Insight Assurance

SOC 2 | ISO 27001 | PCI | HIPAA

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

Report on QuesTek Innovations LLC's Description of Its ICMD® Services System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period November 27, 2023, to February 26, 2024

QUESTEK® INNOVATIONS LLC

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT **1**

INDEPENDENT SERVICE AUDITOR'S REPORT 2

SECTION 2: QUESTEK INNOVATIONS LLC'S MANAGEMENT ASSERTION **7**

QUESTEK INNOVATIONS LLC'S MANAGEMENT ASSERTION 8

SECTION 3: QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® SERVICES SYSTEM **10**

QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® SERVICES SYSTEM 11

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS **28**

TRUST SERVICES CRITERIA FOR SECURITY CATEGORY 30

SECTION 5: OTHER INFORMATION PROVIDED BY QUESTEK INNOVATIONS LLC **80**

MANAGEMENT RESPONSE TO EXCEPTIONS 81

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
SOC 2 | ISO 27001 | PCI | HIPAA

INDEPENDENT SERVICE AUDITOR'S REPORT

To: QuesTek Innovations LLC

Scope

We have examined QuesTek Innovations LLC's ('QuesTek Innovations' or 'the Service Organization') description of its ICMD® Services System found in Section 3 titled "QuesTek Innovations LLC's description of its ICMD® Services System" throughout the period November 27, 2023, to February 26, 2024 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (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 November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 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 Innovations uses Amazon Web Services (AWS) 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 Innovations, to achieve QuesTek Innovations' service commitments and system requirements based on the applicable trust services criteria. The description presents QuesTek Innovations' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of QuesTek Innovations' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at QuesTek Innovations, to achieve QuesTek Innovations' service commitments and system requirements based on the applicable trust services criteria. The description presents QuesTek Innovations' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of QuesTek Innovations' 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 the management of QuesTek Innovations to provide additional information and is not part of QuesTek Innovations LLC's description. Information about QuesTek Innovations

management 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 meet the applicable trust services criteria, and accordingly, we do not express an opinion on it.

Service Organization's Responsibilities

QuesTek Innovations 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 Innovations' service commitments and system requirements were achieved. In Section 2, QuesTek Innovations has provided the accompanying assertion titled "QuesTek Innovations LLC' Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. QuesTek Innovations is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

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

Inherent Limitations

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

Description of Test of Controls

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

Basis for Qualified Opinion

QuesTek Innovations states in its description of its ICMD® Services System that QuesTek Innovations requires penetration testing to be performed at least annually and vulnerability scanning to be performed monthly and implement changes to remediate the identified critical and high vulnerabilities in accordance with SLAs. However, 3 out of 3 high vulnerabilities identified during penetration testing and 24 out of 24 high vulnerabilities identified during vulnerability scans were not remediated in accordance with SLAs. As a result, the controls were not operating effectively during the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on trust services criteria.

- CC4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- CC4.2: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

- 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.
- CC7.2: 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.

Opinion

In our opinion, except for the matters giving rise to the modifications described in the preceding paragraphs in all material respects,

- the description presents QuesTek Innovations' ICMD® Services System that was designed and implemented throughout the period November 27, 2023, to February 26, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of QuesTek Innovations' controls throughout that period.
- the controls stated in the description operated effectively throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' 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 Innovations' controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of QuesTek Innovations, user entities of QuesTek Innovations' ICMD® Services System throughout the period November 27, 2023, to February 26, 2024, and business partners of QuesTek Innovations subject to risks arising from interactions with the ICMD® Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, 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 Assurance LLC

Tampa, Florida
July 18, 2024

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 Innovations' or 'the Service Organization') ICMD® Services System entitled "QuesTek Innovations LLC's description of its ICMD® Services System" throughout the period November 27, 2023, to February 26, 2024 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) The description is intended to provide report users with information about the ICMD® Services System that may be useful when assessing the risks arising from interactions with QuesTek Innovations' system, particularly information about system controls that QuesTek Innovations 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*.

QuesTek Innovations uses Amazon Web Services (AWS) 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 Innovations, to achieve QuesTek Innovations' service commitments and system requirements based on the applicable trust services criteria. The description presents QuesTek Innovations' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of QuesTek Innovations' controls. The description does not disclose the actual controls at the subservice organization.

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

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

- the description presents QuesTek Innovations' ICMD® Services System that was designed and implemented throughout the period November 27, 2023, to February 26, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of QuesTek Innovations' controls.

