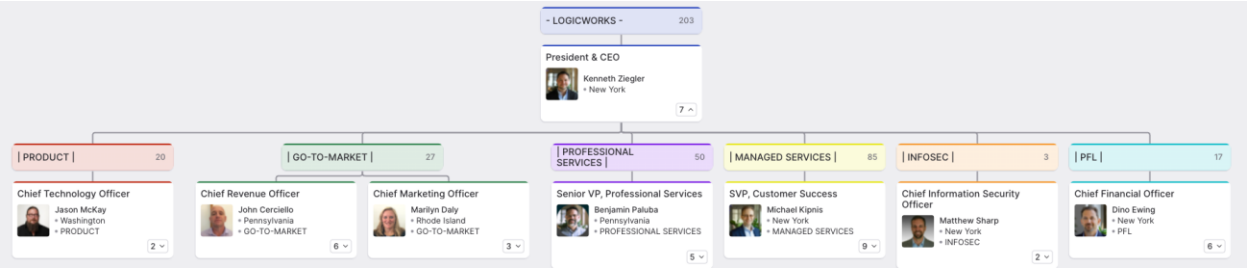

Figure 2: Logicworks Organization Chart

Managed Services Department

The Managed Services department directly supports both internal and client systems and environments. Managed Services consists of the following:

- Cloud Service Delivery group – provides ongoing client services, coupled with an understanding of the customer's technical requirements, to support their ongoing and changing operational requirements and business.
- Engineering – responsible for senior-level engineering support of customers whose managed services environments are more complex. Engineering has responsibility for the Company's service provider environment and for the support and resolution of complex issues escalated from the Network Operations Center (NOC). Engineering includes the roles and responsibilities defined below:
  - Senior Cloud Systems Engineers – focused on developing, maintaining, and supporting various technologies, such as networking, Linux, Windows, storage, and DevOps.
  - Cloud Systems Engineers – responsible for supporting Senior Systems Engineers in DevOps.
  - Database Administrators – responsible for installing and configuring database applications for both internal and customer use. They are responsible for supporting MySQL, Microsoft SQL, Oracle, and PostgreSQL solutions, including upgrading server software, installing patches for the database software, generating status reports, managing backups, and performing data restoration. They are also responsible for scripting and automating tasks related to database administration, helping to further define database offerings, developing internal systems used for customer support, and providing training and documentation for other engineers regarding database issues.
  - Network Architecture – responsible for the deployment and support of internal and client networking designs and devices within both private and public cloud environments.

  - Security Operations – responsible for the installation of and response to security alerts generated by the in-scope services and tools. They also provide updates to clients of emerging vulnerabilities and offer guidance on security best practices related to cloud native security tooling in AWS and Azure.

- NOC – responsible for fielding calls, email requests, and requests placed through the ticketing system (Jira) at all hours of the day, providing the equivalent of Tier 2 support and escalating to systems engineers and senior engineering groups to maintain SLOs. The NOC includes the roles and responsibilities defined below:
  - Tier 3 – Cloud Subject Matter Expert – has a solid understanding of Linux and Windows system administration and has a solid foundational knowledge and the ability to support AWS.
  - Tier 2 – Cloud Support Associate – focuses on obtaining either Linux or Windows system administration skills and mastering VMware and bare metal builds. This role has monitoring, backups, AlertLogic, and networking responsibilities, as well as basic AWS support. This is the main 24/7 support group within the department.
  - Tier 1 – Cloud Operations Specialist – typically consists of an entry-level IT job with a focus on soft skills. Communication with clients and ticket assessment are key for this role.
- Datacenter Operations group – responsible for performing any hands-on tasks that need to be undertaken at the various co-location facilities. They are stationed at the Company's data centers 24 hours a day, seven days a week. They also handle all AlertLogic incidents.
- Corporate IT – responsible for the Active Directory Domain and internal Okta tenant. Thus, this team performs provisioning and deprovisioning of employee access; management of user endpoints, including desktops and laptops; and active management of collaboration tools. They also implement configuration hardening of these systems.

Professional Services Department

The Professional Services Department is comprised of several different roles, including the following:

- Client Engagement Manager – responsible for project managing non-recurring projects, typically for the purposes of migrating a customer to the cloud or adding new workloads to an existing cloud deployment.
- Solutions Architect (SA) – responsible for understanding client requirements and designing solutions that leverage a combination of cloud native services, Logicworks intellectual property, and supported independent software vendors that comprise Logicworks' Managed Cloud Operations. SAs are active in the development of Service Orders and Cloud Solution Workbooks that document the scope and boundary of services delivered for non-recurring projects.
- Cloud Solutions Engineer – responsible for implementing the solutions designed by SAs.

Product Department

The Product Department is organized into three independent teams that develop the platform tools on AWS and Azure, as well as the Company's proprietary, customer-facing, web-based CMP, Logicworks Pulse. The Product team is comprised of the following:

- Technical Product Manager – determines requirements with internal and external stakeholders, schedules resources, and sets the development roadmaps by organizing work into bi-weekly sprints.

