CYBERGUARD COMPLIANCE

THREAD™

System and Organization Controls 2 (SOC 2) + HITRUST CSF Type 2

Report on controls placed in operation at THREAD
relevant to Security, Availability and Confidentiality with HITRUST CSF requirements and the suitability of the design and operating effectiveness of its controls

For the Period July 1, 2021 to June 30, 2022

TABLE OF CONTENTS

SECTION ONE

Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of THREAD
Tustin, CA

Scope

We have examined THREAD's ("Service Organization") accompanying description of its Platform System found in Section 3 titled "THREAD's Description of Its Platform System" throughout the period July 1, 2021 to June 30, 2022 (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* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that THREAD'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the implementation requirements set forth in the HITRUST CSF version 9.4 that are applicable to THREAD's Platform System required for a HITRUST CSF Security Assessment.

The information included in Section 5, "Other Information Provided by THREAD," is presented by THREAD's management to provide additional information and is not a part of THREAD's description of its Platform System made available to user entities during the period July 1, 2021 to June 30, 2022. Information about THREAD's management responses testing exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

THREAD uses a subservice organization as the cloud hosting provider services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at THREAD, to achieve THREAD's service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF requirements. The description presents THREAD's controls, the applicable trust services criteria and HITRUST CSF requirements, and the types of complementary subservice organization controls assumed in the design of THREAD'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 certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at THREAD, to achieve THREAD's service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF requirements. The description presents THREAD's controls, the applicable trust services criteria and HITRUST CSF requirements, and the complementary user entity controls assumed in the design of THREAD's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

THREAD 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 THREAD's service commitments and system requirements were achieved. In Section 2, THREAD has provided the accompanying assertion titled, "Assertion of THREAD Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. THREAD 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 HITRUST CSF requirements and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF requirements. 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 and HITRUST CSF requirements.
- 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 and HITRUST CSF requirements.
- 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 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 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 and HITRUST CSF requirements. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects:

a. the description presents THREAD's Platform System that was designed and implemented throughout the period July 1, 2021 to June 30, 2022 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that THREAD's service commitments and system requirements would be achieved based on the applicable trust services criteria and HITRUST CSF requirements, 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 THREAD's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that THREAD's service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of THREAD's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of THREAD, user entities of THREAD's Platform System during some or all of the period July 1, 2021 to June 30, 2022, business partners of THREAD subject to risks arising from interactions with the Platform 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, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria and HITRUST CSF requirements.
- 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.

CyberGuard Compliance, LLP

Las Vegas, NV

November 29, 2022

SECTION TWO

Assertion of THREAD Management

THREAD™

ASSERTION OF THREAD MANAGEMENT

November 29, 2022

Scope

We have prepared the accompanying description of THREAD's ("Service Organization" or "THREAD") Platform System titled "THREAD's Description of the Platform System" throughout the period July 1, 2021 to June 30, 2022 (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* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Platform System that may be useful when assessing the risks arising from interactions with THREAD's system, particularly information about system controls that THREAD has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the implementation requirements set forth in the HITRUST CSF version 9.4 that are applicable to THREAD's Platform System required for a HITRUST CSF Security Assessment.

THREAD uses a subservice organization as the cloud hosting provider services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at THREAD, to achieve THREAD's service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF requirements. The description presents THREAD's controls, the applicable trust services criteria and HITRUST CSF requirements, and the types of complementary subservice organization controls assumed in the design of THREAD's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

1) The description presents THREAD's Platform System that was designed and implemented throughout the period July 1, 2021 to June 30, 2022 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that THREAD's service commitments and system requirements would be achieved based on the applicable trust services criteria and HITRUST CSF requirements, 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 THREAD's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that THREAD's service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of THREAD's controls operated effectively throughout that period.

THREAD

SECTION THREE

THREAD's Description of Its Platform System

THREAD'S DESCRIPTION OF ITS PLATFORM SYSTEM

1 Overview of THREAD's Operations

This report describes the control structure of THREAD's Platform systems for the period from July 1, 2021 to June 30, 2022 for the Security, Availability and Confidentiality Trust Services Criteria.

The description is intended to provide THREAD's customers, prospective customers and auditors with information about the system controls related to criteria for the Security Trust Services Principles set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report and the suitability of the design and operating effectiveness of the controls included in the Description to provide reasonable assurance that THREAD's service commitments and system requirements would be achieved based on the trust services criteria for Security, Availability and Confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for *Security, Availability, Processing Integrity, Confidentiality, and Privacy,* commonly referred to as the Applicable Trust Services Criteria and the implementation requirements set forth in the HITRUST CSF version 9.4. This description may not provide information about THREAD's system controls that do not relate to the Applicable Trust Services Criteria.

Company Overview and Background

The THREAD Platform is a proprietary solution enabling sponsors and CROs to capture research data from sites and participants data during, in-between, and in lieu of clinic visits. THREAD is a unique and cost-effective Software-as-a-Service solution that supports customers to configure, launch, and manage a decentralized research study. A decentralized clinical trial (DCT) is comparable to a traditional clinical research study but with a virtual approach. In this approach the data is collected without the patient needing to visit a clinic for a face-to-face visit with the principal investigator or other study staff. The data is collected directly from participants via a study-specific THREAD mobile application and/or website with a variety of activities included (I.e. ePRO, surveys, eDRO, etc.), external sensors worn by the participant and/or research site team data entry via a THREAD web interface (I.e. telehealth, eDC, eSource, etc.).

THREAD's platform was built to provide the ability to conduct Decentralized Trials for all study types. Our technology solutions support remote research platforms, hybrid, and full decentralized models.

Founded in 2009, THREAD has supported life science organizations with customer, site, and patient engagement solutions via websites and mobile apps since 2012. Our journey to support decentralized studies continued with the below milestones:

- 2015 – THREAD partnered with Apple to support the development and launch of four of the first eight Research Kit studies. These were non-interventional, observational mobile health studies that enrolled 40k+ participants and received positive market response.
- 2016 – THREAD invested in developing and launching a proprietary platform to enable repeatable use, global scale, and cost efficiency in launching studies with eConsent, ePRO/eCOA, sensors, telehealth, etc.
- 2019 – THREAD was acquired by JLL Partners and Water Street in August 2019 to accelerate offering expansion.
- Today – THREAD continues rapid growth and is recognized as a leader in decentralized research including the consistent use of modern eConsent, ePRO/eCOA, sensors, surveys, and telehealth Virtual Visit approaches.

THREAD has a single, unified platform for all services. THREAD built, owns, and operates its platform and suite of solutions to provide comprehensive DCT services. This offering allows THREAD mobility for change, seamless data capture, and ease of use for all stakeholders, including sites and participants. The THREAD platform allows for scalability and cost-effective expansion of studies and programs on a global basis.

The systems in-scope for this report are the systems hosted at Amazon Web Services (AWS) and the supporting IT infrastructure and business processes, policies, and procedures.

Overview of Platform Key Features Provided

- **THREAD's Guided Configurator** is an intelligent web tool that enables project teams to design, launch, and manage their study from start to finish. This technology guided process includes configuration of all study activities, automated documentation and instant provision of the Participant App on your phone.
- **THREAD's Participant App** includes a study-branded iOS/Android app available on mobile/tablet and via BYOD (Bring Your Own Device) and/or provisioned device approaches as required per study.
- **THREAD's Participant Recruitment Website** includes a responsive website to support digital recruitment pre-screening, onboarding and registration to potentially move forward within a clinical trial.
- **THREAD's Portal** is a browser-based, responsive web portal to support Site Users (PI, Sub-I, SC, Home Health, Contact Center, Rater) with oversight of patient-generated data, conduct telehealth eVisits, capture data (i.e. eSource, eDC, eCOA/ClinRO) and more via a simple unified technology approach to reduce site burden. This web portal also supports Study Team (i.e. Trial Manager, CRA, DM, PhV, etc.) to manage study progress, clean data, access de-identified study data at any time and quality review of study operations. Externally audited and compliant with HIPAA, 21 CFR Part 11, SOC2 and other regulatory requirements. THREAD Portal provides role-based access to the platform allowing continuous

data access to raw data exports. Data conversions to SAS and data transfer agreements are optional services available.