- except for the matter described in the bullet point below, the controls stated in the description operated effectively throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' 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 Innovations' controls operated effectively throughout that period.
- QuesTek Innovations states in its description of its ICMD® Services System that QuesTek Innovations requires penetration testing to be performed at least annually and vulnerability scanning to be performed monthly and implement changes to remediate the identified critical and high vulnerabilities in accordance with SLAs. However, 3 out of 3 high vulnerabilities identified during penetration testing and 24 out of 24 high vulnerabilities identified during vulnerability scans were not remediated in accordance with SLAs. As a result, the controls were not operating effectively during the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on trust services criteria.
    - CC4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
    - CC4.2: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
    - 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.
    - CC7.2: 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.

QuesTek Innovations LLC
July 18, 2024

SECTION 3: QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® SERVICES SYSTEM

QUESTEK INNOVATIONS LLC'S DESCRIPTION OF ITS ICMD® Services System

COMPANY BACKGROUND

QuesTek Innovations LLC ("QuesTek Innovations") is a privately held company established in October 1998 that offers Software as a Service. QuesTek Innovations is an LLC headquartered in Evanston, Illinois.

DESCRIPTION OF SERVICES OVERVIEW

ICMD® is a digital materials design platform including toolkits for materials design, accelerated qualification and certification, informatics and analytics, and simulation. Toolkits utilize QuesTek's Materials by Design® technology to provide proven models, datasets, and workflows, including third-party software and databases to support design processes. Access the expertise, models, and materials data generated over our 25-year history as pioneers and leaders in integrated computational materials engineering.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

QuesTek Innovations designs its processes and procedures related to the QuesTek Innovations' ICMD® Services system ("System") to meet its objectives. Those objectives are based on the service commitments that QuesTek Innovations makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that QuesTek Innovations has established for the services.

QuesTek Innovations' commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and other customer agreements, as well as in the description of the service offering provided online.

Security Commitments

Security commitments are standardized and 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.
- Uptime availability of production systems.

QuesTek Innovations establishes operational requirements that support the achievement of security, availability, and confidentiality, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In

addition, how to carry out specific manual and automated processes required in the operation and development of the System.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

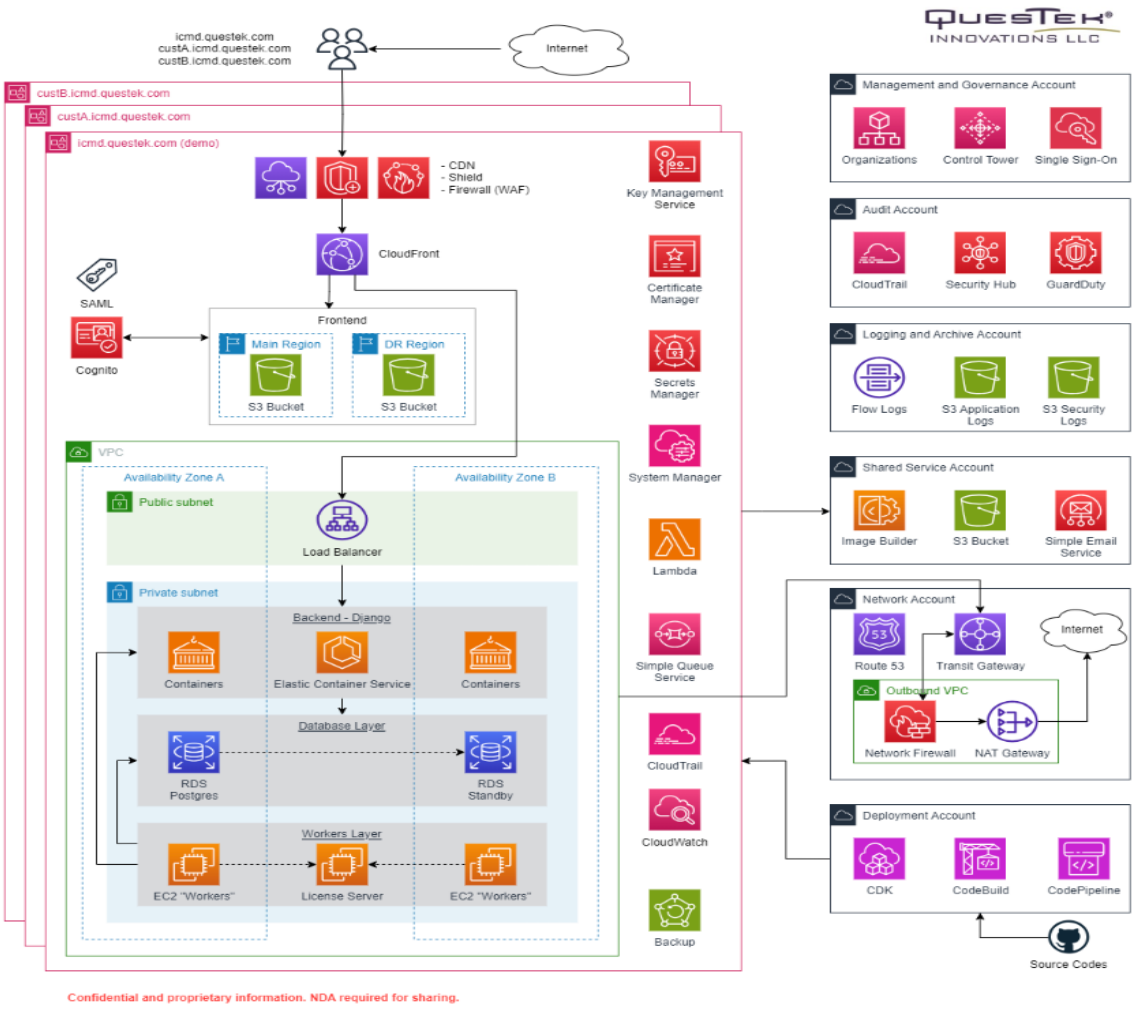
- **Infrastructure** – The collection of physical or virtual resources that support an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile 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 supports 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 Innovations maintains a system inventory that includes AWS, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, device type, vendor function, OS, location, and notes.

