A-LIGN

TraceLink

Type 2 SOC 3

2022

tracelink

NETWORK FOR GREATER GOOD

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2021 to October 31, 2022

Table of Contents

SECTION 1

ASSERTION OF TRACELINK MANAGEMENT

ASSERTION OF TRACELINK MANAGEMENT

November 28, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within TraceLink's (the Company) Life Sciences Cloud Platform and Track & Trace Services Software as a Service System throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that TraceLink's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "TraceLink's Description of Its Life Sciences Cloud Platform and Track & Trace Services Software as a Service System throughout the period November 1, 2021 to October 31, 2022" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that TraceLink's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). TraceLink's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "TraceLink's Description of Its Life Science Cloud Platform and Track & Trace Services Software as a Service System throughout the period November 1, 2021 to October 31, 2022".

TraceLink uses Amazon Web Services, Inc. ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TraceLink, to achieve TraceLink's service commitments and system requirements based on the applicable trust services criteria. The description presents TraceLink's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TraceLink's 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 TraceLink, to achieve TraceLink's service commitments and system requirements based on the applicable trust services criteria. The description presents TraceLink's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TraceLink's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that TraceLink's service commitments and system requirements were achieved based on the applicable trust services criteria.

Daniel Nelson

Daniel Nelson
Chief Information Security Officer
TraceLink

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To TraceLink:

Scope

We have examined TraceLink's accompanying description of LSC Platform and T&TS SaaS System titled "TraceLink's Description of Its Life Sciences Cloud Platform and Track & Trace Services Software as a Service System throughout the period November 1, 2021 to October 31, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that TraceLink's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within TraceLink's Life Sciences Cloud Platform and Track & Trace Services Software as a Service System were suitably designed and operating effectively throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that TraceLink's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on TraceLink's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of TraceLink, user entities of TraceLink's LSC Platform and T&TS SaaS during some or all of the period November 1, 2021 to October 31, 2022, business partners of TraceLink subject to risks arising from interactions with the LSC Platform and T&TS SaaS, and those who have sufficient knowledge and understanding of the 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.

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

A-LIGN ASSURANCE

Tampa, Florida
November 28, 2022

SECTION 3

TRACELINK'S DESCRIPTION OF ITS LIFE SCIENCES CLOUD PLATFORM AND TRACK & TRACE SERVICES SOFTWARE AS A SERVICE SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2021 TO OCTOBER 31, 2022

OVERVIEW OF OPERATIONS

Company Background

TraceLink was founded in July 2009 with the introduction of the Life Sciences Cloud, a suite of Software as a Service (SaaS) applications natively integrated with AWS. TraceLink's software allows manufacturers, distributors, and dispensers to secure their drug supply chain and stop the trade of counterfeit medicines. TraceLink operates the world's largest track and trace network for connecting the Life Science and Healthcare supply chains with over 290,000 members. TraceLink solutions are designed to help customers meet compliance requirements, support more efficient collaboration and exchange of essential information between trade partners, and protect their supply chain against counterfeit products. Services are designed for the various roles in the end-to-end supply chain from manufacturing to dispensing.

The organization is based in Wilmington, Massachusetts with additional locations in Rochester, New York, Uxbridge, United Kingdom, Mumbai and Pune, India, Singapore, and São Paulo, Brazil.

TraceLink has achieved ISO 27001:2013 certification, inclusive of ISO 27017:2015 controls, for its information security management system (ISMS), as well as ISO 9001:2015 certification for its quality management system (QMS).

TraceLink's solutions are used by almost 1,300 companies in 51 countries to meet strategic goals in ensuring global compliance, fighting drug counterfeiting, improving on-time and in-full delivery, protecting product quality, and reducing operational cost.

Description of Services Provided

TraceLink provides multi-enterprise applications for the end-to-end life sciences supply chain. These applications are delivered as Software as a Service (SaaS) to customers and their trade partners, creating a digital supply chain network for the global pharmaceutical industry. Applications on the platform are designed to assist network entities with serialization and track & trace requirements, data exchange, partner collaboration, and compliance reporting. Solutions include:

- Serialization Applications:
    - Application suite that enables serializing finished goods with unique identity and capturing events that track product from point of manufacturer through exports, imports, customs, warehouse, channel distribution, and returns
    - The application suite supports:
        - Creation and replenishment of serial numbers
        - Integrating the production line and site management systems to furnish serial numbers and capture serial number assignment to product, and product packaging hierarchy
        - Integration of inventory, warehouse and logistic systems to manage events associated with serialized product for inbound and outbound movements, status changes, and pack/repack activities
        - Mobile application supporting the handling of serialized product for inventory and warehouse operations
    - Application suite supports integration between the customer and the contract agents of the customer, including those engaging in production, packaging, labeling, warehousing and third-party logistics providers (3PLs) and exchange of serialized event data among these supply chain partners
    - The applications can be accessed via a web user interface, application programming interface (API) integration, or business to business (B2B) gateway supporting multiple protocols and formats
- Country-Specific Compliance Applications:
    - Application suite that supports customers in meeting their country specific compliance and reporting goals