- **THREAD's Launch Process** provides an integral framework and services to rapidly kick-off, design, configure and launch decentralized study approaches using THREAD's platform and services. This process allows a standard remote research approach to utilizing THREAD's expertise with fit-for-purpose features and content.
- **THREAD's eConsent** standardizes the use of Electronic Consent via THREAD's Platform in each available remote search model. eConsent is available for the Participant via iOS and/or Android and supports both BYOD and provisioned device approaches with inclusion of study specific informed consent language and video. Options are available for the Participant to remotely complete the process by receiving "pushed" documents from the Site while conducting an in-person, telephone, or telehealth session. THREAD eConsent supports a variety of approaches including self-directed consent (for Phase IIIb/IV studies and registries), paper upload (for regions/countries where eConsent will not be approved for use) and the ability to upload site-specific IRB/EC approved consents/agreements as they are approved for site use.
- **THREAD's eCOA/ePRO** allows the Study Team to select from a library of validated electronic patient reported outcomes with digital license availability. The team can quickly search, review, and add available ePROs to their study. If an ePRO is not currently in the library, THREAD can add, validate, and confirm with the license holder to add the ePRO for current and future studies. The THREAD Platform provides tools to configure, intelligently schedule, and assign reminders or notifications around the study's ePRO to engage patients to completion throughout their journey.
- **THREAD's eCOA/ClinRO** allows the Study Team to select from a library of validated clinician reported outcomes with digital license availability. The team can quickly search, review, and add available ClinROs to their study. If a ClinRO is not currently in the library, THREAD can add, validate, and confirm with the license holder to add the ClinRO for current and future studies. The THREAD Platform provides tools to configure, intelligently schedule, and assign reminders or notifications around the study's ClinRO to engage sites and patients to completion throughout their journey.
- **THREAD's Sensors** allow pre-connected medical devices, wearables, and health apps to be added to studies to support provisioned device and BYOD data donation models. THREAD has more than 300 pre-built integrations with medical devices, wearables, and health apps.
- **THREAD's Survey** provides the capability to build any survey with instructions, icons, and diverse question and response types. The platform's user-friendly survey builder allows for rapid creation of research surveys, the ability to build a library of surveys for future use, and intelligently schedule and assign reminders or notifications around surveys to engage patients in completion throughout their journey.

- **THREAD's Telehealth** enables participants and sites to hold telehealth sessions together to conduct virtual visits, capture data, and increase low-friction engagement. The platform provides auto-scheduling for configuring and enabling reminders for participants to schedule their eVisits based on the site's scheduled availability. The telehealth module also enables Virtual Visits to include features such as screen sharing and session recording.
- **THREAD's eDRO** allows the Study Team to pick from a library of electronic device reported outcomes and activity-based data collection tools. The team can quickly search, review, and add available eDROs to their study. The Study Team can develop their own eDRO with THREAD to integrate device connection, sensors, patient training and assessments into one activity. The THREAD Platform provides tools to configure, intelligently schedule, and assign reminders or notifications around the study's eDRO to engage patients to completion throughout their journey.
- **THREAD's Site Data Capture** enables sites to easily capture data on-site, remotely, or during telehealth eVisits. This tool enables the completion of electronic case report forms (eCRFs), electronic source forms (eSource) and other Site Team forms. The THREAD Platform provides easy-to-use dashboards, flags, sorting, and filters to enable rapid data completion and data management. The platform can be accessed on any web browser to contribute data during on-site visits, remote check-ins, phone calls, and/or during telehealth eVisits. Powerful data management tools are included to enable role-based team members to review, query, verify, approve, and sign-off to produce quality data.
- **THREAD's Analytics** provide predictive and actionable analytics that have been purpose-built for DCT and hybrid approach trials where Sponsors, CROs, and Stakeholders are able to gain deeper insights from all critical areas of the study including enrollment, compliance, data management, engagement, retention, and overall study performance. The proprietary metrics and scores allow Stakeholders to quickly see where their study currently is and where it's going, allowing them to identify any potential issues before they arise and take any necessary corrective action.

Principal Service Commitments and System Requirements

THREAD's security, availability and confidentiality commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service document published on the customer-facing website. The principal security, availability and confidentiality commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the THREAD platform and the customer data in accordance with THREAD's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:

    - Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) examinations.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of THREAD personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

THREAD establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in THREAD's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

2 Overview of the System and Applications

Scope and System Boundaries

As outlined in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria), and the implementation requirements set forth in the HITRUST CSF version9.4,* a system is designed, implemented, and operated to provide reasonable assurance that THREAD's service commitments and system requirements are achieved.

The scope of this examination is limited to the THREAD Platform. The specific criteria and related control activities included in the scope of this engagement can be found in Section 4. All criteria and controls within the security, availability and confidentiality are applicable to the THREAD Platform required for a HITRUST CSF Security Assessment.

The boundaries of the THREAD Platform include applications and infrastructure that directly support the services provided to THREAD's clients. Any applications, databases, and infrastructure that indirectly support the services provided to THREAD's clients are not included within the boundaries of the THREAD Platform.

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system

Infrastructure

The IT Infrastructure listed below is used by THREAD employees to deliver the industry leading platform to decentralize, automate and transform how clinical research is conducted. The THREAD platform makes studies more efficient, comprehensive, and inclusive to bring pharmaceutical and medical products to market.

Each THREAD employee has a company-issued laptop running Windows or macOS used for day-to-day performance of their job duties.

THREAD's platform is hosted at Amazon Web Services (AWS) data centers, using the AWS Infrastructure-as-a-Service offering. THREAD has separate AWS accounts for its development and production environments. The various services making up the runtime and provisioning systems for THREAD are deployed in multiple AWS regions across the world (specifically us-east-1, us-west-2, ca-central-1, eu-central-1, sa-east-1 with further plans to expand to other regions).

Provisioning Architecture

To provision and de-provision THREAD platform applications and optional sensor devices for customers, THREAD runs a set of systems, each with their own responsibility area. The customer interacts with the provisioning systems through a web portal DesignKit, where they, respectively, can design their study, approve configurations, configure, and approve prototypes, perform User Acceptance Testing, order translations, select sensor devices, create reports to send to IRB for approval, then submit confirmation of application release approval. This leads to Go Live through LaunchKit. When one of those interactions results in a change, a request is sent to the service which manages the workflow across the systems that need to provide resources for THREAD. Once provisioning workflow successfully completes, a record of all the instance configuration is saved and made available to the runtime environment.

AWS Services	Purpose
Amazon Elastic Compute Cloud (EC2)	Used for creating new virtual servers and maintaining existing virtual servers to host the Platform within a VPC.
AWS Cloud Watch	Used to collect and monitor log files generated by AWS.
AWS CloudTrail	Generates logs of API calls made to THREAD's AWS account.
AWS Guard Duty	AWS Intrusion Detection System. Used as thread detection service to continuously monitor for malicious or unauthorized behavior within AWS VPC and workloads. Guard Duty also detects potentially compromised virtual servers or reconnaissance by attackers.
AWS Inspector	Used to perform regular scans on THREAD cloud environment, flagging high-severity events.
Amazon Machine Images (AMIs)	Used to provide the baseline of approved software and configurations used to launch a new instance of the Platform. THREAD uses Amazon Linux for its platform.
AWS Relational Database Service (RDS)	Used for storing and uploading customer data. Customer data is logically separated from other customers' data.
AWS Secrets Manager	Used for storing secret keys that are used for encrypting and decrypting data stored within customer premises.
AWS Secure File Transfer Protocol (SFTP)	Used as a secure, pre-configured SFTP server that saves customer uploaded files to an Amazon S3 bucket.
AWS Simple Storage Service (S3)	Used for storing and uploading customer data. Customer data is logically separated from other customers' data.

AWS Services	Purpose
AWS Virtual Private Cloud (VPC)	Used for creating dedicated virtual network within AWS. It is logically isolated from other virtual networks in the AWS Cloud.
AWS Identity Access Management (IAM)	Used to manage roles and permission to AWS services and resources.
AWS Web Application Firewall (WAF)	Used to protect web application and APIs against common exploits and bots that may affect availability, compromise security, or consume excessive resources.
AWS Key Management Service (KMS)	Used to create and manage cryptographic keys and control their use across of AWS services and in our THREAD application. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, to protect our keys. AWS KMS is integrated with AWS CloudTrail to provide THREAD with logs of all key usage.
AWS Security Group (SG)	Acts as a stateful, virtual firewall for inbound and outbound traffic control to EC2 instances. Security groups deny by default, so THREAD can only specify allow rules to enable traffic filters based on protocols and port numbers.
AWS Route 53	Used as a highly available and scalable Domain Naming Service (DNS) web service, which translates names like www.example.com into numeric IP addresses like 192.0.2.1 that computers use to connect to each other. AWS Route 53 is fully compliant with IPv4 and IPv6.

NOTE: This AWS hosted infrastructure is *not* directly used by customers, it is only used by THREAD employees for providing services to customers within the THREAD platform.

THREAD Corporate Offices:

US EAST COAST	US WEST COAST
2000 Centregreen Way, SUITE 200	155 El Camino Real
Cary, NC 27513	Tustin, CA 92780

Software

THREAD leverages commercially available software to support some features of the THREAD Platform. Below is a summary of the software in use for the THREAD Platform:

Software	Purpose
Validic	Validic provides THREAD one mobile health API connection to access data from a select group of medical devices and sensors utilized by THREAD.
Veratad	THREAD leverages Veratad's Identity Verification Service to reduce fraud and compliance risk while maximizing efficiency with cloud-based global ID verification technologies.
Vonage, (formally TokBox)	Vonage is a PaaS company that provides THREAD a hosted infrastructure, APIs and tools required to deliver enterprise-grade WebRTC (Web Real-Time Communication) capabilities.
Bitrise	THREAD leverages Bitrise as a continuous integration and delivery tool for mobile applications.
Jenkins	Jenkins helps THREAD automate the non-human part of the software development process, with continuous integration and facilitating technical aspects of continuous delivery.
Rixon Technology, (formally NXT Security)	THREAD leverages Rixon Technology as an enterprise vaultless smart tokenization solution.
Veracode	Veracode detects source code vulnerabilities and helps improve code security.
DataDog	Used for infrastructure monitoring.
Atlassian JIRA & Confluence, BitBucket	Platform for tracking support tickets, projects and change management. Support tickets: All support tickets received are tracked in this system. Project Management: All projects are managed to track time, tasks and progress. Change Management: Changes to customers' infrastructure are recorded in the system, tested and approved by appropriate personnel, and recorded by asset.
Twilio SendGrid	SendGrid provides a cloud-based service that assists businesses with email delivery.
Applanga	Applanga is a modern, cloud-based translation management system.
Microsoft 365	THREAD's provider for email, calendaring, Internal communications, intranet, and cloud file storage.
1Password	1Password is a password vault. All credentials for internal and customer accounts are encrypted locally and stored in 1Password.
OpenVPN	Provides secure remote access to our AWS infrastructure.