To outline the topology of its network, the organization maintains the following network diagram.

ICMD® Architecture:



The QuesTek Innovations application infrastructure is located at AWS data centers. SSO acts as a hosting subservice organization for the company. The subservice organization provides the physical security and environmental protection controls, as well as managed services for QuesTek Innovations' infrastructure.

SSO's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, QuesTek Innovations uses anti-virus and anti-spyware applications to protect systems from viruses.

QuesTek Innovations' Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the QuesTek Innovations network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping

the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on QuesTek Innovations-owned computers. The IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

Primary Infrastructure		
Category	**Description**	**Examples**
AWS Elastic Compute Cloud (EC2)	AWS	Compute system in the cloud
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload, and download
AWS CloudFront	AWS	Masks S3 bucket paths
AWS CloudWatch	AWS	Monitoring service and log storage
AWS Internet Gateway	AWS	Allows communication between instances in your Amazon VPC and the Internet
AWS WAF	AWS	Web application firewall
Amazon RDS	AWS	Simplifies database management in the cloud

SOFTWARE

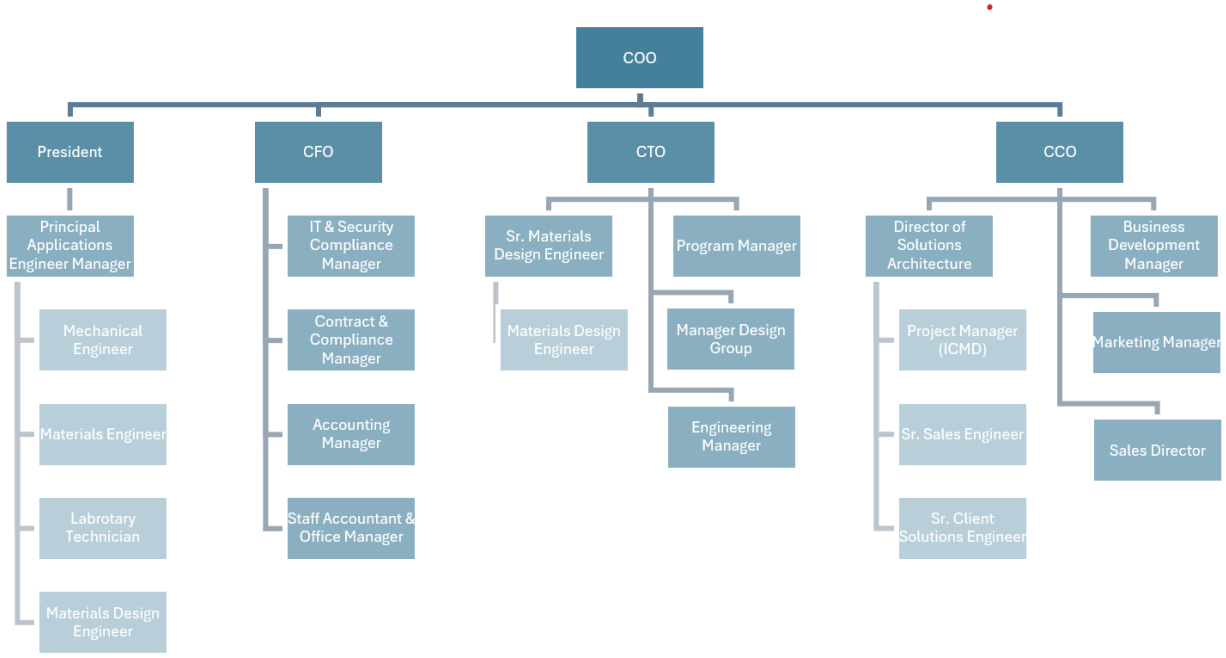
QuesTek Innovations maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

