System and Organization Controls Report (SOC 2® Type 2)

Report on QuesTek Innovations LLC's Description of Its ICMD® Digital Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period March 1, 2025, to February 28, 2026

QUESTEK® INNOVATIONS LLC

INSIGHT ASSURANCE

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: QuesTek Innovations LLC

Scope

We have examined QuesTek Innovations LLC's ("QuesTek", "the Company" or "the service organization") accompanying description of its ICMD® Digital Platform found in Section 3 titled "QuesTek Innovations LLC's description of its ICMD® Digital Platform" throughout the period March 1, 2025, to February 28, 2026 (the "Examination Period") ("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)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2025, to February 28, 2026, to provide reasonable assurance that QuesTek's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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)* in AICPA*, Trust Services Criteria.*

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

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

The information included in Section 5, "Other Information Provided by QuesTek Innovations LLC ," is presented by QuesTek management to provide additional information and is not part of the description. Information about QuesTek's management's responses to exceptions has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to achieve QuesTek's service commitments and

system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

QuesTek is responsible for its service commitments and system requirements, and designing, implementing, and operating effective controls within the system to provide reasonable assurance that QuesTek's service commitments and system requirements were achieved. In Section 2, QuesTek has provided the accompanying assertion titled "QuesTek Innovations LLC's Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. QuesTek 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; 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 the design and the 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 meet our other ethical responsibilities in accordance with 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.

Opinion

In our opinion, in all material respects,

- the description presents QuesTek's system that was designed and implemented throughout the Examination Period, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the Examination Period, to provide reasonable assurance that QuesTek's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of QuesTek's controls throughout that period.
- the controls stated in the description operated effectively throughout the Examination Period, to provide reasonable assurance that QuesTek's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of QuesTek's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of QuesTek; user entities of QuesTek's system during some or all of the Examination Period; business partners of QuesTek

subject to risks arising from interactions with the system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

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

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

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
June 11, 2026

SECTION 2:
QUESTEK INNOVATIONS LLC'S MANAGEMENT ASSERTION

QUESTEK INNOVATIONS LLC'S MANAGEMENT ASSERTION

We have prepared the description of QuesTek Innovations LLC's ("QuesTek", "the Company" or "the service organization") ICMD® Digital Platform entitled "QuesTek Innovations LLC's description of its ICMD® Digital Platform" throughout the period March 1, 2025, to February 28, 2026 (the "Examination Period") ("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)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the ICMD® Digital Platform that may be useful when assessing the risks arising from interactions with QuesTek's system, particularly information about system controls that QuesTek 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 (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)* in AICPA*, Trust Services Criteria.*

QuesTek uses Amazon Web Services and Microsoft Azure (the "subservice organizations") to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at QuesTek, to achieve QuesTek's service commitments and system requirements based on the applicable trust services criteria. The description presents QuesTek's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of QuesTek's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

- the description presents QuesTek's System that was designed and implemented throughout the Examination Period, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the Examination Period, to provide reasonable assurance that QuesTek's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization(s) and user entities applied the complementary controls assumed in the design of QuesTek's controls.

- the controls stated in the description operated effectively throughout the Examination Period, to provide reasonable assurance that QuesTek's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of QuesTek's controls operated effectively throughout that period.

QuesTek Innovations LLC
June 11, 2026

SECTION 3:
QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® DIGITAL PLATFORM

QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® DIGITAL PLATFORM

COMPANY BACKGROUND

QuesTek Innovations LLC ("QuesTek Innovations") is a privately held company established in October 1997 that offers materials science software as a service. QuesTek Innovations is an LLC headquartered in Evanston, Illinois.

DESCRIPTION OF SERVICES OVERVIEW

ICMD® Digital Platform is QuesTek's digital platform for simulation-led materials design, decision-making, and qualification. It enables engineering teams to predict how materials will behave across composition, processing, and service conditions before committing to costly testing or long qualification cycles.

Built on nearly 30 years of ICME leadership, ICMD® Digital Platform helps organizations move from trial-and-error development to Digital Once engineering.

Grounded in QuesTek's proven Materials by Design® technology, the ICMD® Digital Platform combines physics-based modeling, simulation, and real-world metallurgical expertise to bring predictive accuracy and speed to every phase of the materials lifecycle.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

QuesTek designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that QuesTek makes to user entities, the laws and regulations governing the provision of the services, and the financial, operational, and compliance requirements that QuesTek has established for the services. The system services are subject to security commitments established internally by QuesTek. Commitments to user entities are documented and communicated in service-level agreements and other customer agreements, as well as in descriptions of the service offering provided online.

Security Commitments

Security commitments include, but are not limited to, the following:

- Security principles within the fundamental designs of services that are designed to permit system users to access the information they need based on their role in the system, while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Protection of production systems against security events that could impair availability

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The system description comprises the following components:

- **Infrastructure –** The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- **Software –** The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- **People –** The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data –** The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedures –** The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