Software	Purpose
Azure MFA	A solution providing multi-factor authentication for services that contain sensitive information.
Hexnode/Intune	Mobile Device Management solution for remote monitoring and management.
Crowdstrike Falcon	Extended detection and response tool for endpoint security.
PagerDuty	Alerting tool for monitoring of availability.

Data

Database
THREAD uses logically separate relational databases for each platform instance, meaning that customer data is separated at the database level. Multiple databases may share the same database server that is hosted by AWS. Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data lost due to hardware failure. Database logs are kept for at least 24 hours, and backups are kept for 30 days as redundancy to allow restoration within a reasonable point in time, if needed.

Attachments stored in the THREAD platform are stored in the document storage platform in AWS S3 to increase durability guarantees and segregated by tenant using a unique identifier that is stored in the platform database. The unique identifier is stored in RDS, which relates the customer to the attachment stored in AWS S3.

The THREAD platform ingests a wide range of data from customers, depending on the particular use case of each. Examples include, PHI, PII, and de-identified tokens over clinical trial datasets and other THREAD platform features.

Personally, Identifiable Information (PII) Collection and Tokenization
The THREAD Platform uses in-transit encryption during the collection process to protect PII data from point of origin and then leverages tokenization and encryption at-rest to point of destruction.

- ***In-Transit Encryption:*** Encrypted data is sent via HTTPS (TLS 1.2).
- ***At-Rest Encryption:*** Encrypted data is stored using AES 256 encryption.
- ***Data Pseudo anonymization (Tokenization)***

    - Direct Identifiers (PII) data collected from the mobile app is securely routed to RIXON via encrypted channel for pseudo anonymization (Tokenization). RIXON Tokenizes the data and sends the Token back to the mobile app then the Tokens are sent into THREAD. All Tokenization processes are calculated in-memory and data is never stored on RIXON Systems. pseudo anonymized content (Tokens) is stored in THREAD database, which is also encrypted.

- Direct Identifiers (PII) data collected from the web apps is securely routed to THREAD via an encrypted channel for pseudo anonymization (Tokenization) then routed to RIXON for tokenization and sends the Token back to THREAD. All Tokenization processes are calculated in-memory and data is never stored on RIXON Systems. pseudo anonymized content (Token) is stored in THREAD database, which is also encrypted.
- THREAD is committed to international compliance with data protection laws as part of our commitment to conducting our business ethically and to observing applicable laws, rules, and regulations. THREAD's Data Privacy Office (DPO) and our designated representative in the EU support the domestic and global presence and expansion of THREAD's platform. THREAD's DPO, with offices in the UK, the Netherlands and Washington DC, ensures that all global privacy and sovereignty laws are adhered to. THREAD's privacy program aligns closely with the key principles of GDPR and the ISO 27701 controls: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality (security), and accountability.

THREAD's internal data consists of:

- **ZenDesk**: Holds contact information for customers, list of support tickets and history of tickets which may include all manner of information about specific related issues which the customer has submitted a ticket.
- **Microsoft365**: Hold's customer information, spreadsheets and documents generated as part of supporting THREAD platform, vendor information, proposals, IT Strategy documents, and more. O365 OneDrive also holds THREAD company information such as HR files, accounting information, proposals, legal agreements, vendor information, marketing information, etc. Holds contact information for customers, list of IT assets, reports, and all manner of information about specific IT-related issues which the customer has submitted a ticket about.
- **Intune(Corporate Devices)/Hexnode (Mobile Device)**: Holds the same list of IT assets that Office365 holds but has a detailed history of the performance metrics for assets, antivirus software status, the security patching status and more.
- **1Password**: Holds all THREAD and customer related passwords. The system is encrypted and configured with multifactor authentication.

Information Classification

All THREAD information must be properly handled and controlled. THREAD classifies information as Public, Internal, Confidential, and Restricted. All client and vendor information are classified as Confidential and requires encryption at-rest and in-transit.

Data Retention

THREAD complies with the relevant data protection legislation and privacy laws in the relevant countries where THREAD operates and with customer-specific Master Service Agreements (MSAs). THREAD classifies data to ensure proper data retention and destruction

is adhered to. A Record Retention Schedule has been developed those details the retention period for each data classification type. Data that reaches the end of cycle time is purged according to the Record Retention Schedule.

People

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- *Chief Executive Officer (CEO*) – Provides leadership and visibility for strategy through communications to internal and external stakeholders.
- *Chief Information Security Officer (CISO*) – The Head of Security is responsible and accountable for designing, developing, implementing, maintaining, monitoring, and approving THERAD's system controls and other risk mitigation strategies.
- *Chief Product Officer* – The head of product development and technology, responsible and accountable for the development of the roadmap and the deployment of technology supporting the THREAD platform.
- *Board of Directors* (BOD) reviews, establishes, and support the organization with business and strategic objectives to meet the interests of stakeholders, and provides independent oversight of financial and operational performance. THREAD's board of directors meets with the executive management team monthly and ad-hoc as needed. Management presents operational and third-party assessment results to the board of directors upon completion. Board attendance is tracked, and discussion points and decisions are documented. The board operates under its' charter that defines responsibilities, including the oversight of management's system of internal control. The board includes key company owners who are independent from organizational management and support objective decision making.
- *Executive Management* - oversees, and is ultimately responsible for, all aspects of financial performance, platform development, service delivery, organizational quality and security commitments. Among other responsibilities, Executive Management ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.
- *Data Protection Officer (DPO)* – The Data Protection Officer is responsible for developing THREAD's policies around data protection, and for communicating with customers about the privacy and security practices at THREAD.
- *Human Resources* - is responsible for leading all efforts related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with THREAD's mission, vision, and values.

- *Information Technology (IT)* – The IT team is responsible for user employee technology operations, access control and THREAD company software management.

THREAD is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. THREAD endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

THREAD has a Chief Information Security Officer (CISO) who is responsible for the design and oversight of security and privacy initiatives. The CISO reports directly to the Chief Operating Officer and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the THREAD Platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CISO.

All employees are expected to adhere to THREAD's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

THREAD maintains a Quality Management System to help ensure policies and procedures:

- Are properly communicated throughout the company
- Are properly owned, managed and supported
- Clearly outline business objectives
- Show commitment to meet regulatory requirements
- Are focused on continual iteration and improvement
- Support the Policy Framework and Structure

THREAD defines policies, standards, guidelines, and procedures and each document maintained by THREAD is classified into these three categories based on the content of the document.

Item	Defines	Explanation
Policy	General Rules and Requirements	Outlines specific requirements or rules that must be met.

Item	Defines	Explanation
Standard Operating Procedures	Steps to achieve Policy Requirements, in accordance with the rules	Positioned underneath policies, it is a set of instructions on how to accomplish a task. From a compliance perspective, a SOP is also referred to as Control Activity. The goal of a SOP is to help ensure consistent outcome defined by the Policy.
Work Instruction	Common Practice, recommendations, and suggestions	Collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met but are strongly recommended.

Policy Requirements
Every policy has a Policy Owner who is responsible for managing the risk outlined in the Policy Objective. All policies are reviewed, at least annually, to help ensure they are relevant and appropriately manage risk in accordance with THREAD's risk appetite. Changes are reviewed by the Global Quality Assurance and Compliance team and approved by the corresponding Policy Owner.

Policy Review Process
In order to advance a policy, SOP or Work instruction to be available internally to all THREAD employees, each document undergoes a review process. The review process follows THREAD's internal process where feedback is sought from subject matter experts on the topic. After feedback is incorporated, the draft document is submitted to the Global Quality Assurance and Compliance team. Any announcements of changes or updates to policies, SOPs (Standard Operating Procedures) or Work Instructions are communicated immediately to all THREAD employees.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect THREAD's service commitments or system requirements.

3 Trust Services Criteria and Related Controls

THREAD's criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the criteria and related control activities are included in Section 4, they are nevertheless, an integral part of THREAD's system. The description of the service auditor's test and the results of those tests are also presented in the Section 4, adjacent to the service organization's activities. The description of the tests and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Control Environment

Management's Philosophy and Operating Style

THREAD's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel.

Integrity and Ethical Values
The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of THREAD's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of THREAD's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. Employees are provided with an Employee Handbook upon hire, which explains the corporate values and code of conduct. Employees acknowledge that they have read, understand, and agree to abide by these values and behavioral standards for the duration of their employment with THREAD.