Primary Software		
System/Application	**Operating System**	**Purpose**
AWS	Linux/ Windows	The cloud provider that hosts the ICMD® Software
Datadog	SaaS	Monitoring of 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 centralized knowledge repository

PEOPLE

The QuesTek Innovations staff provides support for the above services. QuesTek Innovations employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep QuesTek Innovations and its data secure.

QuesTek Innovations' 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.

Chief Commercial Officer (CCO) – Plans and directs all aspects of an organization's marketing and sales policies, objectives, and initiatives. Directs the planning, forecasting, marketing program development, partner relationship development, collateral material development, and customer satisfaction initiatives. Establishes short- and long-term sales goals and quotas in line with corporate objectives. Identifies key marketing outlets and competitive strategies that will enable the achievement of maximum sales volume. Manages a business unit, division, or corporate function with major organizational impact. Establishes overall direction and strategic initiatives for the given major function or line of business. Has acquired the business acumen and leadership experience to become a top function or division head.

Sales and Marketing – Directs the execution of the business development vision, strategy, plans, and processes to drive sales, increase revenue, expand markets, and accomplish financial objectives. Identifies and evaluates new markets, partners, channels, and customers. Develops and uses contacts and relationships within the industry, business environment, and customer

base to understand and respond to competition, pricing, and product demand changes. Oversees the development of proposals and contracts for new business opportunities and manages negotiations. Collaborates with marketing, sales, product development, and other stakeholders to support business development plans. Manages a departmental sub-function within a broader departmental function. Creates functional strategies and specific objectives for the sub-function and develops budgets/policies/procedures to support the functional infrastructure.

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

Chief Information Officer – Responsible for the long-range direction of an organization's technology function. Directs the strategic design, acquisition, management, and implementation of an enterprise-wide technology infrastructure. Monitors and analyzes technology and trends that could improve the company's products and performance. Establishes technology standards and communicates technical information to the organization. Manages a business unit, division, or corporate function with major organizational impact. Establishes overall direction and strategic initiatives for the given major function or line of business. Has acquired the business acumen and leadership experience to become a top function or division head.

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 of 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 the support of end-users with day-to-day issues, as well as assisting in the onboarding, implementation, and migrations 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 Innovations in delivering its ICMD® Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed, or written on paper, and spoken in conversations. All employees and contractors of QuesTek Innovations are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to QuesTek Innovations' business and finances are, as a matter of QuesTek Innovations policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring

compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

QuesTek Innovations has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Data Category		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for QuesTek Innovations.	• 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 by QuesTek Innovations. QuesTek Innovations 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 Innovations to operate the business. QuesTek Innovations 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

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and are located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

These policies and procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security and Environmental Controls

QuesTek Innovations' production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. QuesTek Innovations reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

SSO handles the network, physical host, and virtual server infrastructure. QuesTek Innovations handles the administrative responsibilities involved in supporting the web, application, and database components of the system. QuesTek Innovations has full access to log into their servers remotely using a secure shell (SSH) or Windows Remote Desktop, depending on the platform. Dedicated firewalls are used to restrict administrative access to servers. Appropriate firewall rules are in place to restrict access to customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

Logical access to QuesTek Innovations' networks, applications, and data is limited to properly authorized individuals. For both the client-hosted network and the QuesTek Innovations local network, logical access is controlled via standard user authentication credentials (user ID and password). No other outside access is permitted.

Computer Operations

Customer data is backed up and monitored by the Technology and Engineering Team for completion and exceptions. If there is an exception, the Technology and Engineering Team will

perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

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

QuesTek Innovations 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.

Change Management

For internally developed software platforms/solutions, QuesTek Innovations uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before the final release. All software development activities follow the internal project-related business process model.

QuesTek Innovations has a Change Management Policy in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require forethought, monitoring, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of Information Resources. The QuesTek Innovations Change Management Policy applies to all individuals who install, operate, or maintain Information Resources.

Patch Management

QuesTek Innovations takes a proactive approach to patch management. The CIO and engineers regularly monitor various websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. This allows the company to plan for upcoming patches.

The DevOps team reviews the availability of patches and independently determines if it is necessary to deploy within the production environment. Approved patches are scheduled for installation in the test environment weekly as applicable. If there are no issues in the test environment after a week, the patch will be applied to the production environment. The patching process is tracked via a JIRA SEC ticket.