    - The application suite supports:
        - Integration with TraceLink's Serialization Applications to capture events that occur to products with traceability requirements, and capture specific data required for submitting compliance reporting transactions to government systems and/or supply chain partners
        - Maintaining a record of transactions sent and received to support record retention requirements
        - Ability to report on and retrieve transactions sent and received
    - The applications can be accessed via a web user interface
- Product Information Manager:
    - Manages sharing of product master data information and verification of unique product identifiers, in a network ecosystem that includes direct and indirect supply chain partners
    - The application can be accessed via a web user interface or application programming interface (API) integration

Principal Service Commitments and System Requirements

TraceLink designs its processes and procedures related to its LSC Platform and T&TS SaaS System to meet its objectives for its SaaS services. Those objectives are based on the service commitments that TraceLink makes to user entities, the laws and regulations that govern the provision of SaaS services, and the financial, operational, and compliance requirements that TraceLink has established for the services. The SaaS services of TraceLink are subject to the security and privacy requirements of the European Union (EU) General Data Protection Regulation (GDPR), as well as state privacy security laws and regulations in the jurisdictions in which TraceLink operates.

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

- Security concepts within the fundamental designs of the LSC Platform and T&TS SaaS System 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

TraceLink establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in TraceLink's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the LSC Platform and T&TS SaaS System.

Components of the System

Infrastructure

Primary infrastructure used to provide TraceLink's Life Science Cloud Platform and Track & Trace Services Software as a Service System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Cloud host	TraceLink leverages AWS as a cloud hosting provider. No TraceLink production services are hosted on physical hardware owned by TraceLink

Software

Primary software used to provide TraceLink's Life Science Cloud Platform and Track & Trace Services Software as a Service System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Amazon CloudSearch	AWS	Managed search service
Amazon DynamoDB (DDB)	AWS	Managed NoSQL database
Amazon ElastiCache	AWS	In-memory caching service
Amazon GuardDuty	AWS	Managed threat detection service
Amazon OpenSearch	AWS	Search services
Amazon RDS	AWS	Managed relational database
Amazon Redshift	AWS	Data warehouse
Amazon Simple Storage Service (S3)	AWS	Storage services
AWS CloudTrail	AWS	User and API activity logging
AWS Config	AWS	Configuration assessment
AWS Key Management Service (KMS)	AWS	Key storage and management
AWS Shield	AWS	DDoS protection
ClamAV	Linux	Malware detection
Cleo Harmony	Linux	Business to Business (B2B) gateway
Nagios	Linux	System monitoring
OpenText Contivo	Linux	Data transformation map development
Puppet	Linux	Configuration management and automation
SendGrid	Cloud hosted solution	Outbound e-mail services

Primary Software		
Software	**Operating System**	**Purpose**
Wazuh	Linux	Security information and event management (SIEM)

People

TraceLink has a staff of approximately 750 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as legal, accounting, finance, human resources, and IT
- *Product Management*. Responsible for defining product roadmap based on regulatory, industry, and customer requirements to ensure that products are designed to be compliant with relevant global regulations and standards. Manages the release process in accordance with the roadmap and customer needs
- *Architecture*. Responsible for technology direction and foundational architecture of products
- *Engineering*. Responsible for the engineering, testing, and ongoing maintenance of products
- *Cloud Operations*. Responsible for the continuous and secure operation and maintenance of the TraceLink solutions
- *Security*. Responsible for setting TraceLink's security strategy and overseeing its implementation across the TraceLink organization and its products/services, maintaining TraceLink's Information Security Management System, providing governance and risk management, and providing guidance to the other departments on security topics
- *Regulatory & Quality Compliance*. Responsible for providing global strategy, operational framework, and governance through the software development lifecycle, for compliance with relevant regulations and customer quality requirements
- *Customer Success.* Responsible for designing, managing, and enhancing the customer journey that clients take across their entire experience with TraceLink solutions, beginning with initial solution discovery and scoping through to solution value quantification and realization
- *Network Success.* Responsible for maintaining integrity of the TraceLink Network, verifying all entities integrated using multiple identifiers (such as DUNS, HIN, GLN, or license numbers)
- *Professional Services.* Assists customers with onboarding and integration into the network, assisting with design, configuration, and integration
- *Technical Support.* Post-implementation, responsible for providing customers with dependable, high-quality, technical support for all TraceLink applications. Technical Support attends to issues promptly to resolve or escalate according to TraceLink support policies
- *TraceLink University.* Provides training and certification to help customers understand the features, functionality, and administration of the Trace & Trace Services applications
- *Business Management, Sales, and Marketing*. These departments are focused on bringing to market strategic solutions that meet the needs of customers and the broader industry, and engaging for customers and prospects to educate them on solutions, provide value assessment