Commitment to Competence
Management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. THREAD has focused on hiring experienced employees for the various positions required for the business.

Organizational Structure and Assignment of Authority and Responsibility
THREAD's organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored. THREAD's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. THREAD has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

The control environment at THREAD entails the involvement and ongoing management of Executive and Senior Management. The Global Quality Assurance and Compliance team engages the Executive and Senior Management in several ways:

- Policies – THREAD follows specific policies that enable the organization to exercise practices around security, availability, quality, reliability, and confidentiality.

- Tools – THREAD leverages tools designed specifically to assist in identifying, analyzing, tracking, deciding, implementing, and monitoring risks and findings. In addition, the tools allow THREAD to effectively communicate and collaborate using workflows to help ensure activities are properly tracked.
- Risk Management process – THREAD uses a Risk Management process that is modeled after ISO 31000:2018 "Risk Management - Guidelines".
- Unified Approach – As THREAD becomes involved across various best practices, legal and regulatory requirements, it becomes more essential to create control activities that are universal and not unique to specific policies, standards, and guidelines. Instead of tracking control activities specific to a policy or standard, THREAD tracks activities that are universal and meet multiple policy requirements. This approach has enabled THREAD to speak a common Quality Compliance language across the company. Along with a unified approach comes operational efficiency and a way to establish a controlled environment more effectively.

Internal Access Management

Controls have been established to help ensure key processes operate as intended. These activities are designed to address both the relevant business risks and the underlying infrastructure relevant to the THREAD platform. The control activities are integrated into the policies and procedures outlined in the previous section.

System Inventory

The IaaS infrastructure items are inventoried using AWS tools and the AWS console. THREAD hardware is limited to Windows and Mac laptops, which are tracked using system enrollment. THREAD manages, controls, and disposes of hardware and removable media in accordance with our IT Asset Management procedure.

User Authentication

Data and services are operated by third-party cloud as-a-Service providers. Two-factor authentication is enforced, VPN use is required, and AWS password requirements are enforced. AWS is configured to match the password standards set forth in THREAD's company policy.

Access to the AWS EC2 server instance is restricted using AWS IAM. Authorization to the AWS RDS database is controlled by AWS IAM. Access to the underlying database machines is not possible by design of the RDS service.

Network Security

The THREAD platform is architected using network segmentation and security groups to create logical trust boundaries between THREAD platform components. This architecture also restricts access to public-facing networks through a defined set of ports and protocols.

THREAD uses AWS Security Groups or Access Control Lists (ACLs), which act as stateful firewalls, to control inbound and outbound traffic to the THREAD platform. Access to modify

security to these security groups or other AWS configurations is restricted to specific members of the DevOps team.

THREAD also engages with a third party to perform penetration testing of the THREAD platform's software and infrastructure at least quarterly. The Global Quality Assurance and Compliance team works with the DevOps team to track remediation of any identified critical vulnerabilities.

Encryption
THREAD uses Transport Layer Security (TLS 1.2) protocols for transmitting data over unsecured networks. THREAD only offers encrypted endpoints vis Secure File Transfer Protocol (SFTP) or Hypertext Transfer Protocol Secure (HTTPS) for sensitive data.

PII is stored and processed in a tokenized format which does to provide any direct identification to its original form. Customer content is stored and processed on AWS RDS, which is logically segregated using program logic and unique customer identifiers. Customer content stored is S3 is separated using separate directories. Access is configured to prevent any unauthorized access by one customer to another customer's data.

THREAD's Information Security Policy and Data Classification, Transfer and Handling SOP requires the encryption of customer data at rest on the THREAD platform by leveraging built-in encryption functionality within AWS. Data at rest within S3 buckets is also encrypted, and access is restricted through IAM which controls access to S3.

Access to AWS resources and services are managed using policies, roles, and groups, and is based on job roles. AWS IAM is administered by the Chief Technology Officer, or designee.

Additional access to AWS, operating systems, and databases may be granted to an individual user by the DevOps/IT team through a ticketing system which is used for managing tools. The system is configured so requests are routed to the approver. Once approved, a user account is created. Quarterly access reviews are conducted for each component of the THREAD system to substantiate that access for each user is relevant and in line with job responsibilities.

THREAD uses AWS IAM to manage employee's and contractors' access to AWS resources. Access to modify security groups and other AWS configurations is restricted to members of the DevOps team. A unique user account is created for each user and permission to access AWS is assigned.

When individuals leave the company, THREAD HR team updates the terminated employee's details in the HR systems and creates a ticket aligned with the termination checklist, disabling accounts and access immediately.

Antivirus
THREAD manages antivirus on user endpoints using Crowdstrike Falcon. Endpoint devices have Falcon Sensor installed and configured to run in the background. The software automatically updates definitions and rules via their cloud platform.

Vulnerability Management
THREAD has implemented a vulnerability management policy comprising of a combination of technical controls and organizational procedures which aim to identify, respond and resolve security incidents. Vulnerability monitoring scans are performed continually. The DevOps team reviews the results of these scans and addresses any critical vulnerabilities. Critical security incidents are identified, and a process is outlined to reach a resolution.

System Monitoring
AWS CloudWatch agents, AWS CloudTrail are used to collect log files generated from THREAD's cloud resources, which are monitored with DataDog Security Information and Event Monitoring (SIEM).

THREAD employees use macOS and Windows laptops. Mobile device management (MDM) software is automatically installed on devices and is used to administer security configurations. The MDM software inventories and maintains encryption on the laptops.

Multi-factor authentication (MFA) is enforced to access production instances through administrative non-console access, remote access, and access to the AWS cloud. MFA requires the use of valid login and time-based token.

Internal Control Reviews
THREAD uses a combination of methods to verify internal control effectiveness. The Global Quality Assurance and Compliance team performs an annual internal assessment over internal controls used in the achievement of THREAD's service commitments and system requirements. Identified issues are evaluated and resolved in accordance with the Risk Management Procedure. THREAD reviews policies and procedures annually and makes changes to improve the effectiveness. The Global Quality Assurance and Compliance team works with department heads to review user account permissions at least quarterly to determine if the access is commensurate with the current job role. The Global Quality Assurance and Compliance team monitors the compliance of subservice providers annually by evaluating their SOC reports or other attestation reports.

External Control Review
As part of the annual risk assessment performed by Global Quality Assurance and Compliance team , management contracts with an outside third party to perform a HIPAA risk assessment on THREAD's policies, procedures, and the environment. The results of this assessment are reviewed, cataloged, and acted on where applicable.

Thread also does a quarterly penetration testing of its software. Third party firms are contracted with to perform the penetration testing and results are reported to THREAD teams for review and action. Items requiring remediation are tracked by the Global Quality Assurance and Compliance team.

THREAD uses third party and native AWS tools to scan its environment. The DevOps and Global Quality Assurance and Compliance teams review the results and address any critical vulnerabilities.

Physical Security
The THREAD Platform and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security of the infrastructure hosting the platform.

Physical access to THREAD office locations is restricted by badge access. Badges are approved and removed as part of the new hire/termination process. All visitors must sign in and be escorted to office locations.

Third Party Management
THREAD assesses vendors for risk to determine the level of due diligence necessary, tracks and manages vendors in accordance with THREAD's Vendor Management Procedure. THREAD assesses vendors for risk in multiple factors including regulatory, reputational, financial, security and operations risks before engaging them as a vendor. This takes the form of inspecting compliance reports or other documentation. Vendors are then added to the vendor tracking documents. The Global Quality Assurance and Compliance team monitors the compliance of key subservice providers annually by evaluating their SOC reports or other attestation reports/questionnaires.

Information and Communication

To help align THREAD business strategies and goals with quality, THREAD has implemented various methods of communication to provide assurance that employees understand their individual roles and responsibilities and that events that impact the entire company are communicated. These methods include orientation for new employees, training for current employees, and the use of messages to communicate time-sensitive information. Information and training on how to report quality, privacy and security incidents or process deviations are published internally and accessible to employees.

THREAD also provides copies of its policies and standard operating procedures and training documentation in accessible locations for employees. The Global Quality Assurance and Compliance team reviews and approves these policies and procedures on an annual basis for effectiveness and potential issues.

Internal Communications

THREAD has a centralized organization structure. Effective communication channels exist not only within departments, but between departments, as well. Leadership is committed to information-based quality decision making and has invested in the systems required to maintain the appropriate quantity and quality of information flow.

THREAD provides a mandatory security and privacy awareness training course for employees and contractors.

External Communications

THREAD contracts contain a description of the platform, its boundaries, and quality, security and privacy commitments for prospects and customers to review.

Customers can obtain customer support in many ways including emails and online via the company website. Customers can also use these established methods to submit complaints or inquiries.

Systems Development

THREAD follows Software Development and Coding Standards that address security throughout the software development life cycle. Products are developed in accordance with the Agile Software Development Framework. Software development activities are subject to THREAD's Change Management Policy and tracked using Git Repository.

Developers follow secure coding practices, and all code is reviewed prior to implementation. Coding standards ensure that code is developed securely throughout the development life cycle and security vulnerabilities are addressed. Developers are trained on secure coding techniques.