Backup and Recovery

QuesTek Innovations maintains full system replication of the production platform within the AWS architecture. All ICMD components containing customer data are backed up with a 30-day retention period, following the Well-Architected suggestions from AWS for minimum risks of losing customer data. Critical codebases for the ICMD system, which do not store any customer data, are also backed up or secured. All backup methods are encrypted and separated from their sources/services for maximum security.

Problem Management

QuesTek Innovations maintains an Incident Response Policy 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, the organization provides formal security breach training.

The organization provides a customer service request form where clients can report potential security breaches, and clients are also provided with an email and phone number for this same purpose. Internal users are directed to report incidents through an internal portal for documentation and tracking purposes.

System Monitoring

The Network Security and Vulnerability Management Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses CloudWatch for system logging within the AWS environment, and the organization collects logs from the firewall. CloudWatch logs and firewall logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using Guard Duty.

AWS Guard Duty and Sentry.io are used for threat and intrusion detection by analyzing several types of logs such as VPC flow logs, API logs, Cloud access logs, DNS logs, etc. Alert rules are implemented with a subscription to notify relevant QuesTek Innovations employees within Sentry.io and in AWS using AWS Event Bridge.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Trend Micro antivirus 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. Alert Logic is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Vendor Management

The organization 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. The organization 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. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Data Communications

QuesTek Innovations has elected to use Amazon Web Services (AWS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The AWS simplifies our logical network configuration by providing an effective firewall around all the QuesTek Innovations application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The AWS also automates 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 the underlying hardware.

QuesTek Innovations uses a monitoring service to perform vulnerability scans before each deployment and engages an external firm to perform an annual penetration test to look for unidentified vulnerabilities. The Technology and Engineering Team responds to any issues identified via the regular incident response and change management policies.

Boundaries of the System

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

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

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

The Security category is used to evaluate the suitability of the design of controls stated in the description. Security criteria and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services Security criteria are included in Section 4 of this

report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of QuesTek Innovations' description of its system.

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. The Board of Directors and/or senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Management Philosophy, Integrity, and Ethical Values

QuesTek Innovations' control environment reflects the philosophy of senior management concerning the importance of the security of data. Integrity and ethical values are essential elements of QuesTek Innovations' control environment. Management is responsible for setting the tone at the top, establishing, communicating, and monitoring control policies and procedures.

Formal policies, code of conduct, and employee handbooks are documented and communicated to employees to ensure that entity values, ethics, integrity, and behavioral standards are a primary focus, and risks are mitigated in daily operations. In addition, a sanctions policy is in place to address deviations from established security and personnel standards.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. QuesTek Innovations places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions, departmental meetings, and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under QuesTek Innovations' policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Commitment to Competence

QuesTek Innovations has standardized human resource policies and procedures. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization.

Training and development opportunities are provided to staff and performance evaluations are performed to communicate goals based on job responsibilities and address any performance issues.

Employees are trained on their specific roles and policies through on-the-job training and procedures are reviewed. Management communicates any changes to these policies on an ongoing basis and policies are updated as needed. In order to protect confidential internal and client information employees are prohibited from divulging any information regarding client affairs or taking action, not in the interests of the client or QuesTek Innovations.

Organizational Structure and Assignment of Authority and Responsibility

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

QuesTek Innovations 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 individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

Human Resources Policies and Procedures

QuesTek Innovations 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 including 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. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employee's performance for the last fiscal year.

RISK ASSESSMENT PROCESS

QuesTek Innovations regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security, availability, and confidentiality. The Risk assessment process is performed by management to identify and manage risks and consider possible changes in the internal and external environment to mitigate these risks. Risk mitigation activities include the prevention, mitigation, and detection of risk via the implementation of internal controls. In addition, management also transfers risk through the organization's business insurance policies.

The QuesTek Innovations management team and other members of the engineering team monitor risk on an ongoing basis using information derived from employee input, system monitoring, audit results, industry experience, business environment, and internal system and/or process changes.

On an annual basis, management completes a risk assessment as part of the annual risk management activities. Risks identified during the annual risk assessment process include the following:

- Operational Risk
- Strategic Risk
- Compliance Risk
- Fraud Risk
- Environmental Risk

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 Innovations 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 Innovations.

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

MONITORING CONTROLS

In addition to daily oversight, and vulnerability assessments, management uses monitoring software to monitor the security and availability of their systems. Ongoing monitoring of internal controls is also performed by management.

Monitoring of the Subservice Organization

QuesTek Innovations uses a subservice organization to provide hosting services.