- Software Developer / Platform Engineer – writes software or platform code to enhance Logicworks operations or deliver the CMP.
- Quality Assurance (QA) / Software Development Engineer – performs testing to ensure that the development efforts meet minimum quality standards

Procedures

Procedures include the automated and manual procedures involved in the operation of the Managed Cloud Operations. The following table provides an overview of the subject matters addressed by various processes and procedures in place for Logicworks' Managed Cloud Operations.

The following tables detail the procedures as they relate to the operation of the Managed Cloud Operations:

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Managed Services Private Cloud	Managed AWS Public Cloud	Managed Azure Public Cloud
• Data centers • Logical access and data security • Customer access • Company access • Network security • System software change control • System and data backups • Production monitoring and issue resolution • Antivirus protection • Backup-as-a-Service	• Logical access and data security • Client access • Company access • Network security • System software change control • System and data backups • Production monitoring and issue resolution • Anti-malware protection and integrity monitoring • Intrusion detection	• Logical access and data security • Client access • Company access • Network security • System software change control • System and data backups • Production monitoring and issue resolution • Anti-malware protection and integrity monitoring • Intrusion detection

Additionally, the following procedures are used internally by the Company:

- Customer Onboarding Procedures – the Company collaborates with customers for onboarding. During the onboarding phase, the Company's Professional Services team, Client Engagement Managers, and Service Delivery group work with customers on technical adoption and alignment of architecture to requirements for security and applications.

- Platform Availability Monitoring Procedures – as part of the Company's information security policy, the health and availability of Logicworks' Managed Cloud Operations are monitored and communicated. Internal processes and Operating Level Agreements between teams are in place to carry out the intent of the policy. Customers of the Company work with their representative to receive information.
- Security Incident Policy and Procedures – as part of the Company's information security policy, security incidents are monitored and communicated. Internal processes and SLOs between teams are in place to carry out the intent of the policy. Customers of the Company work with their representative to receive information. If the Company has a contractual obligation on disclosure, it is carried out through the office of the General Counsel

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. The Company does not encrypt and decrypt data within a customer's system. Customers are encouraged to encrypt data at the application or database layer before storing information on Logicworks' Managed Cloud Operations. Alternatively, the Company can assist in configuring server-side encryption upon customer request.

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from February 1, 2022 to January 31, 2023.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability, and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the

categories of availability, and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Information and communication:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

Control Environment

Integrity and Ethical Values

The Company has developed a code of conduct that is displayed in the Employee Handbook. This statement addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. The Employee Handbook is provided to all new employees. All employees are required to sign an acknowledgement form that they have received and agree to follow the Employee Handbook and code of conduct.

There is an established tone at the top, including both explicit guidance about what is right and wrong and an Anti-Bribery and Corruption Policy with import and export regulations. This tone is communicated and practiced by executives and management throughout the Company. The importance of high ethics and controls is discussed with newly hired employees throughout both the interview process and orientation.

Board of Directors

The Company has a board of directors that meets annually and is consulted and involved in all significant business decisions. The board of directors is comprised of four members: the current CEO, two outside directors, and the founder and former CEO of the Company.

The board of directors has, in a board resolution, formally acknowledged their responsibility for oversight of internal control.

Organizational Structure

The Company has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements.

The Company has an organization chart that sets forth the Company's lines of reporting. The organization chart is updated as necessary.

Management's Philosophy and Operating Style

The Company's senior management takes a hands-on approach to running the business. Senior management is heavily involved in all phases of the business operations.

The Company has staff meetings at least quarterly that enable the senior management team to remain in close contact with all personnel and to consistently emphasize appropriate behavior to all employees and to key vendor personnel.

Authority and Responsibility

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

Human Resources

The Company maintains formal hiring and termination policies and procedures, such as the performance of background checks on all new personnel offered employment. The Company maintains current job descriptions and roles for key personnel. Also, the Company has a process to ensure that the correct personnel are responsible for key processes and technology.

Information and Communication

Management is responsible for drafting, implementing, and updating all new and existing IT policies and procedures. Additionally, they are responsible for reviewing and approving all new and existing IT policies and procedures, as well as ensuring that all members of management and staff are aware of and understand the IT policies. Management also ensures that controls are in place by working with and training personnel.

Management has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities. Changes to employee responsibilities resulting from industry changes and significant events are properly communicated in a timely manner, utilizing the following methods:

- Regularly scheduled meetings
- Detailed written policies and procedures
- On-the-job training

The CEO, along with members of the ELT, communicate the Company's strategy and operational updates to employees and the board of directors. The CEO meets with the ELT continuously to review changing strategies and how to best implement them. The ELT reports significant events or failures to the CEO immediately. The CEO and ELT review this information, along with departmental updates, new initiatives, and operational improvements.