Non-production and production environments are segregated. Virtual non-production and production environments exist in separate virtual networks. The non-production environment has virtual servers that are separated from production. Non-production hosts all the lower-level environments (i.e. development, staging, and UAT). The non-production environment is used to develop code and conduct quality testing of the code. The staging environment is used for customer user acceptance and overall product evaluation. The production environment is used for live applications and data. Role-based access to all three environments is controlled using VPN with MFA. Access to the production environment is limited to approved users based on roles and responsibilities for administering the environment. Access to the production environment can be obtained temporarily for troubleshooting by following the defined production access escalation process.

Change Management

THREAD has documented Software Development Life Cycle (SDLC) and change management procedures, which govern the process and protocols for making code and configuration changes to the THREAD platform. This procedure requires and configuration changes, Access Control Lists (ACLs) changes, and other infrastructure-related changes to be documented and authorized in accordance with the SDLC.

THREAD follows an agile model for software development including continuous integration of code. Code review, unit tests, functional tests, and security tests (including static code analysis) are required, and no change is merged to production in the BitBucket repository until tests have passed. The code repository used to manage the SDLC is configured to enforce review and testing prior to changes being deployed into production. Testing is conducted following manual processes.

Sprints are performed on a regular basis, and product and technical specifications that establish requirements for product releases are documented and retained. Major new system developments follow THREAD's SDLC.

Application and infrastructure related changes follow an established change management process in the THREAD environment. When requests are entered for a change, the request is assigned to a severity level based on the nature and impact of the change:

- Standard – A repeatable change, such as maintenance work
- Normal – A regular, non-standard change that is not an emergency
- Emergency/Hotfix – A risk that must be remediated immediately

Standard Amazon AMIs are used for creating new virtual server instances. AWS Systems Manager is used to identify any missing security parches and automatically apply them if relevant for the THREAD environment.

Data Security

TLS, PKI, and currently supported AES encryption standards are used to protect data used, transmitted, and stored. Trusted keys and/or certificates are used for security incident reporting, TLS connections, and interconnections between applications and databases.

Electronic hardware previously used to process or store data must be physically destroyed or wiped using a method that overwrites the data.

A Clean Desk Policy is in place to ensure that sensitive/confidential information is secured when not in use. All sensitive/confidential information must be removed from an employee's

user workspace and locked away when the items are not in use, or an employee leaves his/her workstation.

Incident Management

THREAD maintains incident response and escalation procedures in place to efficiently and effectively manage unexpected incidents that can potentially impact the business. The incident response process defines activities to identify and mitigate security breaches and manage communications with THREAD personnel, as well as customers, legal counsel, or law enforcement, as necessary. Actions taken to contain and resolve incidents are documented in a ticketing system. When a security event is detected or reported, IT examines and attempts to resolve the issue, and escalates the incident if necessary.

The Incident Response Policy includes procedures for incident preparation, detection and analysis, notification, containment, eradication and recovery, and post incident activity. Security incidents are logged in THREAD's Quality Management System and appropriately followed through the incident response lifecycle. The Incident Response Plan is tested on an annual basis or more frequently as needed. THREAD defines a security incident as any irregular or suspicious event that might affect the security, confidentiality, integrity, or availability of systems and data. For security incidents, a root cause analysis is conducted and documented by the Global Quality Assurance and Compliance team. Based on the root cause analysis, corrective and preventive actions are taken and documented for all critical incidents.

Post-mortem activities include holding a "lessons learned" meeting with all involved parties after a major incident, and optionally after lesser incidents as deemed necessary. This meeting seeks to review what occurred, what was done to intervene, and how well intervention worked. The Incident Response Policy is updated as needed as after each lesson learned session.

Backup and Recovery

THREAD has implemented a comprehensive, multi-layered system for backup of its own data and the data it manages on behalf of customers within the AWS infrastructure. For AWS hosted infrastructure, THREAD employs Elastic Block Store (EBS) snapshots which are captured at least daily, RDS snapshot backups for SQL databases, backups of the source code of the configuration management and infrastructure orchestration system which are automatically sent to encrypted Simple Storage Service (S3) which is a highly durable object storage service with 11 9's of durability (99.9999999999%). The disaster recovery strategy is predicated on a high availability scheme that has been established and configured for the THREAD platform to reside at AWS in multiple availability zones. As part of the AWS S3 service offering, all data stored within AWS S3 includes cross region replication which automatically replicates data across different AWS regions. In the event one zone is unavailable, complete copies of production systems are available in other AWS zones.

The Disaster Recovery and Business Continuity Policy outlines the disaster recovery and business continuity strategy in place for THREAD operations and production systems and data located at AWS.

The Disaster Recovery and Business Continuity Plan is tested on an annual basis. The test is conducted within a realistic environment that includes simulating conditions that are applicable in an actual emergency. Results of this test are reviewed, and updates are made to the plan/policy, as necessary.

Risk Assessment

A Quality Risk Management process is in place to manage risks associated with THREAD strategy and business objectives.

THREAD utilizes a process which:

- Establishes the context, both internal and external, as it is related to the company business objectives
- Assesses the risks
- Facilitates development of strategies for risk treatment
- Communicates the outcome
- Monitors the execution of the risk strategies, as well as changes to the environment

The Quality Risk Management process is modeled after ISO 31000:2018 "Risk Management - Guidelines".

When performing a risk assessment under the Quality Risk Management framework, risk is considered holistically on its impact to the company, not just to individual functions/department/product that is directly impacted by the risk. While there may be specifics for a particular function, product, or service, they are always considered in terms of affecting the entire company. This principle is followed, not only in the analysis but also in the evaluation of the risks.

To perform activities supporting the Quality Risk Management process, various sources of information are crucial to encompass all areas of the company. Information sources include but are not limited to:

- High level business goals and objectives, and the strategies in place to achieve those.
- Large projects or initiatives that could have a significant impact on THREAD’s risk profile.
- Throughout the period, THREAD performs several periodic and ad-hoc assessments, which includes key product stakeholders.

- THREAD utilizes a common Incident Management Process including Postmortem Review. The goal of Postmortem Review is to not only establish the root cause but also to create actions aimed at reducing risk of repeated incident.
- Organizational policies have been put in place to achieve the company's strategic goals and objectives.
- As part of the structured Quality Risk Management process, interviews with major stakeholders and subject matter experts are engaged as needed.
- THREAD may consult industry publications, regulations, legal authorities, analyses, incidents, etc., as necessary.
- Internal and external context of the Quality Risk Management process includes but is not limited to understanding:

    - Competitive environment – who are THREAD's major competitors, what threat level they represent, what are the trends in THREAD's history
    - Legal/Regulatory environment – what are THREAD's obligations within our operating jurisdictions, what are the industry standards THREAD needs to abide by
    - Financial environment – status as well as trends in the financial and currency markets that could affect us, perceptions, and values of external stakeholders
    - Technological environment – what are the trends in technology and software development
    - Business environment – markets THREAD is currently in or has plans to enter, what is the perception of THREAD and its platform services, what are the current development trends in THREAD's ecosystem, major vendor, and customers
    - Human environment – what are the social and cultural trends that could affect us, what are the status and trends of the talent pools where THREAD currently has or plans to establish presence
    - Natural environment – considerations related to natural disasters, pandemic planning, and office locations

The goal of establishing the external context is to identify potential key drivers and trends that could impact the company.

- Organizational structure, governance, roles, and accountabilities
- Short and long-term strategies, objectives, initiatives, programs, and projects
- Resources and capabilities (people, skillsets, tech, facilities, capital)
- Operations (services, systems, and processes)
- Company culture and values
- Information, information flow and decision-making
- Policies, SOPS and Work Instructions
- Vendor agreements and dependencies

The goal of establishing internal context is to identify potential key internal misalignments between strategy, objectives, capabilities, and execution.

The Quality Risk and Compliance function plays a crucial role in THREAD's ability to integrate Quality Risk Management throughout the company. The risk assessment process entails the following:

- Identification of risks
- Analysis of risks identified
- Evaluation of the risks
- Treatment of the risks

Throughout all stages of the Quality Risk Management process, the Quality Risk and Compliance team communicates with the relevant stakeholders and consults with appropriate subject matter resources.

All risks and associated treatment plans are recorded. Quality Risk and Compliance team monitors progress and provides oversight of the plan's execution. Progress review is part of the operational business function meetings.

THREAD's Quality Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred. The Quality Risk and Compliance team meets on a weekly basis with strategic planning sessions to discuss:

- Risk and Compliance strategic direction
- Changes happening within the company that affect Quality Risk and Compliance efforts and initiatives
- Changes happening outside of THREAD that affect Quality Risk and Compliance efforts and initiatives
- The Quality Risk and Compliance pipeline of how THREAD approaches quality risk and compliance with internal customers
- Changes to existing and ingesting of new compliance standards and regulations

Internal Audit

The internal audit team conducts internal audits around Service Organization Control (SOC 2), HIPAA, International Organization for Standardization (ISO), and operational audits, and results are communicated, and corrective actions monitored. The internal audit team engages with third-party qualified auditors to perform compliance audits against standards on an annual basis. The results of the audits are captured as findings and remediation is tracked with regular reports to management and the internal audit team.