Data

The classes of customer data that reside in the TraceLink platform is made up of certain types of master data used to configure applications and data that defines the business objects that are part of and operated on by individual applications. The data that is captured includes, but is not limited to:

- Master Data (Product, Company, Trade Partners)
- Users and User Roles (for user management and user access)
- Product serial number data to support product identification and traceability
- Product event lifecycle data to support product traceability (serial number request and assignment, product packaging hierarchy, inbound and outbound movements, status changes, pack/repack activities, product verification requests, etc.)
- Compliance reports that record events that occur to products with traceability requirements

- Info Exchange monitor that captures asynchronous data exchanges with supply chain partners and with government systems
- Audit Trail of user login, and operations that create, modify or delete data

Customers interact with their data to query, create, or update data via a web user interface, application programming interface (API) integration, or asynchronous B2B messaging integration. When using the web user interface, customers may create or update certain data using file upload and retrieve data using file download.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to TraceLink's policies and procedures that define how the covered solutions should be built and managed, and services should be delivered. These are located within TraceLink's electronic Quality Management System (eQMS) and can be accessed by any TraceLink team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the hosted in-scope system. TraceLink obtains and reviews AWS' compliance artifacts (SOC 2 Type II) on an annual basis.

Logical Access - TraceLink

Upon hire, workforce members are assigned to a position in the HR management system. HR initiates the onboarding process in the HR Information System (HRIS) which triggers notification and opens an onboarding ticket for IT to provision core workforce member accounts as required. IT sends requests to other teams as needed to create accounts in other systems based on the individual's role. Access rules have been pre-defined based on the defined roles. A similar process is initiated by HR for internal transfers and status changes to ensure access remains aligned with the individual's role.

TraceLink uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, TraceLink implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All company-owned assets are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for adhering to TraceLink policies for conducting business activity and adhering to acceptable use. Only TraceLink-owned assets can connect to the internal network.

Workforce members sign on to the TraceLink network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of TraceLink's Single Sign-On (SSO) solution. Passwords must conform to defined password standards and are enforced through parameter settings in Active Directory or the apps where needed. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and lock workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Workforce members accessing the system from outside the TraceLink network are required to use the approved VPN client and multi-factor authentication (MFA). In addition, login to the SSO solution requires MFA prior to accessing any integrated applications.

On a quarterly basis, access to the LSC Platform and T&TS SaaS System and other relevant systems for TraceLink personnel is reviewed. Entitlements for each workforce member for various systems, including whether they are privileged, are shared with each department head. Recipients must recertify the access or identify any changes that are required. The access review is not considered complete until all departments have responded. Any changes required are logged in separate tickets within the ticketing system to ensure the required action is taken.

The HR system initiates notification of terminated employees to a defined audience. This notification opens a ticket to initiate and track termination of access. Access managed by IT will be taken by that team, and other actions will be distributed to other system administrators as needed. Removal of access is to be completed within twenty-four (24) hours per TraceLink policy.

Logical Access - Customers

Access to specific customer environments within the T&TS SaaS System is controlled directly by the respective TraceLink customer. During implementation, TraceLink establishes an application-level administrator account for the primary contact or designee, after which all subsequent accounts are to be created, managed, and disabled by the customer. Per the published Acceptable Use Policy, a unique login for each user is required to provide traceability and conformance with relevant regulations.

Customer employees' access the LSC Platform and T&TS SaaS System through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password (for native login functionality) or other authentication mechanism (if using the customer company's SSO solution integration) to gain access to customer cloud resources. For native login, passwords must conform to password configuration requirements. Sign-on settings are configured by the customer's Company Administrator account(s). The customer employee sets his/her own password during registration, eliminating the need for secure distribution and forced change of an initial password.