Risk Assessment and Mitigation

The Company considers risk as a part of its normal management routine. To ensure proper risk assessment and mitigation for both the short and long term, the Company's senior management monitors and mentors employees and takes corrective action as appropriate.

The Company seeks to identify, assess, and take steps to reduce risk to an acceptable level, with the primary purpose of protecting the Company and its ability to perform its mission, goals, and objectives. This analysis is prepared by the Company's Chief Information Security Officer (CISO) with input from the Information Security and Risk Committee, which meets quarterly.

The risk analysis methodology and approach are conducted using guidelines in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Risk Management Guide for Information Technology Systems, and NIST SP 800-39, Managing Information Security: Risk Organization, Mission, and Information System View. The assessment phase includes identifying organizational areas that support clients through an entire lifecycle of services with the Company. This phase identifies major business processes to be included as part of the analysis along with management network components used in direct support of clients.

Once the organizational, mission, or business threats and vulnerabilities are identified, management converts the vulnerabilities into risks based on categorizing the likelihood of vulnerabilities being exploited, mitigating controls, and the possible business impact. The Risk Analysis team analyzes the effectiveness of controls for maintaining good governance at the corporate level and for meeting availability and security objectives for customers. Management determines the overall likelihood rating, which indicates the probability that a vulnerability (technical or organizational) could be exploited by a threat-source (internal or external) given security and other controls in place, as well as the adverse impact resulting from a threat successfully exploiting the vulnerability.

The result of the risk assessment process is a body of recommendations to safeguard the Company as a corporate entity, its information systems, and the information systems of the customers for whom the Company provides services. These provide a basis by which senior management can evaluate and prioritize the identified risks and their associated controls. From the safeguards and controls presented, a risk mitigation implementation plan can be developed with conversations around acceptance of the recommendations, alternative suggestions, or rejection of control recommendations and acceptance of risk.

Monitoring

Senior management monitors internal controls and procedures to ensure that they adequately mitigate existing and potential risks. Procedures are disseminated to employees in order to provide them with an understanding of their individual and departmental responsibilities. As system features are changed or enhanced, or as regulations or operating conditions dictate, procedures are reviewed and modified by management. The performance of all required procedures is monitored through completion and sign-off of checklists, reviewing reports, and ongoing monitoring focused on the identification and escalation of potential issues.

The Company has several mechanisms by which internal controls are monitored, measured, and reported on. For example, penetration testing is performed at least annually, and internal and external vulnerability scans are performed quarterly for the public and private cloud infrastructure. Management performs regular reviews of user access, network configuration, change requests, and problem tickets to ensure conformance to the Company's control environment.

Control Activities

The Company's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical and Physical Access

The security policy establishes the access control requirements for requesting and provisioning user access for the system. The policy requires that access be denied by default, follow a least privilege principle, and be granted only upon business need. The Company uses centralized authentication and authorization to restrict access to the systems and services within the environment. Each user account is unique and identifiable to an individual user.

Domain-account management requests are routed to the designated asset owner or associated employee for approval according to established account provisioning and de-provisioning processes. Typically, access is controlled through the addition of individual user accounts to established domain security groups within the Active Directory (AD). Based on the configuration of a security group, any access request requires explicit approval from the assigned security group owner. Requests are automatically forwarded to the security group owner for approval in the system.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals that do not have valid Human Resources records. Select users can request the removal of user accounts from the system. In addition, system owners can directly remove users from security groups. Upon termination, employees are required to return their badges and workstations to the Company.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. Company personnel are required to follow the Company password policy for all domains as well as local user accounts for all assets.

Access to the production environment is controlled through a designated set of access points and restricted to Company personnel. Remote access to production systems is further restricted by way of two-factor authentication. Users are authenticated to access points using AD domain credentials depending on where the production assets are located. Production servers are configured to authenticate via AD.

The Company maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within the Company and prioritized based on the asset's business value and criticality to the organization. The inventory of servers is monitored and maintained by the information security team.

System Operations

Technical standards and baselines have been established and communicated for OS deployments and network architecture. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and deviations from the baseline in the production environment. Further, network teams review and update configuration standards and baseline configurations at least annually.

The Company has implemented an agent-based monitoring infrastructure within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potential unauthorized activity and security events, such as the creation of unauthorized local users, local groups, drivers, services, or IP configurations. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events, and sending the aggregated abnormal log information to a centralized log repository either at regular intervals or in real time.

The Company has implemented an alerting system to provide real-time alerting through the automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Component teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior, and, when necessary, appropriate actions are taken in accordance with incident handling procedures. The component teams manage the response to malicious events, including escalation to and engaging specialized support groups. In addition, the Company monitors relevant external information to stay up to date with and share current threat scenarios and countermeasures.

The Company carries out quarterly internal and external network vulnerability scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel, and remediation efforts are conducted in a timely manner.

The applicable security patches are applied based on the severity of the vulnerability and according to internally documented patch management procedures. Processes are in place to evaluate patches and their applicability to the environment. Once patches have been reviewed and their criticality level determined, service teams determine the release cadence for implementing patches without service disruption.