The management of QuesTek Innovations receives and reviews the SOC 2 report of AWS on an annual basis. In addition, through its daily operational activities, the management of QuesTek Innovations monitors the services performed by AWS to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

Ongoing Monitoring

QuesTek Innovations 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 Innovations 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 the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of QuesTek Innovations personnel.

Reporting Deficiencies

Our 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.

TRUST SERVICE CATEGORY

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

CONTROL ACTIVITIES AND CRITERIA

The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancies that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of QuesTek Innovations' description of controls.

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

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 Period

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

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

QuesTek Innovations' controls related to the System cover only a portion of overall internal control for each user entity of QuesTek Innovations. It is not feasible for the trust services criteria related to the System to be achieved solely by QuesTek Innovations. Therefore, each user entity's internal controls should be evaluated in conjunction with QuesTek Innovations' controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Amazon Web Services (AWS) is responsible for maintaining the physical security controls over the data centers hosting the QuesTek Innovations infrastructure.	CC6.4
2	Amazon Web Services (AWS) is responsible for the destruction of physical assets hosting the production environment.	CC6.5

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

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

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

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

User auditors should determine whether the following controls have been in place in operation at the user organization:

- Controls to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
- User entities are responsible for reporting issues with QuesTek Innovations systems and platforms.
- User entities are responsible for understanding and complying with their contractual obligations to QuesTek Innovations.
- User entities are responsible for notifying QuesTek Innovations of changes made to the administrative contact information.

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

Trust Services Category, Criteria, Related Controls, and Test 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 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 November 27, 2023, to February 26, 2024.

The trust services criteria for the Security category and related controls specified by QuesTek Innovations 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.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.1.2	The company requires employees to acknowledge a Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	Inspected the Code of Conduct acknowledgment for a sample of new employees during the examination period to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Inspected the Code of Conduct acknowledgments for a sample of active employees during the examination period to determine that the Code of Conduct was acknowledged at least annually.	No exceptions noted.
CC1.1.3	The company requires employees to review and acknowledge the Information Security policies at the time of hire and active employees to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of new employees during the examination period to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC1.1.3 *(cont.)*	The company requires employees to review and acknowledge the Information Security policies at the time of hire and active employees to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of active employees during the examination period to determine that the information security policies were acknowledged at least annually.	No exceptions noted.
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.1.5	The company performs background checks on new employees.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement prior to access to confidential information and processing facilities.	Inspected the signed non-disclosure agreements for a sample of new employees to determine that new employees were required to review and acknowledge the confidentiality agreement at the time of hire.	No exceptions noted.
Criteria: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
QuesTek Innovations does not have an independent board of directors; therefore, this criterion is not applicable.			