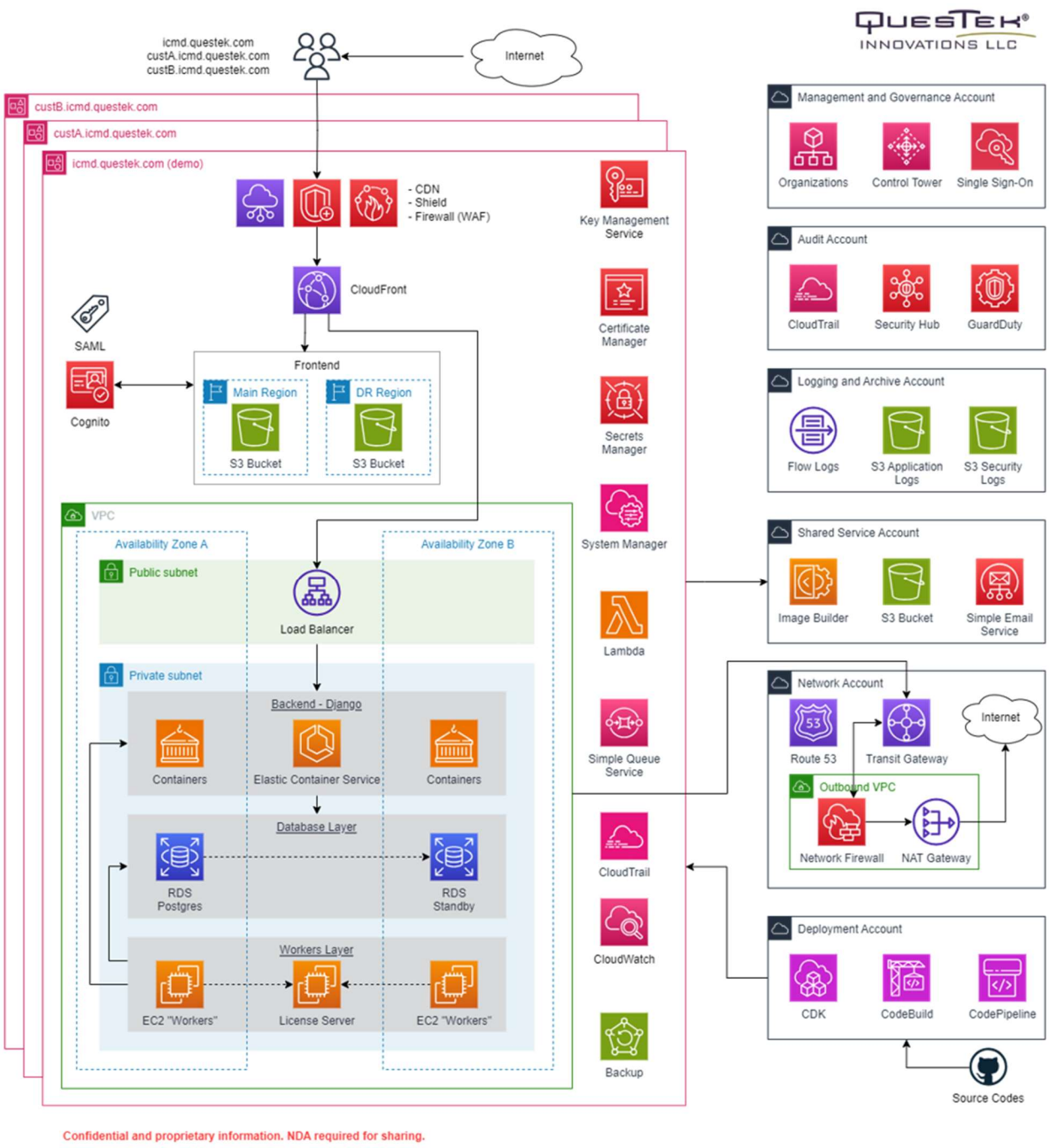
INFRASTRUCTURE

QuesTek maintains a system inventory that includes virtual machines (EC2 instances) and computers (desktops and laptops). The inventory documents device name, device type, vendor function, OS, location, and notes. QuesTek utilizes Amazon Web Services and Microsoft Azure as subservice organizations to host QuesTek's processing system. QuesTek leverages the infrastructure and platform services provided by Amazon Web Services and Microsoft Azure to support the achievement of its service commitments and system requirements. QuesTek is responsible for designing and configuring its processing system architecture within those environments.

The in-scope infrastructure components are shown in the table below. To outline the topology of its network, the organization maintains the following network diagram.

Primary Infrastructure		
Asset	**Type**	**Purpose**
Elastic Compute Cloud (EC2)	AWS	Compute system in the cloud
Elastic Container Service (ECS)	AWS	Hosts and manages application containers
Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud (VPC)	AWS	Protects the network perimeter and restricts inbound and outbound access

Primary Infrastructure		
Asset	**Type**	**Purpose**
S3 Buckets	AWS	Storage, upload, and download
CloudFront	AWS	Masks S3 bucket paths
Internet Gateway	AWS	Allows communication between instances in your VPC and the Internet
WAF	AWS	Web application firewall
Relational Database Service (RDS)	AWS	Simplifies database management in the cloud
Virtual Machine	Azure	Virtual Machine - License Server
Virtual Network Gateway	Azure	Encrypted network traffic
Load Balancer	Azure	Distributes incoming traffic



SOFTWARE

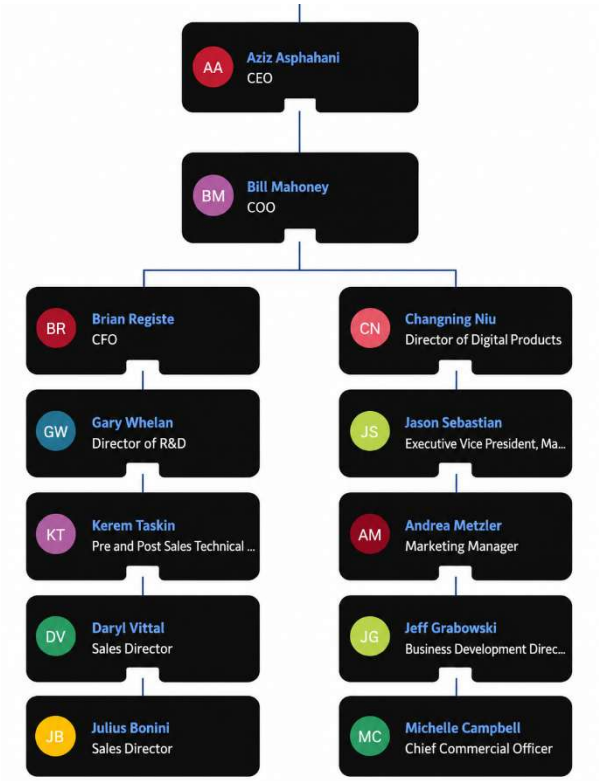
QuesTek is responsible for managing the development and operation of the system. The software supporting the system consists of the applications, programs, and other software components used to build, secure, maintain, and monitor the system. The list of software is shown in the table below.

Primary Software		
System/Application	**OS**	**Purpose**
AWS CloudWatch	SaaS	Provides system monitoring and alerting
AWS CloudTrail	SaaS	Records administrative and system activity
AWS GuardDuty	SaaS	Provides threat-detection capabilities
Drata	SaaS	Continuous security and compliance monitoring of the cloud infrastructure
Sentry	SaaS	Error tracking and performance monitoring
GitHub	SaaS	Store, track, collaborate on software projects, and version control
Atlassian	SaaS	Collaborative tool for a centralized knowledge repository

PEOPLE

QuesTek employs dedicated team members to handle major product functions, including operations that directly support the system. The responsibilities of each group are detailed below.

QuesTek's corporate structure includes the following roles.



Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Marketing Director – Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of QuesTek.

Sales and Marketing – This role is responsible for customer relations and working closely with both the Marketing Director and the Sales Director to ensure there is transparency between marketing and sales efforts.

Sales – Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewals of existing customer contracts.

Chief Technology Officer – Responsible for the technological direction and advancement of the organization. Directs the operations, engineering, and support teams to efficiently develop and deliver new services, maintain existing services, and support QuesTek's customer base in its use of the service.

Technology and Engineering – This role is responsible for the operations of the day-to-day items to maintain the integrity of the environment. This role is also responsible for the provisioning, research, and development of new and upcoming services within the company.

Operations and Support – This role includes the support team and crosses over to the engineering team. It is primarily responsible for daily support aspects of the business. This includes, but is not limited to, supporting end users with day-to-day issues, as well as assisting in the onboarding, implementation, and migration of new and existing customers as part of their ongoing maintenance.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured, which is utilized by QuesTek in delivering its managed Services.

All employees and contractors of QuesTek are obligated to respect and, in all cases, to protect customer data. Additionally, QuesTek has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed at least annually.