The Company has implemented an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers.

The Company has established incident response procedures and centralized tracking tools that consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms

include system monitoring processes for alerting the information security team per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email. Users are made aware of their responsibilities of reporting incidents and are assured that incidents will be investigated without any negative consequences.

Change Management

The change management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Infrastructure changes are managed through a formal change and release management procedure and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked, and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, evaluated, and approved for acceptance by the designated personnel.

Formal security and QA testing are performed as applicable prior to the change release based on defined acceptance criteria. The results of the QA testing are reviewed and approved by the appropriate personnel prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure.

Availability

The availability category refers to the accessibility of the system or services as committed by the Company's service agreements. The availability of the Managed Cloud Operations is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes the consideration of risks during normal business operations and during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Availability risks are addressed through the use and testing of various monitoring tools, replication setup, and backup and disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but rather from routine processing errors and failures of system elements.

Complementary User Entity Controls (CUECs)

The Company's controls related to the Managed Cloud Operations cover only a portion of overall internal control for each user entity of the Managed Cloud Operations. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS, Azure, and Equinix, as subservice organizations for data center colocation services. The Company's controls related to the Managed Cloud Operations cover only a portion of the overall internal control for each user entity of the Managed Cloud Operations. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS, Azure, and Equinix.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls

related to availability. The subservice organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the AWS, Azure and Equinix SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, Azure, and Equinix to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS, Azure, and Equinix management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Managed Cloud Operations to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS, Azure, and Equinix as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• AWS, Azure, and Equinix data centers restrict their access to authorized personnel through the use of a card key reader. • AWS, Azure, and Equinix data centers are monitored by closed circuit cameras. • AWS, Azure, and Equinix data centers are monitored 24/7 by security personnel.
CC6.5 CC6.7	• AWS, Azure, and Equinix data centers are responsible for securely decommissioning and physically destroying production assets in their control.
CC7.2 A1.2	• AWS, Azure, and Equinix data centers have installed fire suppression, fire detection, and environmental monitoring systems. • AWS, Azure, and Equinix data centers are protected against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Environmental protections at AWS, Azure, and Equinix data centers are subject to regular maintenance.

Specific Criteria Not Relevant to the System

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC) that were not relevant to the system as presented in this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the Managed Cloud Operations were used to provide the service from February 1, 2022 to January 31, 2023.

Subsequent Event

On February 1, 2023, Logicworks was acquired by Cox Enterprises, Inc. As a result, oversight of Logicworks now resides with the board of directors of the parent company.

Report Use

The description does not omit or distort information relevant to the Managed Cloud Operations while acknowledging that 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 their own particular needs.