Significant System and Control Changes

The IT environment has been stable throughout the period and there have been no significant changes to the system. The description does not omit or distort information relevant to THREADs system. THREAD acknowledges the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

4 Monitoring

The CPO and CISO monitor the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to determine if objectives are achieved, identify any new risks that develop, and implement appropriate measures to address those risks. THREAD adopts a proactive approach to the monitoring of application and network security to ensure that any issues or risks are identified and addressed as soon as possible.

Separate Evaluations
Evaluations of internal control vary in scope and frequency, depending on the significance of risks being managed and the importance of the controls in reducing risks. Evaluations often take the form of informal self-assessments, where personnel responsible for a particular function determine the effectiveness of controls for their activities.

Security reviews, vulnerability assessments, and penetration tests are performed or coordinated by Information Security personnel periodically to identify threats and assess their potential impacts to system security. Any detected security vulnerabilities are investigated and documented through remediation.

Subservice Organization

THREAD utilizes a subservice organization to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at Amazon Web Services are not included in the scope of this report. The affected criteria are included below along with the expected controls of Amazon Web Services (AWS).

Amazon Web Services (AWS)
THREAD uses Amazon Web Services (AWS) as the cloud hosting provider for the THREAD application. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at AWS, alone or in combination with controls at THREAD to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Control
6.1,6.2, 6.3, 6.6	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.
6.4, 6.5	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.
A 1.1	AWS is responsible for ensuring capacity demand controls are in place to meet availability commitments and requirements.
A 1.2	AWS is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.

THREAD Management receives and reviews the AWS SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 1 or SOC 2 report are analyzed for relevance to and effect on THREAD's organization and its users. As part of the review:

- Management confirmed that the SOCs listed above were covered within the scope of AWS's SOC 2 Type 2 report and were found to be operating effectively during the audit period.
- Management determined that the Complementary User Entity Controls (CUECs) identified in AWS's SOC 2 Type 2 report are included in the scope of this SOC 2 report as controls that were tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by AWS to ensure that operations and controls expected to be implemented are functioning effectively.

5 Complementary User Entity Controls and Responsibilities

The control activities performed by THREAD were designed with the understanding that certain user organization controls would be implemented by each customer. Each customer's internal control structure must be evaluated in conjunction with THREAD's controls, policies and procedures described in this report. The Complementary User Entity Controls (CUECs) below are the minimum controls that customers must have in operation to complement the controls of the THREAD system and should not be regarded as a comprehensive list of all controls that should be employed by customers.

THREAD designed its controls with the assumption that certain controls will be the responsibility of its customers. The following is a representative list of controls that are recommended to be in operation at user entities to complement the controls of THREAD's

platform. This is not a comprehensive list of all controls that should be employed by THREAD's customers.

Change Management

- Customers are responsible for validating the accuracy and completeness of data contained in their THREAD platform (portal/study)

Logical Access

- Customers are responsible for creating a username and password for access
- Customers are responsible for inviting team members and managing team members' access rights to THREAD's platform (portal/study)
- Customers are responsible for establishing their own usage and access policies to their THREAD accounts
- Customers are responsible for identifying approved points of contacts to coordinate with THREAD
- Customers are responsible for the appropriate set-up following logical security settings: IP whitelisting, Authorization setup, MFA, if applicable
- Customers are responsible for requesting and approving THREAD's customer support access to their (portal/study)
- Customers are responsible for performing periodic review of access and configurations for appropriateness (portal/study)

Incident Management

- Customers are responsible for alerting THREAD of incidents (related to Quality, Security, Availability and Confidentiality) when they become aware of them

Anti-virus and Data Protection

- Customers are responsible for running virus scans on all media attachments and its contents

Add-ons/Integrations

- Customers are responsible for managing the actions that an add-on or integration will have on their THREAD (portal/study)

6 Non-Applicable Trust Services Criteria

All criteria within the security, availability and confidentiality categories are applicable to the THREAD Platform system.

SECTION FOUR

Trust Services Criteria, Related Controls, and Tests of Controls

TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

1 Scope, Purpose, and Objectives of the Report

The scope of CyberGuard Compliance, LLP's procedures was based on the AICPA and trust services criteria relevant to security, availability, and confidentiality as they relate to the system and the design and operating effectiveness of the applicable controls and the implementation requirements set forth in the HITRUST CSF version 9.4 that are applicable to THREAD's Platform System required for a HITRUST CSF Security Assessment. This report, when combined with an understanding and assessment of the internal controls at user organizations, is intended to meet the needs of a broad range of users that need information and assurance about the controls at THREAD that affect the security, availability, and confidentiality criteria of the system. Stakeholders who may need this report are: management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls.

APPLICABLE TRUST SERVICES CRITERIA

The applicable trust services criteria and related controls presented in Section 4, "Trust Services Criteria, Related Controls, and Tests of Controls," are an integral part of THREAD's system description throughout the period July 1, 2021 to June 30, 2022.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

i. information during its collection or creation, use processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of THREAD service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

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

Confidentiality
The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements. Confidentiality addresses THREAD's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from THREAD's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Our examination was restricted to the Trust Services Criteria specified above and related control procedures specified in Section 4. It is the stakeholders' responsibility to evaluate this information in relation to the controls in place at each user organization.

2 Tests of Operating Effectiveness

Our tests of the operating effectiveness of controls were designed to cover a representative number of transactions for the period July 1, 2021 to June 30, 2022 for each of the trust services criteria listed in Section 4, which are designed to achieve the specific criteria. Tests of design and operating effectiveness were based off the criteria and illustrative controls within each trust services criteria.

Type of Test	General Description of Test
Inquiry or Corroborative Inquiry	Inquired of appropriate personnel to ascertain compliance with controls.
Observation	Observed application of specific controls.
Inspection	Obtained and examined documents and reports indicating performance of the controls.
Re-Performance	Re-performed application of the controls.

In addition, as required by paragraph .35 of ATC Section 205, Assertion-Based Examination Engagements (AICPA, *Professional Standards*), and paragraph .30 of ATC Section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

3 Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), CGC performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1) Inspect the source of the IPE,
2) Inspect the query, script, or parameters used to generate the IPE,
3) Tie data between the IPE and the source, and/or
4) Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above, procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), CGC inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria for Security

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
1.1.1		The Company has a formalized Code of Conduct, which demonstrates the importance of integrity and ethical values. The Code of Conduct is included in the Employee Handbook, which is available to employees via the intranet.	**Inspection:** Obtained and reviewed the Code of Conduct contained within the Employee Handbook, and a screenshot of the handbook on the company intranet. Verified the Company has a formalized Code of Conduct, which demonstrates the importance of integrity and ethical values. The Code of Conduct is included in the Employee Handbook, which is available to employees via the intranet.	No exceptions noted.
1.1.2	05.a 02.d	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Inspection:** Obtained and reviewed the policy acceptance report for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
1.1.3		Employees receive a formal performance review annually.	**Inspection:** Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received an annual performance review.	No exceptions noted.

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1.4	02.f 06.e	The Company has established disciplinary policies for employees who violate security policies/acceptable use policies/company policies.	**Inspection:** Obtained and reviewed the Sanctions Policy. Verified the Company had established disciplinary policies for employees who violated security policies/acceptable use policies/company policies.	No exceptions noted.
1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
1.2.1		The board of directors operates independently and provides oversight on the system of internal control.	**Inspection:** Obtained and reviewed the board of directors charter. Verified the board of directors operated independently and provided oversight on the system of internal control.	No exceptions noted.
1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
1.3.1	02.a	Reporting relationships and organizational structures are reviewed annually by senior management as part of organizational planning and are adjusted as needed based on changing Company commitments and requirements.	**Inspection:** Obtained and reviewed the Organizational Chart and review. Verified reporting relationships and organizational structures were reviewed annually by senior management as part of organizational planning, and were adjusted as needed based on changing Company commitments and requirements.	No exceptions noted.

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.3.2	07.c	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Inspection:** Obtained and reviewed the job descriptions for the sampled employees hired during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.
1.3.3	00.a 07.c	The Company maintains an Information Security Management Program that is defined in terms of the characteristics of the business, and is established and managed including monitoring, maintenance, and improvement. The Company establishes implements, maintains and continually improves the Information Security Management System, in accordance with the requirements of the standards.	**Inspection:** Obtained and reviewed the Information Security Policy and the Employee Training Plan. Verified the Company maintained an Information Security Management Program that was defined in terms of the characteristics of the business, and was established and managed including monitoring, maintenance, and improvement. Verified the Company established, implemented, maintained and continually improves the Information Security Management System, in accordance with the requirements of the standards.	No exceptions noted.
1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
1.4.1		Employees receive a formal performance review annually.	**Inspection:** Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received an annual performance review.	No exceptions noted.

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.4.2	02.b 05.k	Personnel must pass a criminal background check before they may be hired by the Company.	**Inspection:** Obtained and reviewed the background check reports for the sampled employees hired during the audit period. Verified Personnel passed a criminal background check before they were hired by the Company.	No exceptions noted.
1.4.3		The experience and training of candidates for employment are verified before they assume the responsibilities of their position.	**Inspection:** Obtained and reviewed the interview notes and scoring for the sampled employees hired during the audit period. Verified candidate experience and training for employment was verified before they assumed the responsibilities of their position.	No exceptions noted.
1.4.4	07.c	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Inspection:** Obtained and reviewed the job descriptions for the sampled employees hired during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.
1.4.5	02.e	Personnel are required to attend annual security awareness training.	**Inspection:** Obtained and reviewed the security awareness training report for the sampled current employees during the audit period. Verified personnel attended annual security awareness training.	No exceptions noted.