Data is classified into the following major categories as outlined below.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer Data	Information received from customers for processing or storage. QuesTek must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company Data	Information collected and used by QuesTek to operate the business. QuesTek must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries • Research and Engineering Data

PROCEDURES

Management has developed and communicated policies and procedures involved in the operation of the system. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business at least annually. The following provides a summary of QuesTek's policies and procedures that comprise the internal control for the system.

Physical Security

QuesTek's production servers are maintained by Amazon Web Services and Microsoft Azure. The physical security protections are the responsibility of Amazon Web Services and Microsoft Azure. QuesTek reviews the attestation reports and performs a risk analysis of Amazon Web Services and Microsoft Azure on an annual basis.

Logical Access

QuesTek provides employees and contractors access to infrastructure via a role-based access control system to ensure uniform, least privileged access to identified users and to maintain simple user provisioning and deprovisioning processes.

Access to these systems is split into three levels: Administrator, User, and No Access. User access and roles are reviewed on an annual basis to ensure the least privileged access.

QuesTek's onboarding team provisions access to the system based on the employee's role. Background checks are performed for applicable personnel as part of the hiring process. Employees are responsible for reviewing QuesTek's policies and completing required security training.

When an employee is terminated, QuesTek's offboarding team is responsible for deprovisioning access to all in-scope systems within 1 business day of the employee's termination.

Change Management

QuesTek maintains documented policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Testing of changes is performed in an environment that is logically separated from the production environment. The Change Control Board approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Patch Management

Software patches and updates are applied to systems in a timely manner. Infrastructure supporting the services provided is patched as a part of the change management process to help ensure that servers supporting the service are hardened against security threats. Routine updates are applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Security patches are applied upon identification, and all patches are installed during off-peak hours to minimize disruption to business processes.

Backups and Recovery

Customer data is backed up and monitored by the system engineering team for completion and exceptions. If there is an exception, the system engineering team performs troubleshooting to identify the root cause and either reruns the backup or addresses it as part of the next scheduled backup job.

Computer Operations

QuesTek maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

QuesTek internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

QuesTek utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Problem Management

QuesTek maintains an Incident Response Plan that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, QuesTek provides formal security awareness training.

QuesTek provides clients with dedicated communication channels, including email and phone, to report potential security breaches. Internal users are required to report incidents through QuesTek's internal portal or directly to the Director of IT Operations and Compliance, ensuring proper documentation, tracking, and escalation in accordance with QuesTek's Incident Response Plan.

Data Communications

QuesTek has elected to use Amazon Web Services and Microsoft Azure to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations.

Amazon Web Services and Microsoft Azure simplify QuesTek's logical network configuration by providing an effective firewall around all of QuesTek's application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

Amazon Web Services and Microsoft Azure also automate the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

System Monitoring

The Logging and Monitoring Policy and Vulnerability Management Policy describe QuesTek's procedures for system logging and monitoring, as well as vulnerability identification and remediation. QuesTek uses AWS CloudTrail and Microsoft Defender to collect and retain security-relevant logs within its Amazon Web Services and Microsoft Azure environments. Logs include applicable source and destination information, protocol details, and timestamps. QuesTek monitors system performance and capacity using AWS CloudWatch and Microsoft Azure Monitor.

AWS GuardDuty and Microsoft Defender provide threat-detection capabilities using applicable activity logs, network flow logs, and DNS logs.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. QuesTek uses anti-malware and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year, with at least three months readily available.

Vendor Management

QuesTek maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendor's cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. QuesTek is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. QuesTek monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. QuesTek executes non-disclosure agreements with third parties before any information is shared.

Boundaries of the System

The boundaries of the ICMD® Digital Platform are the specific aspects of QuesTek Innovations LLC's infrastructure, software, people, data, and procedures necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, data, and procedures that indirectly support the services provided to customers are not included within the boundaries of the ICMD® Digital Platform.

This report does not include the cloud infrastructure hosting and platform services provided by Amazon Web Services and Microsoft Azure.

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

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and assure effective operational controls. Senior management establishes the tone at the top regarding the importance of internal control and expected standards of conduct.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of QuesTek's control environment, affecting the design, administration, and monitoring of other

components. Integrity and ethical behavior are the product of QuesTek's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy.

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

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

Management Philosophy and Operating Style

The QuesTek management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data entrusted to them by their customers.

The QuesTek management team frequently meets to be briefed on technology changes that affect how QuesTek supports simulation-led materials design, decision-making, and qualification, as well as new security technologies that can help protect the ICMD® Digital Platform and regulatory changes that may require QuesTek to modify its software or operations to maintain compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with QuesTek's core product offerings and duties to new and existing customers.

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

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

Commitment to Competence

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

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

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

Organizational Structure and Assignment of Authority and Responsibilities

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

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

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

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

Human Resources Policies and Procedures

QuesTek has formal hiring procedures that are designed to ensure that new team members are able to meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are performed for all newly hired employees before the start date and include a review of their education and criminal records.

During the onboarding process, the new employees review the Employee Handbook, Code of Conduct, and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Employee Handbook and Code of Conduct. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees, which includes the areas of security and confidentiality, to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees and contractors. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employees' performance for the last fiscal year.

RISK ASSESSMENT PROCESS

QuesTek's risk assessment process identifies and manages risks that could potentially affect QuesTek's ability to provide reliable and secure services to its customers. As part of this process, QuesTek maintains a risk register to track all systems and procedures that could present risks to meeting QuesTek's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular QuesTek product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

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

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEMS

QuesTek has an information security policy to help ensure that employees understand their roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security, confidentiality, and availability purposes that notify the key personnel in the event of problems.

Additional communication methods include department meetings to communicate company policies, procedures, industry or business issues, or other topics management deems key to the achievement of the organization's objectives. Communication is encouraged at all levels to promote the operating efficiency of QuesTek.

QuesTek also updates its website on an ongoing basis to inform clients and other external parties of company and industry-related issues that could affect its services and what steps QuesTek is taking to reduce or avoid the impact on its operations. QuesTek's security commitments regarding the system are included in the services agreement.

MONITORING CONTROLS

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

Ongoing Monitoring

QuesTek's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

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

Monitoring of the Subservice Organizations

QuesTek uses Amazon Web Services and Microsoft Azure to provide hosting services. QuesTek management obtains and reviews the applicable SOC reports for Amazon Web Services and Microsoft Azure at least annually to evaluate the design and operating effectiveness of relevant controls at the subservice organizations. Through its ongoing operational activities, QuesTek also monitors the availability and performance of the cloud services supporting the ICMD® Digital Platform and follows up on identified service issues, as necessary.

Reporting Deficiencies

QuesTek's internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE EXAMINATION PERIOD

No significant incidents have occurred to the services provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

QuesTek's controls related to the system cover only a portion of the overall internal control. It is not feasible for the applicable trust services criteria related to the system to be achieved solely by QuesTek's control procedures; the achievement of certain criteria depends on complementary controls implemented at the subservice organizations (Amazon Web Services and Microsoft Azure). Accordingly, the complementary subservice organization controls assumed in the design of QuesTek's controls, presented below, should be evaluated in conjunction with QuesTek's controls and the related tests and results described in Section 4 of this report.