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned within the Information Security Policy.	Inspected the company's Information Security Policy to determine the IT & Compliance Analyst roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls that were formally assigned.	No exceptions noted.
CC1.3.3	The company requires employees to review and acknowledge the Information Security policies at the time of hire and active employees to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of new employees during the examination period to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Inspected the information security policies acknowledgment for a sample of active employees during the examination period to determine that the information security policies were acknowledged at least annually.	No exceptions noted.
Criteria: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company performs background checks on new employees.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned within the Information Security Policy.	Inspected the company's Information Security Policy to determine that the IT & Compliance Analyst roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls that were formally assigned.	No exceptions noted.
CC1.4.4	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.5.2	The company requires employees to acknowledge a Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	Inspected the Code of Conduct acknowledgment for a sample of new employees during the examination period to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Inspected the Code of Conduct acknowledgments for a sample of active employees during the examination period to determine that the Code of Conduct was acknowledged at least annually.	No exceptions noted.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned within the Information Security Policy.	Inspected the company's Information Security Policy to determine that the IT & Compliance Analyst roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls that were formally assigned.	No exceptions noted.
CC1.5.5	The company requires new employees to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees and contractors to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were reviewed and approved annually.	No exceptions noted.
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned within the Information Security Policy.	Inspected the company's Information Security Policy to determine that the IT & Compliance Analyst roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls that were formally assigned.	No exceptions noted.
CC2.2.3	The company requires new employees to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC2.2.3 *(cont.)*	The company requires new employees to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the training records for a sample of active employees to determine that the company required employees and contractors to complete security awareness training annually.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were reviewed and approved annually.	No exceptions noted.
CC2.2.5	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.2.6	The company communicates system changes to authorized internal users.	Inspected the example communication to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
Criteria: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in the Privacy Policy and Terms of Use.	Inspected the Terms of Use and Privacy Policy to determine that the company's security commitments were communicated to customers in the Terms of Use and Privacy Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's Resources page to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.3	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company described its products and services to internal and external users.	No exceptions noted.
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that the company had the contact information on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3.5	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Conditions and Privacy Policy for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected Release Notes to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and the subservice organization.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's Business Continuity and Disaster Recovery Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan testing exercise report to determine that the BC/DR plan was tested annually.	No exceptions noted.
Criteria: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed at least annually.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	**Exceptions noted.** For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC4.1.3	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report within the examination period to determine that vulnerability scans were performed monthly on in-scope systems.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	**Exceptions noted.** For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.
CC4.1.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and the subservice organization.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and the subservice organization.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC4.2.3	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed at least annually.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	**Exceptions noted.** For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.
CC4.2.4	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report within the examination period to determine that vulnerability scans were performed monthly on in-scope systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC4.2.4 *(cont.)*	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	**Exceptions noted.** For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were reviewed and approved annually.	No exceptions noted.
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.1.4	Role-based access is configured within AWS, and other supporting applications to enforce segregation of duties and restrict access to confidential information.	Inspected the system configuration for AWS, and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
Criteria: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.2.3 *(cont.)*	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were reviewed and approved annually.	No exceptions noted.
Criteria: 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's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were reviewed and approved annually.	No exceptions noted.
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Software Development Life Cycle (SDLC) Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.3.2 *(cont.)*	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.3	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.3.6	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned within the Information Security Policy.	Inspected the company's Information Security Policy to determine that the IT & Compliance Analyst roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls that were formally assigned.	No exceptions noted.
CC5.3.8	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and the subservice organization.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access & Authorization Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.2	The company has a Data Management program to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's Data Classification Policy, Data Protection Policy, and Data Retention Policy to determine that the company had Data Classification Policy, Data Protection Policy, and Data Retention Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	Inspected the configuration of the AWS housing sensitive customer data and determined that data was encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Encryption Policy to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
		Inspected the list of users with privileged access to encryption keys to determine that the company restricted privileged access to authorized users with a business need.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.1.5	Role-based access is configured within AWS, and other supporting applications to enforce segregation of duties and restrict access to confidential information.	Inspected the system configuration for AWS, and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	Inspected the list of users with privileged access to the cloud infrastructure and application to determine that the company restricted privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the list of users with privileged access to the firewall to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.1.9	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.13	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network diagram/ network configurations to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access & Authorization Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the offboarding checklist and in-scope user listings for a sample of terminated employees and contractors to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs	No exceptions noted.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.2.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: 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's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access & Authorization Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the offboarding checklist and in-scope user listings for a sample of terminated employees and contractors to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.3.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: 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 AWS to provide physical access security of its production systems; therefore, this criterion is carved out.	This criterion is the responsibility of the subservice organization. Refer to the Subservice organization's section above for controls managed by the subservice organization.	
Criteria: 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 company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.	Per inquiry with management and inspection of the data disposal log, no disposal performed during the examination period; therefore, no testing was performed.	No testing performed. Insight Assurance did not perform any testing of the operating effectiveness of this control activity as the circumstances that warranted the operation of this control activity did not occur during the examination period.
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of AWS; therefore, part of this criterion is carved out.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
Criteria: CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
Criteria: 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 encrypts portable and removable media devices when used.	Inspected the company's Data Classification Policy to determine that the company encrypted portable and removable media devices when used.	No exceptions noted.
		Inspected employee computers and determined that each was protected with full-disk encryption.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7.3	The company has a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	Inspected the company's mobile device monitoring system to determine that the company had a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	No exceptions noted.
Criteria: 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 deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks.	No exceptions noted.
		Inspected the anti-malware configurations for a sample of workstations to determine that the anti-malware software was configured to scan workstations daily and install updates as new updates/signatures were available.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.8.2	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Software Development Life Cycle (SDLC) Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1.3	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report within the examination period to determine that vulnerability scans were performed monthly on in-scope systems.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	**Exceptions noted.** For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed at least annually.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	**Exceptions noted.** For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.
CC7.1.5	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Asset Management Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC7.1.6	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.2.5	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report within the examination period to determine that vulnerability scans were performed monthly on in-scope systems.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	**Exceptions noted.** For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.2.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed at least annually.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	**Exceptions noted.** For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.
CC7.2.7	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	Inspected the security incident report covering the observation period to determine that security incidents were reported to the IT personnel and tracked through to resolution in a ticketing system.	No exceptions noted.
Criteria: 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 security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's 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.
		Inspected the incident ticket for a sample of incidents to determine that the company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
Criteria: 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 security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's 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			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.4.3	The company has a documented Incident Response Plan and tests it at least annually.	Inspected the company's Incident Response Plan Policy is in place and approved by management.	No exceptions noted.
		Inspected the company's incident response plan test notes to determine that the company tests its incident response plan at least annually.	No exceptions noted.
Criteria: CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Operations Security Policy and Incident Response Plan to determine that the company's 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.
		Inspected the incident ticket for a sample of incidents to determine that the company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.5.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.5.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's Business Continuity Policy and Disaster Recovery Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan testing exercise report to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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 has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Software Development Life Cycle Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Software Development Life Cycle (SDLC) Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC8.1.3	Segregation of duties is in place to prevent developers from pushing changes to production.	Inspected the user listing and branch protection settings for the company's change management tool to determine that developers do not have access to the production environment.	No exceptions noted.
CC8.1.4	The company restricts access to the production environment to authorized personnel.	Inspected the users with access to production to determine that the company restricts access to the production environment to authorized personnel.	No exceptions noted.
CC8.1.5	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC8.1.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC8.1.6 *(cont.)*	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate the identified High, Med, and Low vulnerabilities in accordance with SLAs.	**Exceptions noted.** For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.
CC8.1.7	Vulnerability scans are performed monthly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report within the examination period to determine that vulnerability scans were performed monthly on in-scope systems.	No exceptions noted.
		Inspected the remediation plan and tickets to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	**Exceptions noted.** For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Criteria: CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and the subservice organization.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