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
1.5.1	05.a 02.d	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies and a screenshot of the policies on the Company's intranet. Verified documented internal control policies were updated annually and are available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
1.5.2	04.a 04.b	Information Security Policy documents: • Establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable • Are supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. • Are reviewed annually or if significant changes occur to ensure its continuing adequacy and effectiveness.	**Inspection:** Obtained and reviewed the Information Security Policy. Verified the Information Security Policy documents: • Established the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable • Were supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. • Were reviewed annually or if significant changes occur to ensure its continuing adequacy and effectiveness.	No exceptions noted.

1.0 CONTROL ENVIRONMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.5.3		The Chief Information Security Officer is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the Chief Information Security Officer's job description. Verified the Chief Information Security Officer was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.
1.5.4		The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.
1.5.5	02.e	Personnel are required to attend annual security awareness training.	**Inspection:** Obtained and reviewed the security awareness training report for the sampled current employees during the audit period. Verified personnel attended annual security awareness training.	No exceptions noted.
1.5.6		Employees receive a formal performance review annually.	**Inspection:** Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received an annual performance review.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
2.1.1		The Company reviews its data flow diagram annually.	**Inspection:** Obtained and reviewed the data flow diagram and management's review. Verified the Company's data flow diagram was reviewed annually.	No exceptions noted.
2.1.2		The Data Classification Policy details roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	**Inspection:** Obtained and reviewed the Data Classification and Handling Policy. Verified the Data Classification Policy detailed roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	No exceptions noted.
2.1.3	07.a	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and management's review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
2.2.1		The Chief Information Security Officer is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the Chief Information Security Officer's job description. Verified the Chief Information Security Officer was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.
2.2.2	05.a 02.d	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies and a screenshot of the policies on the Company's intranet. Verified documented internal control policies were updated annually and are available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
2.2.3		The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.2.4	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
2.2.5		Changes made to systems are communicated to appropriate users.	**Inspection:** Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified system changes were communicated to appropriate users.	No exceptions noted.
2.2.6	06.d	A data protection and privacy policy is documented and implemented. This policy is communicated to all individuals involved in the processing of covered information.	**Inspection:** Obtained and reviewed the Privacy Policy and a screenshot of the policy on the Company's website. Verified a data protection and privacy policy was documented and implemented. This policy was communicated to all individuals involved in the processing of covered information.	No exceptions noted.
2.2.7	06.d	A data protection officer or privacy officer, who is responsible for the Company's privacy protection program, reports directly to the COO and serves as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints.	**Inspection:** Obtained and reviewed the Data Privacy Officer's job description. Verified a data privacy officer, who was responsible for the Company's privacy protection program, reports directly to the COO and serves as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
2.3.1	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.
2.3.2		Relevant updates and changes to agreements, policies, and privacy policies are made available to external parties.	**Inspection:** Obtained and reviewed the privacy policy on the Company's website. Verified Relevant updates and changes to agreements, policies, and privacy policies were made available to external parties.	No exceptions noted.
2.3.3	05.i 09.s	Company policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it is encrypted.	**Inspection:** Obtained and reviewed the Data Classification and Transfer Policy. Verified company policies prohibited the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it was encrypted.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.3.4	05.k 09.e 09.n	Applicable Company security, availability and confidentiality commitments regarding the system are included in the Master Service Agreement and/or customer-specific Service Level Agreements.	**Inspection:** Obtained and reviewed the Master Service Agreements (MSA) for the sampled customers obtained during the audit period. Verified the MSA's included applicable Company security, availability and confidentiality commitments regarding the system.	No exceptions noted.
2.3.5	05.i 05.j	Customer responsibilities, which may include the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints, are described in the Master Service Agreements, Statements of Work, or Service Level Agreements.	**Inspection:** Obtained and reviewed the Master Service Agreements (MSA) for the sampled customers obtained during the audit period. Verified the MSA's described customer responsibilities including the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
2.3.6		The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
3.1.1	03.a	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Management Policy. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
3.1.2	03.b 03.c 12.b	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the risk assessment. Verified it evaluated internal and external threats with the likelihood, impact, significance, and mitigation efforts identified.	No exceptions noted.
3.1.3		Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the Risk Management Policy and the risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.1.4	03.d	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes for the sampled quarters during the audit period. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
3.2.1	12.c 12.d	Business Continuity and Disaster Recovery Plans are in place to identify the criticality of information assets.	**Inspection:** Obtained and reviewed the Disaster Recovery Plan. Verified Business Continuity and Disaster Recovery Plans were in place and identified the criticality of information assets.	No exceptions noted.
3.2.2		Internal and external vulnerability scans are performed continually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scan report. Verified internal and external vulnerability scans were performed continually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
3.2.3		Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2.4	05.i	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy and vendor review. Verified the Company maintained a formal process that assessed the potential threats and vulnerabilities from vendors providing goods and services. Additionally, the Company assessed, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	No exceptions noted.
3.2.5	03.b 03.c 12.b	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the risk assessment. Verified it evaluated internal and external threats with the likelihood, impact, significance, and mitigation efforts identified.	No exceptions noted.
3.2.6	03.d	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes for the sampled quarters during the audit period. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2.7		Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the Risk Management Policy and the risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.2.8		Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Obtained and reviewed the risk assessment. Verified unremediated risks were assessed by Management and remediation activities were documented and resolved in a timely manner.	No exceptions noted.
3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
3.3.1		An enterprise risk assessment is performed annually and considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	**Inspection:** Obtained and reviewed the risk assessment. Verified it was performed annually and considered loss of assets and corruption resulting from the various ways that misconduct can occur.	No exceptions noted.
3.3.2		The enterprise risk assessment considers how management and other personnel might engage in or justify inappropriate actions.	**Inspection:** Obtained and reviewed the risk assessment. Verified it considered how management and other personnel might engage in or justify inappropriate actions.	No exceptions noted.
3.3.3		The enterprise risk assessment considers threats and vulnerabilities that arise specifically from the use of IT and access to information.	**Inspection:** Obtained and reviewed the risk assessment. Verified it considered threats and vulnerabilities that arise from the use of IT and access to information.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
3.4.1		The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.
3.4.2		The risk identification process considers changes in the Company's systems and in the technology environment.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes in the systems and in the technology environment.	No exceptions noted.
3.4.3		The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes in vendor and business partner relationships.	No exceptions noted.
3.4.4	03.b 03.c 12.b	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the risk assessment. Verified it evaluated internal and external threats with the likelihood, impact, significance, and mitigation efforts identified.	No exceptions noted.
3.4.5	03.d	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes for the sampled quarters during the audit period. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.

3.0 RISK ASSESSMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.4.6		Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Obtained and reviewed the Risk Management Policy and the risk assessment. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.

4.0 MONITORING ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
4.1.1		Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
4.1.2		Internal and external vulnerability scans are performed continually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scan report. Verified internal and external vulnerability scans were performed continually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
4.1.3	06.h	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the Configuration Standards and the configuration compliance review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, annually.	No exceptions noted.

4.0 MONITORING ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.1.4	05.h	Management conducts an independent review of the organization's information security management program annually, at minimum, to ensure the continuing suitability, adequacy, and effectiveness of the Company's approach to managing information security and privacy. Corrective actions are taken as necessary.	**Inspection:** Obtained and reviewed the Information Security Management Policy. Verified management conducted an independent review of the organization's information security management program annually, at minimum, to ensure the continuing suitability, adequacy, and effectiveness of the Company's approach to managing information security and privacy. Corrective actions were taken as necessary.	No exceptions noted.
4.1.5	06.g	Security, privacy and/or audit individuals conduct reviews of systems' compliance with security and privacy policies, standards, and requirements.	**Inspection:** Obtained and reviewed the system compliance review. Verified reviews of systems are done in compliance with security and privacy policies, standards, and requirements.	No exceptions noted.
4.1.6	09.aa	Information systems create a secure audit record each time a user accesses, creates, updates, or archives covered information via the system. Logs are retained according to Company policy.	**Inspection:** Obtained and reviewed the audit log configuration. Verified a secure audit log was created each time a user accessed, created, updated, or archived covered information via the system and were retained according to Company policy.	No exceptions noted.
4.1.7	09.ab	Monitoring and detection processes are periodically tested, and the Company remediates deficiencies and updates processes as necessary.	**Inspection:** Obtained and reviewed the monitoring and detection processes. Verified they were in place and tested, with remediation and updates completed as necessary.	No exceptions noted.

4.0 MONITORING ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.1.8	09.ad	Proper logging is enabled in order to audit administrator activities, and these logs are reviewed on a regular basis.	**Inspection:** Obtained and reviewed the administrator logging and alert configuration. Verified logging was enabled to audit administrator activities, and these logs were reviewed on a regular basis.	No exceptions noted.
4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
4.2.1		The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.
4.2.2		Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Obtained and reviewed the risk assessment. Verified unremediated risks were assessed by Management and remediation activities were documented and resolved in a timely manner.	No exceptions noted.