Section 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Conduct, Policies and Procedures and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Logicworks' organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period February 1, 2022 to January 31, 2023. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Logicworks' Managed Cloud Operations and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
	Upon hire, employees acknowledge that they have read and agree to a code of conduct that describes their responsibilities and expected behavior regarding data and information system usage.	Inspected the code of conduct to determine that it described employee responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the code of conduct upon hire.	No exceptions noted.
	Employees sign a confidentiality agreement upon hire. This agreement prohibits the disclosure of information and other data to which the employee has been granted access during employment and after termination.	Inspected the confidentiality agreement template to determine that it prohibited the disclosure of information and other data to which the employee had been granted access during employment and after termination.	No exceptions noted.
		Inspected signed confidentiality agreements for a sample of new employees to determine that new employees were provided and signed the agreement upon hire.	No exceptions noted.
	Managers complete performance appraisals for direct reports at least annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the code of conduct.	Inspected the Personnel Security Standard to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the code of conduct.	No exceptions noted.
	New employees offered employment are subject to background checks prior to their start date.	Inspected background check completion evidence for a sample of new employees to determine that new employees were subject to background checks prior to their start date.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
	The board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Inspected the board of directors meeting minutes to determine that the board met during the period and maintained formal meeting minutes.	No exceptions noted.
		Inspected a listing of the board of directors to determine that the board included directors that were independent of the Company.	No exceptions noted.
	The board of directors has documented oversight responsibilities relative to internal control.	Inspected the board of directors' charter to determine that oversight responsibilities of the board of directors relative to internal control were documented.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	An organization chart is documented and defines the organizational structure and reporting lines.	Inspected the organization chart to determine that it was documented and defined the organizational structure and reporting lines.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The board of directors has documented oversight responsibilities relative to internal control.	Inspected the board of directors' charter to determine that oversight responsibilities of the board of directors relative to internal control were documented.	No exceptions noted.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	Employees complete security awareness training upon hire and annually thereafter.	Inspected training completion evidence for a sample of new employees to determine that new employees completed security awareness training upon hire.	No exceptions noted.
		Inspected training completion evidence for a sample of employees to determine that security awareness training was completed during the period.	No exceptions noted.
	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Managers complete performance appraisals for direct reports at least annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	Managers complete performance appraisals for direct reports at least annually.	Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period.	No exceptions noted.
	Upon hire, employees acknowledge that they have read and agree to a code of conduct that describes their responsibilities and expected behavior regarding data and information system usage.	Inspected the code of conduct to determine that it described employee responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
		Inspected acknowledgements for a sample of new employees to determine that new employees acknowledged that they had read and agreed to the code of conduct upon hire.	No exceptions noted.
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the code of conduct.	Inspected the Personnel Security Standard to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the code of conduct.	No exceptions noted.
	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the public cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the public cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly public cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly public cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the private cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the private cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly private cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly private cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.
	The security owner subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies and security on the production systems.	Inspected example security bulletins and email alerts subscribed to by the security owner to determine that the security owner subscribed to industry security bulletins and email alerts and used them to monitor the impact of emerging technologies and security on the production systems.	No exceptions noted.
	A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production systems.	Inspected FIM tool alert configurations and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
	Employees complete security awareness training upon hire and annually thereafter.	Inspected training completion evidence for a sample of new employees to determine that new employees completed security awareness training upon hire.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected training completion evidence for a sample of employees to determine that security awareness training was completed during the period.	No exceptions noted.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
	System changes are communicated to authorized internal users.	Inspected tickets for a sample of system changes to determine that system changes were communicated to authorized internal users.	No exceptions noted.
	A formalized whistleblower policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.	Inspected the formal whistleblower policy to determine that a formalized whistleblower policy was established and an anonymous communication channel was available for employees to report potential security issues or fraud concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
	Customer Master Service Agreements (MSAs) include the communication of the Company's commitments to its customers.	Inspected the MSA template to determine that the Company's commitments were communicated to customers.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were in place and included applicable confidentiality commitments.	No exceptions noted.
	Customers are notified of critical changes that may affect their processing.	Inspected email communications for a sample of critical changes to determine that the Company communicated critical changes to customers that could have affected their processing.	No exceptions noted.
	An external-facing support system is in place that allows users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel.	Inspected the customer reporting portal to determine that an external-facing support system was in place that allowed users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives.	Inspected documentation from the risk assessment performed during the period to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2	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 documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed.	No exceptions noted.
		Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually.	Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.
		Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management.	No exceptions noted.
		Inspected results from the BC/DR plan testing to determine that testing was performed during the period.	No exceptions noted.
	Quarterly security oversight meetings between the Vice President (VP) of Customer Success, Chief Technology Officer (CTO), and Chief Information Security Officer (CISO) are held to address risks and policy changes.	Inspected security oversight meeting minutes for a sample of quarters to determine that security oversight meetings between the VP of Customer Success, CTO, and CISO were held quarterly to address risks and policy changes.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed.	No exceptions noted.
		Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed.	No exceptions noted.
		Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.
	A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production systems.	Inspected FIM tool alert configurations and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution.	No exceptions noted.
	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the public cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the public cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly public cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly public cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the private cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the private cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly private cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly private cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	The Company utilizes a third-party vendor to automatically perform risk assessments on critical vendors and subservice organizations.	Inspected a list of vendor outputs from the GRX tool, as well as the risk assessment content for critical vendors and subservice organizations, to determine that a risk assessment was performed for all critical vendors and subservice organizations.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC4.2	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.		
	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution.	No exceptions noted.
	The Company utilizes a third-party vendor to automatically perform risk assessments on critical vendors and subservice organizations.	Inspected a list of vendor outputs from the GRX tool, as well as the risk assessment content for critical vendors and subservice organizations, to determine that a risk assessment was performed for all critical vendors and subservice organizations.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.1	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 selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected documentation from the risk assessment performed during the period to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	No exceptions noted.
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected documentation from the risk assessment performed during the period to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	No exceptions noted.
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	Inspected system access control procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege	No exceptions noted.