#	Complementary Subservice Organization Control	Criteria
1	Physical security controls over the data centers hosting QuesTek's infrastructure are maintained.	CC6.4
2	Physical assets hosting QuesTek's production environment are destroyed when no longer needed or upon request by QuesTek.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS

QuesTek's controls related to the System only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust services criteria related to the System to be achieved solely by QuesTek's control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of QuesTek.

#	Complementary User Entity Control	Criteria
1	User entities are responsible for notifying QuesTek of changes made to the administrative contact information.	CC2.3
2	User entities are responsible for understanding and complying with their contractual obligations to QuesTek.	CC2.3 and CC3.2
3	User entities should have controls in place to provide reasonable assurance that user access is provisioned and de-provisioned appropriately.	CC6.2 and CC6.3
4	User entities are responsible for reporting issues with QuesTek's systems and platforms.	CC7.4

TRUST SERVICES CATEGORIES, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed,

implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4:
TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TESTS OF CONTROLS

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period March 1, 2025, to February 28, 2026.

The applicable trust services criteria and related controls specified by QuesTek are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section 4 are described below:

- Inquiries – Inquiry of appropriate personnel and corroboration with management.
- Observation – Observation of the application, performance, or existence of the control.
- Inspection – Inspection of documents and reports indicating the performance of the control.
- Reperformance – Reperformance of the control.