SECTION 5: OTHER INFORMATION PROVIDED BY QUESTEK INNOVATIONS LLC

OTHER INFORMATION PROVIDED BY QUESTEK INNOVATIONS LLC

Management's Response to the Exception at CC4.1.3, CC4.2.4, CC7.1.3, CC7.2.5, and CC8.1.7

Exceptions noted:

For 24 of 24 (100%) sampled high-risk vulnerabilities identified during vulnerability scanning, vulnerabilities were not remediated in accordance with company SLA's.

Response:

CBTS reported the vulnerabilities and discussed them in detail as indicated on the attached slide from January. Also provided was a detailed report to review and provide directions.

CBTS does not make these changes without the customer's direction as there could be a risk that it will break the application.

The monthly patches address the OS vulnerabilities but, outside of that, require the customer to request the change.

1. What went wrong?
   Vulnerabilities were discussed in monthly reviews; however, QuesTek did not submit change requests needed to remediate findings. Change risks needed to be evaluated to ensure that changes would not affect the functionality of the application. Monthly patching did address OS vulnerabilities.

2. What is the risk to the organization?
   Most of the findings were related to SSL and TLS. SSL Certification issues can cause the validation process to fail, negating the security benefits of using a certificate to verify the server is trusted. TLS weak Encryption Protocol could allow an attacker to conduct man-in-the-middle attacks or decrypt communications between the affected service and the client.

3. What is being done to rectify the concern?
   Investigate the vulnerability list and determine if they are false positives or if change requests are needed to remediate vulnerabilities.

4. How will management prevent this from reoccurring?
   Management will ensure vulnerability scan results are reviewed and mark false positives or submit changes to remediate vulnerabilities.

Management's Response to the Exception at CC4.1.2, CC4.2.3, CC7.1.4, CC7.2.6, and CC8.1.6

Exceptions noted:

For three of three (100%) sampled high-risk vulnerabilities identified during penetration testing, vulnerabilities were not remediated in accordance with company SLA's.

Response:

We close tickets only after deploying changes and confirming that everything is functioning as expected, effectively eliminating the vulnerability upon deployment. The extended time a ticket remains open may be attributed to the monitoring period we maintain to detect any unforeseen failures.

Additionally, tickets may have longer timelines because we often close JIRA issues at the end of each Sprint (every two weeks). Even if the threat has been mitigated, the ticket remains in “Review” mode to allow developers ample time to re-review any changes.

To address future scenarios, we recommended including a clause in our SLAs to cover instances where a vulnerability fix may take more than three days. Several factors could contribute to this:

1. Complex vulnerabilities that require additional time to identify and resolve. This is common and affects even large tech companies like Microsoft and Google.
2. Dependent software issues where no fixes are available yet, necessitating either waiting for a fix or finding alternatives.
3. Extra testing to ensure that a fix does not introduce worse vulnerabilities.
4. Prioritization of other critical vulnerabilities. For instance, a highly exploitable vulnerability leading to a DoS scenario from an unauthenticated user may be prioritized over a privilege escalation vulnerability that is only exploitable by a logged-in user. Although privilege escalation is generally more severe, the likelihood of exploitation for the DoS scenario is higher.

To ensure better SLA adherence, we could establish a soft deadline of three days. If a resolution is not achieved within this timeframe, we may consider reporting the issue to all our clients and informing them of the situation without diminishing the urgency.