	Information security policies and procedures are documented and define the information security rules and requirements for the service environment.	Inspected the Company's information security policies and procedures to determine that they were documented and defined the information security rules and requirements for the service environment.	No exceptions noted.
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.
	A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was documented to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
	Formal procedures that outline requirements for vulnerability management are documented and include the following components: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines - Handling of system components for which no measures are initiated to remediate or mitigate vulnerabilities	Inspected the vulnerability management procedures to determine that formal procedures that outlined requirements for vulnerability management were documented and included the following components: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines - Handling of system components for which no measures are initiated to remediate or mitigate vulnerabilities	No exceptions noted.
	Formal policies and procedures that outline the requirements for vendor management are documented and include the following components: - Maintaining a list of critical vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Specifications for the contractual agreement and monitoring of third-party vendor requirements	Inspected the vendor management policy to determine that formal policies and procedures that outlined the requirements for vendor management were documented and included the following components: - Maintaining a list of critical vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Specifications for the contractual agreement and	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	- Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	monitoring of third-party vendor requirements - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment	
	Formal policies and procedures that outline the technical and organizational safeguards for change management of system components are documented and include the following components: - Change management roles and responsibilities - Criteria for risk assessment, categorization, and prioritization of changes - Approvals for implementation of changes - Requirements for the performance and documentation of tests, including rollback plans - Requirements for segregation of duties during development, testing, and release of changes - Requirements for the implementation and documentation of emergency changes	Inspected the change management procedures to determine that formal policies and procedures that outlined the technical and organizational safeguards for change management of system components were documented and included the following components: - Change management roles and responsibilities - Criteria for risk assessment, categorization, and prioritization of changes - Approvals for implementation of changes - Requirements for the performance and documentation of tests, including rollback plans - Requirements for segregation of duties during development, testing, and release of changes - Requirements for the implementation and documentation of emergency changes	No exceptions noted.
	A formal security and software development life cycle (SDLC) methodology is in place that governs the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.	Inspected security and SDLC documentation to determine that a formal security and SDLC methodology was in place that governed the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Network and system hardening standards are documented based on Center for Internet Security (CIS) Benchmarks and reviewed at least annually.	Inspected network and system hardening standards to determine that they were documented based on CIS Benchmarks and reviewed during the period.	No exceptions noted.
	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.
	Policies and procedures derived from the information security policy are documented, version controlled, reviewed at least annually, approved by management, and communicated to authorized users.	Inspected the policies and procedures to determine that policies and procedures derived from the information security policy were documented, version controlled, reviewed during the period, and approved by management.	No exceptions noted.
		Inspected the Company intranet to determine that policies and procedures were communicated to authorized users.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	Remote access to production systems is restricted to authorized employees with valid multi-factor authentication (MFA) tokens over an encrypted virtual private network (VPN) connection.	Inspected system configurations and observed a remote login session to determine that remote access to production systems was restricted to authorized employees with valid MFA tokens over an encrypted VPN connection.	No exceptions noted.
	Authentication to the following in-scope production system components requires unique usernames and passwords or authorized Secure Shell (SSH) keys: - Network - Operating system (OS) - Application(s) - Data stores - Amazon Web Services (AWS) Console - Azure Console - Firewalls - Log data - Backup data	Inspected system configurations and observed login attempts to determine that authentication to the following in-scope production system components required unique usernames and passwords or authorized SSH keys: - Network - OS - Application(s) - Data stores - AWS Console - Azure Console - Firewalls - Log data - Backup data	No exceptions noted.
	Passwords for in-scope system components are configured according to the Company's policy, which requires the following (unless there is a system limitation): - 12-character minimum - Complexity enabled - 90-day password change	Inspected the password policy and password configurations for in-scope system components to determine that passwords were configured according to Company policy, which required the following (unless there was a system limitation): - 12-character minimum - Complexity enabled	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	- 24 passwords remembered - Lockout after 3 invalid attempts	- 90-day password change - 24 passwords remembered - Lockout after 3 invalid attempts	
	Logical and network separation is in place for private cloud clients using shared storage services.	Inspected the shared storage configurations to determine that logical and network separation was in place for private cloud clients using shared storage services.	No exceptions noted.
	A master list of the Company's system components is maintained for management's use and accounts for additions and removals.	Inspected the asset inventory to determine that a master list of the Company's system components was maintained for management's use and accounted for additions and removals.	No exceptions noted.
	Encryption is enabled for data stores housing sensitive customer data.	Inspected encryption configurations to determine that encryption was enabled for data stores housing sensitive customer data.	No exceptions noted.
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.		
	User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process.	Inspected termination checklists and system access logs for a sample of terminated employees to determine that a termination checklist was completed and logical access was revoked within 24 hours of termination as part of the termination process.	No exceptions noted.
		Inspected a listing of terminated employees and compared the listing to the active in-scope system access listings to determine that terminated employees did not retain logical access to the in-scope systems after their separation.	No exceptions noted.
	Bi-monthly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.	Inspected access review documentation for a sample of two-month periods to determine that bi-monthly access reviews were conducted by management for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
	A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No changes to user access were required based on the access reviews conducted during the period.	Inquired of management and inspected access review documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether change tickets were created to remove or modify access as necessary in a timely manner as a result of the bi-monthly access reviews.	Not tested. No changes to user access were required based on the sampled access reviews conducted during the period.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	Privileged access to the following in-scope production system components is restricted to authorized users with a business need: - Network - OS - Application(s) - Data stores - AWS Console - Azure Console - Firewalls - Log data - Backup data - Encryption keys	Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to the following in-scope production system components was restricted to authorized users with a business need: - Network - OS - Application(s) - Data stores - AWS Console - Azure Console - Firewalls - Log data - Backup data - Encryption keys	No exceptions noted.
	User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process.	Inspected termination checklists and system access logs for a sample of terminated employees to determine that a termination checklist was completed and logical access was revoked within 24 hours of termination as part of the termination process.	No exceptions noted.
		Inspected a listing of terminated employees and compared the listing to the active in-scope system access listings to determine that terminated employees did not retain logical access to the in-scope systems after their separation.	No exceptions noted.
	Bi-monthly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.	Inspected access review documentation for a sample of two-month periods to determine that bi-monthly access reviews were conducted by management for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
	A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No changes to user access were required based on the access reviews conducted during the period.	Inquired of management and inspected access review documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether change tickets were created to remove or modify access as necessary in a timely manner as a result of the bi-monthly access reviews.	Not tested. No changes to user access were required based on the sampled access reviews conducted during the period.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Access to migrate changes to production is restricted to authorized personnel. Developers must have changes reviewed prior to migration in production.	Inspected system access listings, inquired of management, and compared each user's level of access to their job role to determine that access to migrate changes to production was restricted to authorized personnel.	No exceptions noted.
		Inspected system configurations to determine that developers were required to have changes reviewed prior to migration in production.	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's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.	Not applicable.	Not applicable.
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.		