FOOTNOTES FOR TEST RESULTS WHEN NO TESTS OF OPERATING EFFECTIVENESS WERE PERFORMED

1. The circumstances that warranted the operation of the control did not occur during the examination period; therefore, no tests of operating effectiveness were performed.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management has approved security policies, and all employees and contractors accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the security policies to determine that management reviewed security policies annually and the policies were accessible to active employees and contractors.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of new employees to determine that new employees accepted the security policies at the time of hire.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of active employees to determine that active employees accepted the security policies annually.	No exceptions noted.
		Per inquiry with management and inspection of HR listing, there were no contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.1.2	Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the completed performance evaluations for a sample of employees to determine that the company's managers completed performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.3	The company requires its employees and contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct acknowledgement for a population of new employees to determine that the company's new employees read and accepted the Code of Conduct.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the background check for a population of new employees to determine that the company's new employees passed a background check.	No exceptions noted.
CC1.1.4	Management has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inspected the Information Security Policy to determine that a disciplinary sanctions process was in place for workforce members who violated the company's policies or caused a security or privacy incident.	No exceptions noted.
		Inspected the disciplinary sanctions process to determine that disciplinary actions were enforced in accordance with the disciplinary policy for those who violated the policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors includes members independent from management who are not involved in control operations.	Inspected the profiles for the board of directors to determine that independent directors were included in the board of directors.	No exceptions noted.
CC1.2.2	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Corporate Board Charter to determine that the organization had defined and documented BoD responsibilities for oversight of the security program.	No exceptions noted.
CC1.2.3	The company's board of directors, owners, senior leadership, or equivalent body, has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the BoD charter to determine that the company had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.
CC1.2.4	The company's board of directors, owners, senior leadership, or equivalent body, meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected BoD meeting minutes to determine that the company's board of directors, owners, senior leadership, or equivalent body, met annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies and decisions made and action items were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart to determine that the company reviewed its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted.
CC1.3.2	The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Data Security Roles & Responsibilities to determine that the company had an assigned security team that was responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Inspected the Security Training Program for a sample of new employees to determine that the company had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company security policies and procedures, including the identification and reporting of incidents.	No exceptions noted.
		Inspected the security awareness training for a sample of new employees to determine that employees were required to complete training upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new hired contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the security awareness training for a sample of active employees to determine that employees completed training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.1 *(cont.)*	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Per inquiry with management and inspection of the training completion record for active contractors, there were no active contractors eligible for security awareness training during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.4.2	The company's new hires are required to pass a background check as a condition of their employment.	Inspected the background checks for a sample of new employees during the examination period to determine that the company's new employees passed a background check as a condition of their employment.	No exceptions noted.
CC1.4.3	The company requires its employees and contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct acknowledgement for a population of new employees to determine that the company's new employees read and accepted the Code of Conduct.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.3 *(cont.)*	The company requires its employees and contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the background check for a population of new employees to determine that the company's new employees passed a background check.	No exceptions noted
CC1.4.4	The company has a formal Code of Conduct approved by management and accessible to all employees and contractors. All employees and contractors must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company had a formal Code of Conduct approved by management and accessible to all employees.	No exceptions noted.
		Inspected the Code of Conduct acknowledgement for a sample of new employees during the examination period to determine that new employees accepted the Code of Conduct upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, it was noted that there were no new contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.4.5	The company positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	Inspected the job descriptions for a sample of positions to determine that the company positions had a detailed job description that listed qualifications, such as requisite skills and experience, which candidates must meet in order to be hired.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Inspected the Security Training Program for a sample of new employees to determine that the company had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company security policies and procedures, including the identification and reporting of incidents.	No exceptions noted.
		Inspected the security awareness training for a sample of new employees to determine that employees were required to complete training upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new hired contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the security awareness training for a sample of active employees to determine that employees completed training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.1 *(cont.)*	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Per inquiry with management and inspection of the training completion record for active contractors, there were no active contractors eligible for security awareness training during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.5.2	Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the completed performance evaluations for a sample of employees to determine that the company's managers completed performance evaluations for direct reports annually.	No exceptions noted.
CC1.5.3	The company has a formal Code of Conduct approved by management and accessible to all employees and contractors. All employees and contractors must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company had a formal Code of Conduct approved by management and accessible to all employees.	No exceptions noted.
		Inspected the Code of Conduct acknowledgement for a sample of new employees during the examination period to determine that new employees accepted the Code of Conduct upon hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.3 *(cont.)*	The company has a formal Code of Conduct approved by management and accessible to all employees and contractors. All employees and contractors must accept the Code of Conduct upon hire.	Per inquiry with management and inspection of the company's HR listing, it was noted that there were no new contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.5.4	Management has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inspected the Information Security Policy to determine that a disciplinary sanctions process was in place for workforce members who violated the company's policies or caused a security or privacy incident.	No exceptions noted.
		Inspected the disciplinary sanctions process to determine that disciplinary actions were enforced in accordance with the disciplinary policy for those who violated the policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	Inspected the role-based access for AWS, GitHub, Adobe, Atlassian Sentry, AvePoint, Microsoft, and QuesTek System to determine that the company authorized access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	No exceptions noted.
CC2.1.2	The company has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Compliance Policy to determine that the company defined the policies and procedures to support the functioning of internal control.	No exceptions noted.
CC2.1.3	The company identifies, inventories, classifies, and assigns owners to IT assets.	Inspected the Asset Inventory to determine that the company identified, inventoried, classified, and assigned owners to IT assets.	No exceptions noted.
CC2.1.4	The company maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.	Inspected the network diagram to determine that the company maintained an accurate architectural diagram to document system boundaries to support the functioning of internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1.5	The company has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Cryptography Policy to determine that the company had an established policy and procedures that governed the use of cryptographic controls.	No exceptions noted.
CC2.1.6	The company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine that the company conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company provides a process to employees for reporting security features, incidents, and concerns, and other complaints to company management.	Inspected the Incident Response Plan to determine that the company provided a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	No exceptions noted.
CC2.2.2	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.3	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC2.2.4	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.5	Management has approved security policies, and all employees and contractors accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the security policies to determine that management reviewed security policies annually and the policies were accessible to active employees and contractors.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of new employees to determine that new employees accepted the security policies at the time of hire.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of active employees to determine that active employees accepted the security policies annually.	No exceptions noted.
		Per inquiry with management and inspection of HR listing, there were no contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.6	The security team communicates important information security events to company management in based on the severity of the identified incident.	Inspected the incident log for a sample of incidents to determine that the security team communicated important information security events to company management in a timely manner.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the security team communicated important information security events to company management in based on the severity of the identified incident.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.7	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Inspected the Security Training Program for a sample of new employees to determine that the company had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company security policies and procedures, including the identification and reporting of incidents.	No exceptions noted.
		Inspected the security awareness training for a sample of new employees to determine that employees were required to complete training upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new hired contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the security awareness training for a sample of active employees to determine that employees completed training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.7 (cont.)	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Per inquiry with management and inspection of the training completion record for active contractors, there were no active contractors eligible for security awareness training during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC2.2.8	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.
CC2.2.9	The company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine that the company conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3.1	The company provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected the company website to determine that the company provided a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.3.2	The company tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	Inspected the continuous monitoring tool to determine that the company tracked security deficiencies through internal tools and closed them within an SLA that management had pre-specified.	No exceptions noted.
CC2.3.3	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.
CC2.3.4	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3.5	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC2.3.6	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.
CC2.3.7		Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including their compliance reports.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
	The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the review documentation and the vendor compliance reports for critical vendors to determine that critical vendor compliance reports were reviewed annually.	No exceptions noted.
CC2.3.8	The company's security commitments are communicated to external users, as appropriate.	Inspected the company website to determine that the company security commitments were communicated to external users, as appropriate.	No exceptions noted.
CC2.3.9	The company communicates system changes to customers that may affect security, availability, or confidentiality.	Inspected an example system change communication to determine that the company communicated system changes to customers that may affect security, availability, or confidentiality.	No exceptions noted.
CC2.3.10	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.
CC2.3.11	The company has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company defined a policy that established requirements for third-parties to meet the organization's data preservation and protection requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.1.2	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.
CC3.1.3	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1.4	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.2.2	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2.3	The company's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment report to determine that the company prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC3.2.4	The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity/Disaster Recovery Test to determine that the company conducted annual BCP/DR tests and documented them according to the BCDR Plan.	No exceptions noted.
CC3.2.5	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC3.2.6	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2.7	The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including their compliance reports.	No exceptions noted.
		Inspected the review documentation and the vendor compliance reports for critical vendors to determine that critical vendor compliance reports were reviewed annually.	No exceptions noted.