Computer Operations - Logging

TraceLink's Cloud Operations team monitors the underlying infrastructure of the LSC Platform and T&TS SaaS System 24x7x365. Over 5500 active service checks cover systems and services for both TraceLink-specific services and those provided by AWS. Alarm thresholds are set for most checks, and authorized team members adjust monitoring parameters and alarm thresholds regularly throughout the year to provide the right level of visibility and to support proactive management. Alerting systems provide notification for any events that fall out of normal range, and escalations to TraceLink's Security team occur for events that may pose a potential security concern. Alerts follow automatic escalation procedures 24x7x365.

Infrastructure system logs are immediately forwarded to centralized logging hosts as they are generated and are kept for a minimum of 7 years. Information captured in system logs includes elements such as the date and time of the event, the logging process, user account that initiated the event, and specific activities performed by the user. Event data sources include both AWS services and TraceLink-deployed components to provide comprehensive visibility and support correlation. Logical access to system logs by TraceLink personnel is restricted to those with business need and provisioned following the principle of least privilege based on job function. System logs are reviewed as needed by the Cloud Operations and Security teams and monitored by an automated log analysis system that alerts for events that requirement immediate review.

The LSC Platform and T&TS SaaS System provides customers with an audit trail within the application, available to their user(s) with the Company Administrator role. The audit trail includes the information required for conformance with US Food and Drug Administration's Code of Federal Regulations, Title 21, Chapter 1, Subchapter A, Part 11 (Final Rule) and EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice Medicinal Product for Human and Veterinary Use, Annex 11: Computerised Systems.

Computer Operations - Availability

TraceLink monitors the capacity utilization of the LSC Platform and T&TS SaaS System infrastructure to ensure that service delivery matches service level agreements. TraceLink evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Because the system relies on cloud-based infrastructure, additional capacity can be added quickly to meet demand.

Redundancy is built into the system infrastructure to help eliminate single points of failure. The LSC Platform and T&TS SaaS System runs in active-active mode across multiple Availability Zones (AZs), and multiple instances of each server persona run within each AZ. High speed, low latency network links connect AZs, permitting applications to be architected to run efficiently across multiple data centers. In the event an entire AZ is lost, all traffic is directed to the surviving AZ. In the event of a single server loss, the redundant services carry the load. Tooling is in place to scale instances as needed to meet system load and deploy to another AZ in the event of failure.

The LSC Platform and T&TS SaaS System is deployed in multiple AWS regions to provide data residency for customers within the region they select. These regions are not intended for failover in the event of a region-wide outage but instead contain the data in the customer's desired geographic region.

Network layer controls provide for isolation of the environment supporting the LSC Platform and T&TS SaaS System. Load balancers front-end each of the connection points into the system and route traffic accordingly to manage the load. Amazon Virtual Private Cloud (VPC) is used to provision a logically isolated section of the Amazon Web Services (AWS) Cloud in a virtual network that TraceLink defines and controls. TraceLink has complete control over the virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways. and security groups provide for private network and subnet configuration. Within the VPC, defined data flows are explicitly permitted through security groups, allowing only approved connections on specific ports and protocols, but are not segregated between customers due to the multi-tenant architecture of the application.

TraceLink has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. TraceLink's Cloud Operations and Security teams review available operating system patches to determine whether the patches are relevant and timeframe for application. Patches are first tested in non-customer-facing environments to identify any potential negative impact that would need to be managed prior to deployment to customer-facing environments. TraceLink authorized staff validate that all patches have been installed and if applicable that reboots have been completed.

All servers run a hardened operating system, including only the components needed to support he application. Security controls including anti-malware and file integrity monitoring are added to provide protection and detection capabilities. Configuration management software monitors and maintains conformance of each server with the defined security baseline.

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. In the event of a security breach within the LSC Platform and T&TS SaaS System, TraceLink will notify affected customer(s).

Computer Operations - Backups

A combination of replication, versioning, and backups is used to support data availability for the LSC Platform and T&TS SaaS System. Backups are focused on recovering data on an application-wide basis; partial or sub-set backup and/or restoration (e.g., per customer) is not presently supported.

Data within S3 is replicated by AWS to multiple Availability Zones (AZs) within the Region, providing redundant copies of the data on highly durable storage. TraceLink leverages versioning on S3 buckets where additional protection and recoverability is needed. Versioning allows for retaining prior iterations of a file when changed.

Database and virtual disks are backed up using AWS' snapshot API, creating a full backup with each request. These backups are stored in protected areas of S3 to prevent tampering and unauthorized deletion. Snapshots are created and retained in accordance with TraceLink's Backup and Restore procedure. Restore tests are performed for each snapshot type on a monthly basis to verify successful backups should they be needed.

Change Control

TraceLink maintains documented Systems Development Life Cycle (SDLC) and supporting infrastructure policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, risk assessment, rollback plan, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the AWS Management Console for network configuration management is restricted to authorized employees, requires MFA for authentication to customer accounts, and leverages TLS for secure connection.