	Electronic media containing confidential information is purged or destroyed, and certificates of destruction are issued for each device destroyed. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No electronic media purging or destruction occurred during the period.	Inquired of management and inspected electronic media documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	Not tested. No electronic media purging or destruction occurred during the period.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A master list of the Company's system components is maintained for management's use and accounts for additions and removals.	Inspected the asset inventory to determine that a master list of the Company's system components was maintained for management's use and accounted for additions and removals.	No exceptions noted.
	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	Remote access to production systems is restricted to authorized employees with valid multi-factor authentication (MFA) tokens over an encrypted virtual private network (VPN) connection.	Inspected system configurations and observed a remote login session to determine that remote access to production systems was restricted to authorized employees with valid MFA tokens over an encrypted VPN connection.	No exceptions noted.
	Firewalls, AWS Security Groups, and Azure Network Security Groups are used and configured to prevent unauthorized access.	Inspected the firewall, AWS Security Group, and Azure Network Security Group configurations to determine that firewalls, AWS Security Groups, and Azure Network Security Groups were used and configured to prevent unauthorized access.	No exceptions noted.
	A web application firewall (WAF) is used and configured to prevent unauthorized access to the production environment.	Inspected WAF configurations to determine that a WAF was used and configured to prevent unauthorized access to the production environment.	No exceptions noted.
	Firewall rulesets, AWS Security Groups, and Azure Network Security Groups are reviewed at least semiannually.	Inspected the firewall and security group review for a sample of reviews to determine that firewall rulesets, AWS Security Groups, and Azure Network Security Groups were reviewed during the period.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	AWS and Azure services are accessed by Company engineers and clients through Hypertext Transfer Protocol Secure (HTTPS) connections to the management consoles, through SSH, or using VPN sessions or tunnels.	Inspected HTTPS, SSH, and VPN configurations to determine that AWS and Azure services were accessed by Company engineers and clients through HTTPS connections to the management consoles, SSH, or using VPN sessions or tunnels.	No exceptions noted.
	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	Inspected IDS configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	No exceptions noted.
	Infrastructure supporting the service is patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected evidence of patching for a sample of months to determine that infrastructure supporting the service was patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	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.		
	AWS and Azure services are accessed by Company engineers and clients through Hypertext Transfer Protocol Secure (HTTPS) connections to the management consoles, through SSH, or using VPN sessions or tunnels.	Inspected HTTPS, SSH, and VPN configurations to determine that AWS and Azure services were accessed by Company engineers and clients through HTTPS connections to the management consoles, SSH, or using VPN sessions or tunnels.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant production servers.	Inspected anti-malware software configurations to determine that anti-malware technology was deployed for environments commonly susceptible to malicious attack and was configured to be updated routinely, logged, and installed on all relevant production servers.	No exceptions noted.
	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	Inspected IDS configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	No exceptions noted.
	Infrastructure supporting the service is patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected evidence of patching for a sample of months to determine that infrastructure supporting the service was patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
	A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production systems.	Inspected FIM tool alert configurations and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	Network vulnerability scans are performed quarterly for the public cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the public cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly public cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly public cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the private cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the private cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly private cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly private cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed.	No exceptions noted.
		Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.
	A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production systems.	Inspected FIM tool alert configurations and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems.	No exceptions noted.
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.		
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.	Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the public cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the public cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly public cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly public cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the private cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the private cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly private cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly private cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	Inspected IDS configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	No exceptions noted.
	IT infrastructure monitoring tools are utilized to monitor IT infrastructure availability and performance for the private cloud and managed AWS and Azure services, and they generate alerts when specific, predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance for the private cloud and managed AWS and Azure services and that they generated alerts when specific, predefined thresholds were met.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	No exceptions noted.
	Infrastructure supporting the service is patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected evidence of patching for a sample of months to determine that infrastructure supporting the service was patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	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.		
	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the Company's security incident response policies and procedures.	No exceptions noted.
	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	No exceptions noted.
	Network vulnerability scans are performed quarterly for the public cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the public cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly public cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly public cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Network vulnerability scans are performed quarterly for the private cloud infrastructure to identify, quantify, and prioritize vulnerabilities.	Inspected network vulnerability scans for the private cloud infrastructure for a sample of quarters to determine that network vulnerability scans were performed quarterly to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly private cloud network vulnerability scans.	Inspected remediation plans for vulnerabilities identified during the sampled quarterly private cloud network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans.	No exceptions noted.
	Infrastructure supporting the service is patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected evidence of patching for a sample of months to determine that infrastructure supporting the service was patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
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.		
	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period.	Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.	Not tested. No security incidents were identified during the period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
	Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually.	Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.
		Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management.	No exceptions noted.
		Inspected results from the BC/DR plan testing to determine that testing was performed during the period.	No exceptions noted.
	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period.	Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.	Not tested. No security incidents were identified during the period.
	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected change request tickets for a sample of software and infrastructure changes to determine that software and infrastructure changes were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	Access to migrate changes to production is restricted to authorized personnel. Developers must have changes reviewed prior to migration in production.	Inspected system access listings, inquired of management, and compared each user's level of access to their job role to determine that access to migrate changes to production was restricted to authorized personnel.	No exceptions noted.
		Inspected system configurations to determine that developers were required to have changes reviewed prior to migration in production.	No exceptions noted.
	Infrastructure supporting the service is patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected evidence of patching for a sample of months to determine that infrastructure supporting the service was patched monthly as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program.	No exceptions noted.
	Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually.	Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.
		Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management.	No exceptions noted.
		Inspected results from the BC/DR plan testing to determine that testing was performed during the period.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected multi-location deployment configurations to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	No exceptions noted.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.	Inspected database configurations and example alerts to determine that databases were replicated to secondary availability zones in real time and alerts were configured to notify administrators if replication failed.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
	The Company utilizes a third-party vendor to automatically perform risk assessments on critical vendors and subservice organizations.	Inspected a list of vendor outputs from the GRX tool, as well as the risk assessment content for critical vendors and subservice organizations, to determine that a risk assessment was performed for all critical vendors and subservice organizations.	No exceptions noted.
	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were in place and included applicable confidentiality commitments.	No exceptions noted.