CC3.2.8	The company has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company defined a policy that established requirements for third-parties to meet the organization's data preservation and protection requirements.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.3.2	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.3.3	The company's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment report to determine that the company prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart to determine that the company reviewed its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted.
CC3.4.2	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.4.3	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4.4	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC3.4.5	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.
CC3.4.6	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4.7	The company has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company defined a policy that established requirements for third-parties to meet the organization's data preservation and protection requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company has a defined System Access Control Policy that requires annual access control reviews to be conducted, and access request forms be filled out for new hires and employee transfers.	Inspected the Access Control Policy to determine that the company required an annual access control review to be conducted and access request forms to be filled out for new hires and employee transfers.	No exceptions noted.
CC4.1.2	The company performs annual access control reviews.	Inspected the annual access review documentation to determine that the company performed an annual access control review.	No exceptions noted.
CC4.1.3	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC4.1.4	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1.5	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC4.1.6	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.
CC4.1.7	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC4.2.2	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.
CC4.2.3	The company's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment report to determine that the company prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.4	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC4.2.5	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.6	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.
CC4.2.7	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.8	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC4.2.9	The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Data Security Roles & Responsibilities to determine that the company had an assigned security team that was responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.10	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.
CC4.2.11	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart to determine that the company reviewed its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted.
CC5.1.2	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC5.1.3	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.
CC5.1.4	The company's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment report to determine that the company prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1.5	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC5.1.6	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1.7	The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Data Security Roles & Responsibilities to determine that the company had an assigned security team that was responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.
CC5.1.8	The company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine that the company conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the Backup Policy to determine that management had approved all policies that detail how customer data may be made accessible and should be handled.	No exceptions noted.
		Inspected the Drata platform to determine that all employees and contractors had access to the Backup, Data Classification, and Data Protection Policies.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.2	The company authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	Inspected the role-based access for AWS, GitHub, Adobe, Atlassian Sentry, AvePoint, Microsoft, and QuesTek System to determine that the company authorized access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.	No exceptions noted.
CC5.2.3	The company conducts a Risk Assessment at least annually.	Inspected the Risk Assessment and Risk Assessment Executive Briefing to determine that the company conducted a Risk Assessment annually.	No exceptions noted.
CC5.2.4	The company's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment report to determine that the company prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.5	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC5.2.6	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.7	Management has approved security policies, and all employees and contractors accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the security policies to determine that management reviewed security policies annually and the policies were accessible to active employees and contractors.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of new employees to determine that new employees accepted the security policies at the time of hire.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of active employees to determine that active employees accepted the security policies annually.	No exceptions noted.
		Per inquiry with management and inspection of HR listing, there were no contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC5.2.8	The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Data Security Roles & Responsibilities to determine that the company had an assigned security team that was responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.9	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Inspected the Security Training Program for a sample of new employees to determine that the company had established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company security policies and procedures, including the identification and reporting of incidents.	No exceptions noted.
		Inspected the security awareness training for a sample of new employees to determine that employees were required to complete training upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, there were no new hired contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the security awareness training for a sample of active employees to determine that employees completed training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.9 *(cont.)*	The company has established training programs for privacy and information security to help employees and contractors understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees and contractors are required to complete the training upon hire and annually thereafter.	Per inquiry with management and inspection of the training completion record for active contractors, there were no active contractors eligible for security awareness training during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC5.2.10	The company has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Cryptography Policy to determine that the company had an established policy and procedures that governed the use of cryptographic controls.	No exceptions noted.
CC5.2.11	The company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine that the company conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company provides a process to employees for reporting security features, incidents, and concerns, and other complaints to company management.	Inspected the Incident Response Plan to determine that the company provided a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	No exceptions noted.
CC5.3.2	The company has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Compliance Policy to determine that the company defined the policies and procedures to support the functioning of internal control.	No exceptions noted.
CC5.3.3	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC5.3.4	The company has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Data Security Incident Management Roles & Responsibilities policy to determine that the company has established a Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.5	The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity/Disaster Recovery Test to determine that the company conducted annual BCP/DR tests and documented them according to the BCDR Plan.	No exceptions noted.
CC5.3.6	Management has approved security policies, and all employees and contractors accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the security policies to determine that management reviewed security policies annually and the policies were accessible to active employees and contractors.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of new employees to determine that new employees accepted the security policies at the time of hire.	No exceptions noted.
		Inspected the policy acknowledgment for a sample of active employees to determine that active employees accepted the security policies annually.	No exceptions noted.
		Per inquiry with management and inspection of HR listing, there were no contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC5.3.7	Management reviews security policies on an annual basis.	Inspected the security policies to determine that management reviewed security policies annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.8	The company has a formal Code of Conduct approved by management and accessible to all employees and contractors. All employees and contractors must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company had a formal Code of Conduct approved by management and accessible to all employees.	No exceptions noted.
		Inspected the Code of Conduct acknowledgement for a sample of new employees during the examination period to determine that new employees accepted the Code of Conduct upon hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's HR listing, it was noted that there were no new contractors hired during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC5.3.9	The company has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the company had a defined Business Continuity Plan that outlined the proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC6.1.1	The company maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the network diagram to determine that the company maintained an accurate network diagram that was accessible to the engineering team and it was reviewed by management on an annual basis.	No exceptions noted.
CC6.1.2	The company ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the screensaver configurations for a sample of active employee's devices to determine that the company ensured that all company-issued computers used a screensaver lock with a timeout of no more than 15 minutes.	No exceptions noted.
CC6.1.3	Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configuration to determine that data in transit was encrypted using strong encryption algorithms.	No exceptions noted.
CC6.1.4	Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.	Inspected network security controls to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
CC6.1.5	The company uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Inspected the AWS network configurations to determine that only approved networking ports and protocols were implemented, including firewalls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.6	WAF in place to protect the company's application from outside threats.	Inspected the WAF Ruleset to determine that WAF was in place to protect the company application from outside threats.	No exceptions noted.
CC6.1.7	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Intrusion Detection System (IDS) to determine that an intrusion detection system was in place to detect potential intrusions, alert personnel when a potential intrusion was detected.	No exceptions noted.
CC6.1.8	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the company's website and TLS certificate to determine that users could only access the production system remotely through the use of encrypted communication systems.	No exceptions noted.
CC6.1.9	The company restricts administrative access to system components to only authorized personnel (network, networking devices, database, operating system, application, encryption keys, moving changes to production).	Inspected the listings of administrative users for AWS, GitHub, Adobe, Atlassian Sentry, AvePoint, Microsoft, and QuesTek System to determine that administrative access was limited to only authorized personnel.	No exceptions noted.
CC6.1.10	The company requires authentication methods to in-scope systems to include a unique username, password, MFA, and/or SSH keys.	Inspected the user's listings for Atlassian, AWS, GitHub, AvePoint, AllCloud, Microsoft and QuesTek System to determine that authentication to these systems required a unique username, password, MFA, and SSH keys.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	The company has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the Access Control Policy to determine that the company required an annual access control review to be conducted and access request forms to be filled out for new hires and employee transfers.	No exceptions noted.
CC6.2.2	The company performs annual access control reviews.	Inspected the annual access review documentation to determine that the company performed an annual access control review.	No exceptions noted.
CC6.2.3	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the new employees onboarding forms and the laptop delivery ticket for a sample of new employees to determine that appropriate levels of access to infrastructure and code review tools were granted to new employees within one week of their start date.	No exceptions noted.
CC6.2.4	Access to the corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the user access listing to determine that access to the corporate network, production machines, network devices, and support tools required a unique ID.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2.5	The company uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the termination checklist and the user access list to determine that the company used a termination checklist so that an employee's system access, including physical access, was removed within a specified timeframe and all organization's assets were properly returned.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed within one business day.
CC6.2.6	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected the termination tickets for a sample of terminated employees to determine that access to infrastructure and code review tools was removed from terminated employees within one business day.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed in accordance with the SLA of one business day
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.			
CC6.3.1	The company has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the Access Control Policy to determine that the company required an annual access control review to be conducted and access request forms to be filled out for new hires and employee transfers.	No exceptions noted.
CC6.3.2	The company performs annual access control reviews.	Inspected the annual access review documentation to determine that the company performed an annual access control review.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.3.3	The company uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the termination checklist and the user access list to determine that the company used a termination checklist so that an employee's system access, including physical access, was removed within a specified timeframe and all organization's assets were properly returned.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed within one business day.
CC6.3.4	Role-based security is in place for internal and external users, including super admin users.	Inspected the role-based access control to determine that role-based security was in place for internal and external users, including super admin users.	No exceptions noted.
CC6.3.5	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the new employees onboarding forms and the laptop delivery ticket for a sample of new employees to determine that appropriate levels of access to infrastructure and code review tools were granted to new employees within one week of their start date.	No exceptions noted.
CC6.3.6	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected the termination tickets for a sample of terminated employees to determine that access to infrastructure and code review tools was removed from terminated employees within one business day.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed in accordance with the SLA of one business day