Management access to the underlying infrastructure within AWS is not accessible directly via the Internet. Authorized TraceLink employees may access the LSC Platform and T&TS SaaS System through company-managed assets and after connection to the company's VPN.

Connection to the LSC Platform and T&TS SaaS System requires secure protocols, regardless of the connection channel. The web application portal and API endpoints both require HTTPS. The business-to-business (B2B) gateway supports AS2, FTP over SSH (SFTP), and HTTP POST over TLS. Use of TLS across the channels is limited to TLS 1.2. In addition, TLS encryption is used between servers in the T&TS system and to AWS services where supported. TraceLink also leverages VPC endpoints to privately connect TraceLink's VPC to other AWS services and endpoint services where available.

Data at rest is also encrypted using AES-256. TraceLink manages the encryption keys in accordance with its policies and procedures, leveraging AWS Key Management Service (KMS).

Vulnerability Management

Independent penetration testing is conducted to measure the security posture of the LSC Platform and T&TS SaaS System. The third-party vendor uses a methodology based on accepted industry standards. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. In addition, the vendor is tasked with stressing the implemented authentication and authorization model to ensure the multi-tenant architecture for logical security enforcement is sound. Penetration testing includes external network and application layer testing using both unauthenticated and authenticated access.

Dynamic application security testing (DAST) is performed by TraceLink on at least a monthly basis to identify potential vulnerabilities in the application at runtime. A third-party service provider is used to perform the scans based on TraceLink's defined configuration and schedule. Authenticated access is used to ensure access to the various modules within the LSC Platform and T&TS SaaS System.

Vulnerability scanning is performed by TraceLink on a quarterly basis in accordance with TraceLink policy. Industry standard scanning technologies and a formal methodology are used. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Scan are performed from within the AWS environment with open access through security groups and authenticated access to Track & Trace Services hosts. Retests and on-demand scans are performed on an as needed basis. Tools requiring installation in the TraceLink system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Business Continuity and Disaster Recovery

TraceLink maintains Business Continuity (BC) and Disaster Recovery (DR) plans to ensure ongoing operations in the event of a crisis or disaster. The BC plan focuses on continued operations of TraceLink's corporate functions, including those that support the LSC Platform and T&TS SaaS System environment. The DR plan focused on restoring the LSC Platform and T&TS SaaS System in the event of a disaster. Both plans are tested annually. In the event either plan was enacted, TraceLink customers would be updated throughout the recovery process.

Vendor Management

TraceLink maintains a documented vendor management procedure for managing the lifecycle of vendors. During onboarding, vendors are assigned a risk trier and assessed accordingly. Standard security and data privacy terms are documented for inclusion into vendor agreements as applicable. If a vendor is approved for use, the company will be added to the approved vendor list. Planned change in services will trigger requalification of the vendor. Additionally, requalification activities are based on frequency in the procedure.

Boundaries of the System

The scope of this report includes the Life Science Cloud Platform and Track & Trace Services Software as a Service System performed in the Wilmington, Massachusetts and Mumbai and Pune, India facilities.

This report does not include the cloud hosting services provided by Amazon Web Services, Inc. (AWS) at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security, Availability, and Confidentiality criteria were applicable to the TraceLink Life Science Cloud Platform and Track & Trace Services Software as a Service System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS provides cloud hosting services which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Recovery key materials used for disaster recovery processes are physically secured offline so that no single AWS employee can gain access to the key material.
		Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon owned data centers.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply ('UPS') units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to TraceLink.
2. User entities are responsible for notifying TraceLink of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for the security of its connection(s) to access the system, the security of such link(s), and the security of any endpoints used to access the system.
5. User entities are responsible for account and access management associated with its employees, contractors, agents, trade partners, and data in accordance with customer's policies and procedures. This includes:
    a. provisioning, modifying, and disabling its user accounts in a timely manner
    b. managing role assignments associated with its accounts to ensure
    c. ensuring appropriate authentication (via native sign-on settings provided with the system or integration with separate single sign-on solution)
    d. Configuring optional application authentication configurations.
    e. ensuring information sharing configured within the system aligns with customer's business processes and policies for information classification, handling, and protection
6. User entities are responsible for ensuring the supervision, management, and control of the use of TraceLink services by their personnel in accordance with the obligations in TraceLink's Security Annex and the Agreement and should become aware of any violation of obligations under this Security Annex and the Agreement caused by a customer user, user will immediately suspend access to the Services by such user.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize TraceLink services.
8. User entities are responsible for immediately notifying TraceLink of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.