Additional Criteria for Availability

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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.		
	System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected the configurations of system capacity and their evaluation to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand.	No exceptions noted.
	IT infrastructure monitoring tools are utilized to monitor IT infrastructure availability and performance for the private cloud and managed AWS and Azure services, and they generate alerts when specific, predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance for the private cloud and managed AWS and Azure services and that they generated alerts when specific, predefined thresholds were met.	No exceptions noted.
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.		
	Daily backups are configured for data stores housing sensitive customer data. Alerts are configured to notify administrators of failed backups for investigation and resolution.	Observed the backup configuration to determine that daily backups were configured for the data stores housing sensitive customer data.	No exceptions noted.
		Inspected backup failure alert configurations and example alerts to determine that alerts were configured to notify administrators of failed backups.	No exceptions noted.
		Inspected investigation and resolution evidence for a sample of backup failures to determine that administrators investigated and resolved failed backups upon notification.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually.	Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.
		Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management.	No exceptions noted.
		Inspected results from the BC/DR plan testing to determine that testing was performed during the period.	No exceptions noted.
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected multi-location deployment configurations to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	No exceptions noted.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.	Inspected database configurations and example alerts to determine that databases were replicated to secondary availability zones in real time and alerts were configured to notify administrators if replication failed.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually.	Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.
		Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management.	No exceptions noted.
		Inspected results from the BC/DR plan testing to determine that testing was performed during the period.	No exceptions noted.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.	Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data.	No exceptions noted.

Additional Criteria for Confidentiality

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was documented to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
	Confidential or sensitive customer data is prohibited by policy from being used or stored in non-production systems or environments.	Inspected the Data Management Standard to determine that confidential or sensitive customer data was prohibited by policy from being used or stored in non-production systems or environments.	No exceptions noted.
		Observed the test environment to determine that only test data was used in non-production systems or environments.	No exceptions noted.
	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data.	Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data.	No exceptions noted.
	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.	Inspected contracts for a sample of critical vendors to determine that formal information sharing agreements were in place and included applicable confidentiality commitments.	No exceptions noted.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	Electronic media containing confidential information is purged or destroyed, and certificates of destruction are issued for each device destroyed. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No electronic media purging or destruction occurred during the period.	Inquired of management and inspected electronic media documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	Not tested. No electronic media purging or destruction occurred during the period.
	Customer data in the application, metadata, and data stored in data backups are deleted when customers leave the service in accordance with contractual agreements.	Inspected tickets for data removal or purging for a sample of customers who left the service to determine that customer data in the application, metadata, and data stored in data backups were deleted when customers left the service in accordance with contractual agreements.	No exceptions noted.