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.3.7	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the user access listing to determine that access to corporate network, production machines, network devices, and support tools required a unique ID.	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.			
CC6.4.1	Management contracts with the Amazon Web Services (AWS) and Microsoft Azure to provide physical access security of its production systems; therefore, this criterion is carved out.	This control activity is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	The destruction of physical assets hosting the production environment is the responsibility of the Amazon Web Services (AWS) and Microsoft Azure; therefore, part of this criterion is carved out.	This control activity is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	
CC6.5.2	The company has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the Asset Management Policy to determine that the company had formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
		Inspected the device disposal records and certificates of destruction for a sample of disposed devices to determine that electronic media containing confidential information was purged or destroyed in accordance with best practices and that certificates of destruction were issued.	No exceptions noted.
CC6.5.3	The company disposes of hardcopy material with sensitive data when no longer needed (for legal or business reasons, or upon expiration of their retention period) through secure means such as cross-cut shredding, incinerating, or pulping, so that the data cannot be reconstructed.	Inspected the Asset Management Policy (2025–2026) and confirmed that the policy established procedures for disposing of hardcopy material containing sensitive data when no longer needed (for legal or business reasons, or upon expiration of their retention period) through secure means such as cross-cut shredding, incineration, or pulping, so that the data could not be reconstructed.	No exceptions noted.
		Per inquiry with management and inspection of the Jira ticket queue, it was noted that there were no instances of customer data disposal during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the network diagram to determine that the company maintained an accurate network diagram that was accessible to the engineering team and it was reviewed by management on an annual basis.	No exceptions noted.
CC6.6.2	The company ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the screensaver configurations for a sample of active employee's devices to determine that the company ensured that all company-issued computers used a screensaver lock with a timeout of no more than 15 minutes.	No exceptions noted.
CC6.6.3	Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configuration to determine that data in transit was encrypted using strong encryption algorithms.	No exceptions noted.
CC6.6.4		Inspected the Password Policy to determine that the company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
	The company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the password configurations for GitHub, AWS, AvePoint, Microsoft, Atlassian, and QuesTek systems to determine that the password requirements were enforced in accordance with the company's policy.	Exception noted: For one of six (17%) high-risk systems, the password configuration did not meet the requirements of the company's policy.
CC6.6.5	Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.	Inspected network security controls to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
CC6.6.6	The company uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Inspected the AWS network configurations to determine that only approved networking ports and protocols were implemented, including firewalls.	No exceptions noted.
CC6.6.7	WAF in place to protect the company's application from outside threats.	Inspected the WAF Ruleset to determine that WAF was in place to protect the company application from outside threats.	No exceptions noted.
CC6.6.8	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Intrusion Detection System (IDS) to determine that an intrusion detection system was in place to detect potential intrusions, alert personnel when a potential intrusion was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6.9	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the company's website and TLS certificate to determine that users could only access the production system remotely through the use of encrypted communication systems.	No exceptions noted.
CC6.6.10	The company restricts administrative access to system components to only authorized personnel (network, networking devices, database, operating system, application, encryption keys, moving changes to production).	Inspected the listings of administrative users for AWS, GitHub, Adobe, Atlassian Sentry, AvePoint, Microsoft, and QuesTek System to determine that administrative access was limited to only authorized personnel.	No exceptions noted.
CC6.6.11	The company requires authentication methods to in-scope systems to include a unique username, password, MFA, and/or SSH keys.	Inspected users listings for Atlassian, AWS, GitHub, AvePoint, AllCloud, Microsoft and QuesTek System. to determine that authentication to these systems required a unique username, password, MFA, and SSH keys.	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.			
CC6.7.1	The company uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inspected the encryption configurations to determine that the company used encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7.2	The company has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that a Data Protection Policy was established.	No exceptions noted.
		Inspected the Data Protection Policy acknowledgement for a sample of new employees to determine that new employees accepted the Data Protection Policy upon hire.	No exceptions noted.
CC6.7.3	The company ensures that company-issued laptops have encrypted hard-disks.	Inspected the laptop hard disk encryption settings for a sample of company-issued laptops to determine that company-issued laptops had encrypted hard-disks.	No exceptions noted.
CC6.7.4	Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
CC6.7.5	Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configuration to determine that data in transit was encrypted using strong encryption algorithms.	No exceptions noted.
CC6.7.6	SSH users use unique accounts to access production machines. Additionally, the use of the root account is not allowed.	Inspected the production machines to determine that SSH users used unique accounts to access production machines.	No exceptions noted.
		Inspected the root SSH configuration to determine that the use of the root account was not allowed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7.7	Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.	Inspected network security controls to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
CC6.7.8	The company ensures that company-issued removable media devices (USB drives) are blocked.	Inspected the USB device control configurations to determine that company-issued removable media devices (USB drives) were blocked.	No exceptions noted.
CC6.7.9	The company uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email	Inspected the Data Loss Prevention configurations to determine that the company used a DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the Antivirus configurations for a sample of workstations to determine that the company required antivirus software to be installed on workstations to protect the network against malware.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.8.2	The company's workstations operating system (OS) security patches are applied automatically.	Inspected the workstations configurations for a sample of company-issued workstations during the examination period to determine that workstations operating system (OS) security patches were applied automatically.	No exceptions noted.
CC6.8.3	The company ensures that virtual machine OS patches are applied monthly.	Inspected the patching configurations to determine that the company ensured that virtual machine OS patches were applied monthly.	No exceptions noted.
CC6.8.4	The company has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the infrastructure logging configurations to determine that company had infrastructure logging configured to monitor web traffic and suspicious activity and alerts were automatically created, sent to appropriate personnel and resolved, as necessary when anomalous traffic activity was identified.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC7.1.1	The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Inspected the version control system access listing and configurations to determine that the company used a version control system to manage source code, documentation, release labeling, and other change management tasks.	No exceptions noted.
		Inspected the Admin Access to GitHub to determine that access to the system was approved by a system administrator.	No exceptions noted.
CC7.1.2	When the company's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected the change management tickets for a sample of application code changes to determine that application code changes, code reviews, and tests were performed by someone other than the person who made the code change.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.3	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC7.1.4	The company engages with third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the penetration test report to determine that the company engaged with a third-party to conduct penetration tests of the production environment annually.	No exceptions noted.
		Inspected the annual penetration test report to determine that the results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.
CC7.1.5	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Intrusion Detection System (IDS) to determine that an intrusion detection system was in place to detect potential intrusions, alert personnel when a potential intrusion was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.6	The company has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the infrastructure logging configurations to determine that company had infrastructure logging configured to monitor web traffic and suspicious activity and alerts were automatically created, sent to appropriate personnel and resolved, as necessary when anomalous traffic activity was identified.	No exceptions noted.
CC7.1.7	The company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Drata platform to determine that the company conducted continuous monitoring of security controls using Drata, and addressed issues in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC7.2.1	The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the production patching for a sample of quarterly vulnerability scan remediations to determine that results of vulnerability scans were reviewed by management and high priority findings were tracked to resolution.	Exception noted: For 917 of 932 (98%) high-severity vulnerabilities and 45 of 46 (98%) critical-severity vulnerabilities, remediation was not completed within the defined SLA.
CC7.2.2	The company's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel	Inspected the operational audit system to determine that the company cloud infrastructure was monitored through an operational audit system that sent alerts to appropriate personnel.	No exceptions noted.
CC7.2.3	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.4	The company uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.	Inspected the SIEM configurations to determine that the company used a system that collected and stored server logs in a central location.	No exceptions noted.
		Inspected the SIEM configurations to determine that the system could be queried in an ad hoc fashion by authorized users.	No exceptions noted.
CC7.2.5	The company is using Drata to monitor the security and compliance of its cloud infrastructure configuration	Inspected the Drata platform to determine that the company used Drata to monitor the security and compliance of its cloud infrastructure configuration.	No exceptions noted.
CC7.2.6	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Intrusion Detection System (IDS) to determine that an intrusion detection system was in place to detect potential intrusions, alert personnel when a potential intrusion was detected.	No exceptions noted.
CC7.2.7	The company uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Inspected the Alert Logic FIM to determine that the company used logging software that sent alerts to appropriate personnel.	No exceptions noted.
		Inspected the security incident ticket for a sample of logging alerts to determine that corrective actions were performed, as necessary, in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.8	The company has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the infrastructure logging configurations to determine that company had infrastructure logging configured to monitor web traffic and suspicious activity and alerts were automatically created, sent to appropriate personnel and resolved, as necessary when anomalous traffic activity was identified.	No exceptions noted.
CC7.2.9	The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Incident Response Plan to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
		Inspected the entire population of incidents to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC7.3.1	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.
CC7.3.2	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.3.3	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.3.4	The security team communicates important information security events to company management in based on the severity of the identified incident.	Inspected the incident log for a sample of incidents to determine that the security team communicated important information security events to company management in a timely manner.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the security team communicated important information security events to company management in based on the severity of the identified incident.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.3.5	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.
CC7.3.6	The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Incident Response Plan to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
		Inspected the entire population of incidents to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC7.4.1	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.
CC7.4.2	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.3	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.4.4	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management’s responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.5	The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Incident Response Plan to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
		Inspected the entire population of incidents to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
CC7.4.6	The company ensures that incident response plan testing is performed on an annual basis.	Inspected the Incident Response Plan Test to determine that the Incident Response Plan testing was performed on an annual basis.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Data Security Incident Management Roles & Responsibilities policy to determine that the company has established a Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.2	The company has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included creating, prioritizing, assigning, and tracking follow-ups to completion and lent support to Business Continuity/Disaster Recovery.	No exceptions noted.
CC7.5.3	The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Data Security Incident Management Roles & Responsibilities Policy to determine that the company had identified an incident response team that quantified and monitored incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.4	The company has implemented an Incident Response Plan that includes documenting Lessons Learned and Root Cause Analysis after incidents and sharing them with management/leadership.	Inspected the Incident Response Plan to determine that the company implemented an Incident Response Plan that included documenting lessons learned and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	No exceptions noted.
		Inspected the entire population of security incident tickets to determine that the company had incident response policies and procedures to ensure that security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.5.5	The company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected backup configurations for daily backups to determine that the company performed daily backups and retained them in accordance with a predefined schedule in the Backup Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.6	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.
CC7.5.7	The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Incident Response Plan to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
		Inspected the entire population of incidents to determine that the company tracked and prioritized security deficiencies according to their severity, with severity levels assessed by the internal security team based on predefined criteria.	No exceptions noted.
CC7.5.8	The company has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the company had a defined Business Continuity Plan that outlined the proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.9	The company ensures that incident response plan testing is performed on an annual basis.	Inspected the Incident Response Plan Test to determine that the Incident Response Plan testing was performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC8.1.1	The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Inspected the version control system access listing and configurations to determine that the company used a version control system to manage source code, documentation, release labeling, and other change management tasks.	No exceptions noted.
		Inspected the Admin Access to GitHub to determine that access to the system was approved by a system administrator.	No exceptions noted.
CC8.1.2	When the company's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected the change management tickets for a sample of application code changes to determine that application code changes, code reviews, and tests were performed by someone other than the person who made the code change.	No exceptions noted.
CC8.1.3	Only authorized personnel can push or make changes to production code.	Inspected the GitHub list of users to determine that only authorized the company personnel could push or make changes to production code.	No exceptions noted.
CC8.1.4	Separate environments are used for testing and production for the company's application	Inspected the network diagram to determine that separate environments were used for testing and production for the company application.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.5	The company has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Software Development Lifecycle Policy to determine that the company developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted.
CC8.1.6	The company ensures that code changes are tested prior to deployment to ensure quality and security.	Inspected the change management tickets for a sample of changes to determine that code changes were tested prior to deployment.	No exceptions noted.
CC8.1.7	The company ensures that releases are approved by appropriate members of management prior to production release.	Inspected the change management tickets for a sample of releases to determine that releases were approved by appropriate members of management prior to production release.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Security Risk Strategy Policy to determine that the company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC9.1.2	The company has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Data Security Incident Management Roles & Responsibilities policy to determine that the company has established a Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.
CC9.1.3	The company utilizes multiple availability zones to replicate production data across different zones.	Inspected the replication configurations to determine that the company utilized multiple availability zones to replicate production data across different zones.	No exceptions noted.
CC9.1.4	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the cybersecurity insurance to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1.5	The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity/Disaster Recovery Test to determine that the company conducted annual BCP/DR tests and documented them according to the BCDR Plan.	No exceptions noted.
CC9.1.6	The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the company established an Incident Response Plan that outlined management's responsibilities and procedures for a quick, effective, and orderly response to information security incidents and annual testing.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including its agreements that specified terms, conditions, and responsibilities.	No exceptions noted.
CC9.2.2	The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Drata platform to determine that the company maintained a directory of its key vendors, including their compliance reports.	No exceptions noted.
		Inspected the review documentation and the vendor compliance reports for critical vendors to determine that critical vendor compliance reports were reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.2.3	The company has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company defined a policy that established requirements for third-parties to meet the organization's data preservation and protection requirements.	No exceptions noted.

SECTION 5:
OTHER INFORMATION PROVIDED BY QUESTEK INNOVATIONS LLC

MANAGEMENT'S RESPONSES TO THE NOTED EXCEPTIONS

Control Activity	Noted Exceptions	Management's Responses
The company engages with third parties to conduct vulnerability scans of the production environment continuously. Results are reviewed by management, and high-priority findings are tracked to resolution.	Exception noted: For 917 of 932 (98%) High-severity and 45 of 46 (98%) Critical-severity vulnerabilities, the remediation completion exceeded the defined SLA.	Immediate Remediations: A new MSP has been engaged to remediate vulnerabilities properly within SLA thresholds, with monthly recurring meetings established to review remediation progress. Root Cause & Long-Term Prevention: The prior MSP failed to provide required monthly reports and subsequently closed operations, creating visibility gaps, and management will prevent recurrence by conducting monthly reviews with the new MSP to ensure vulnerabilities are addressed in a timely manner.
The company uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed within one business day.	Immediate Remediations: With the current IT person in place, offboarding tasks are now being executed in a timely manner, and HR will submit the offboarding form directly to the MSP if the IT person is unavailable. Root Cause & Long-Term Prevention: The gap between the departure of the prior IT staff and onboarding of the new IT person caused delays in access revocation, and management will prevent recurrence by ensuring the offboarding form is consistently completed and followed
Access to infrastructure and code review tools is removed from terminated employees within one business day.	Exception noted: For two of four (50%) samples of terminated employees, access was not removed in accordance with the SLA of one business day	

Control Activity	Noted Exceptions	Management's Responses
		through by HR or IT to enforce timely access removal.
The company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Exception noted: For one of six (17%) high-risk systems, the password configuration did not meet the requirements of the company's policy.	Immediate Remediations: Atlassian's password policy has been updated to enforce very strong complexity requirements, requiring all four elements (uppercase, lowercase, numeric, and non-alphanumeric characters). Root Cause & Long-Term Prevention: Atlassian previously failed to enforce the defined password complexity requirements, creating a high risk of potential breaches, and management has now implemented and will maintain the very strong password policy to ensure compliance and prevent recurrence.