5.0 CONTROL ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
5.1.1		The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.
5.1.2		The risk identification process considers changes in the Company's systems and in the technology environment.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes in the systems and in the technology environment.	No exceptions noted.
5.1.3		The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Obtained and reviewed the risk assessment. Verified it included changes in vendor and business partner relationships.	No exceptions noted.
5.1.4		Control activities are mapped to the Company's risk assessment to ensure that risk responses address and mitigate risks.	**Inspection:** Obtained and reviewed the risk assessment. Verified control activities were mapped to the Risk Assessment to ensure the risk responses address and mitigate risks.	No exceptions noted.
5.1.5	03.b 03.c 12.b	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Obtained and reviewed the risk assessment. Verified it evaluated internal and external threats with the likelihood, impact, significance, and mitigation efforts identified.	No exceptions noted.

5.0 CONTROL ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1.6	03.d	The Risk Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the Risk Committee meeting minutes for the sampled quarters during the audit period. Verified the Risk Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	No exceptions noted.
5.2	COSO Principle 11: The entity selects and develops general control activities over technology to support the achievement of objectives.			
5.2.1		Documented configuration standards are reviewed annually, at minimum, and when significant changes are made or integral system components are added.	**Inspection:** Obtained and reviewed the Configuration Standards. Verified configuration standards were documented, reviewed annually at minimum, and when significant changes were made or integral system components were added.	No exceptions noted.
5.2.2	01.b	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Management Policies. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

5.0 CONTROL ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.2.3	06.c	The Company maintains recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	**Inspection:** Obtained and reviewed the Backup and Recovery Policy. Verified the Company maintained recovery strategies, such as data replication, offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	No exceptions noted.
5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
5.3.1	05.a 02.d	Documented internal control policies are updated annually and are available to appropriate employees and contractors. These policies include an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies and a screenshot of the policies on the Company's intranet. Verified documented internal control policies were updated annually and are available to appropriate employees and contractors. These policies included an Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
5.3.2	01.b	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Management Policies. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

5.0 CONTROL ACTIVITIES				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.3.3	11.c	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Security Incident Response Policy. Verified Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
5.3.4	05.a 02.d	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Inspection:** Obtained and reviewed the policy acceptance report for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
5.3.5		The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1	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.			
6.1.1	07.a	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and management's review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.1.2	01.j 01.y	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.1.3	01.q 09.c	Users are required to authenticate via unique user account ID and password before being granted access to the in-scope network.	**Inspection:** Obtained and reviewed the user listing and reconciled with the employee listing. Verified users were required to authenticate via unique user account ID and password before being granted access to the in-scope network.	No exceptions noted.
6.1.4	01.c 01.n	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the administrator user listing and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.5	01.q 01.p 01.n	Administrators must authenticate via unique ID and password before being granted access to the in-scope network.	**Inspection:** Obtained and reviewed the administrator listing. Verified administrators authenticated via unique ID and password before being granted access to the in-scope network.	No exceptions noted.
6.1.6	01.v 06.e 01.b	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inspection:** Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified new user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process.	No exceptions noted.
6.1.7		Modified user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inquiry:** Inquired of management regarding user access modifications during the audit period and determined a population of access modifications during the audit period could not be provided. Therefore, we were unable to verify that modified user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process.	***Exception noted. See Section 5 for further details.***
6.1.8	10.f 06.f	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Data Classification, Transfer, and Handling Policy. Verified policies and procedures on the use of cryptographic controls for protection of information were documented.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.9	01.d	The production network domain is configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	**Inspection:** Obtained and reviewed the production password configuration. Verified the production network domain enforced the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	No exceptions noted.
6.1.10	01.t	The system automatically logs out users after a defined period of inactivity.	**Inspection:** Obtained and reviewed the system timeout configuration. Verified the system automatically logged out users after a defined period of inactivity.	No exceptions noted.
6.1.11	01.w	The sensitivity of application systems has been identified and documented by the application owners.	**Inspection:** Obtained and reviewed the network diagram. Verified sensitive systems have a dedicated and isolated computing environment.	No exceptions noted.
6.1.12	01.w 01.m	Separate environments are used for development, testing, and production. Developers do not have the ability to migrate changes to production.	**Inspection:** Obtained and reviewed the network diagrams, developer listings and reconciled with the production access listing. Verified separate environments were used for development, testing, and production. Developers did not have the ability to migrate changes to production.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.13		Confidential data files are encrypted prior to backup.	**Inspection:** Obtained and reviewed the backup configuration. Verified confidential data files are encrypted prior to backup.	No exceptions noted.
6.1.14	01.h	A clean desk/clear screen policy is defined for paper, removable storage media, and workstations/laptops.	**Inspection:** Obtained and reviewed the Clean Desk and Clear Screen Policy. Verified a clean desk and clear screen policy was defined for paper, removable storage media, and workstations/laptops.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.				
6.2	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.			
6.2.1	01.b	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Management Policies. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.2.2	01.v 06.e 01.b	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inspection:** Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified new user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process.	No exceptions noted.
6.2.3	02.i	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Inspection:** Obtained and reviewed the termination tickets for sampled employees terminated during the audit period. Verified Human Resources was responsible for notifying IT of terminated employees and contractors. IT terminated logical access within 24 hours of notification.	No exceptions noted.
6.2.4	01.v 02.i	Terminated employee and contractor access to Company facilities is removed upon termination and company assets returned.	**Inspection:** Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and company assets returned.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.2.5	05.k	Vendors and third-party providers are required to notify the Company within 15 days of any terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges.	**Inquiry, Observation and Inspection:** Inquired of management, observed the generation of a list of vendor terminations during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Vendor Management Policy, and verified vendors and third-party providers are required to notify the Company within 15 days of any terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
6.2.6	01.e	A user access review of network and application accounts, and associated permissions, is performed semi-annually to ensure appropriate logical access is maintained.	**Inspection:** Obtained and reviewed the user access review. Verified a user access review of network and application accounts, and associated permissions, was performed semi-annually to ensure appropriate logical access was maintained.	No exceptions noted.
6.2.7	01.e	Management performs a review of network and application administrator access semi-annually to ensure that appropriate privileged access is restricted.	**Inspection:** Obtained and reviewed the administrator access review. Verified management performed a review of network and application administrator access semi-annually to ensure that appropriate privileged access is restricted.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.				

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.3	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.			
6.3.1	01.b	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the Access Management Policies. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.
6.3.2	01.v 06.e 01.b	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inspection:** Obtained and reviewed the access request tickets for the sampled employees hired during the audit period. Verified new user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process.	No exceptions noted.
6.3.3	02.i	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Inspection:** Obtained and reviewed the termination tickets for sampled employees terminated during the audit period. Verified Human Resources was responsible for notifying IT of terminated employees and contractors. IT terminated logical access within 24 hours of notification.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.3.4	01.v 02.i	Terminated employee and contractor access to Company facilities is removed upon termination and company assets returned.	**Inspection:** Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and company assets returned.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.				
6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
6.4.1	01.l	Access to network equipment is protected via security mechanisms and is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the list of personnel with access to the secure device provisioning room and reconciled with the employee listing. Verified access to network equipment was protected and limited to authorized personnel.	No exceptions noted.
6.4.2	09.o	Procedures are implemented to enforce controls around the management of removable media. The use of removable media is limited to those with a valid business need.	**Inspection:** Obtained and reviewed the Information Classification Policy and the USB Data Export Process. Verified the use of removable media was limited to those with a valid business need.	No exceptions noted.
6.4.3	01.v 02.i	Terminated employee and contractor access to Company facilities is removed upon termination and company assets returned.	**Inspection:** Obtained and reviewed the termination tickets for the sampled employees terminated during the audit period. Verified terminated employee and contractor access to Company facilities was removed upon termination and company assets returned.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.4.4	08.j	Equipment is maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel perform repairs and service equipment, and this service is documented in a ticket.	**Inspection:** Obtained and reviewed a sample ticket of maintenance performed. Verified equipment is maintained and only authorized personnel performs repairs and service equipment and service is documented in a ticket.	No exceptions noted.
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.				
6.5	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.			
6.5.1	07.a	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory and management's review. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.5.2	09.q	Formal data retention and disposal procedures are in place to guide the secure disposal of data that has been identified for destruction in a manner that prevents loss, theft, misuse, or unauthorized access.	**Inspection:** Obtained and reviewed the Record Retention and Disposal Procedures and Schedule. Verified formal data retention and disposal procedures were in place to guide the secure disposal of data that had been identified for destruction in a manner that prevented loss, theft, misuse, or unauthorized access.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.5.3	08.l 09.p	Prior to disposal, all electronic media is securely wiped and sanitized to remove all data and software.	**Inquiry, Observation and Inspection:** Inquired of Management, observed the generation of a list of data disposals during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Record Retention and Disposal Policy, and verified all electronic media is securely wiped and sanitized to remove all data and software, prior to disposal.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
6.5.4	01.x	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed encryption screenshots for sampled employees during the audit period. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.				

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
6.6.1	01.c 01.n	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the administrator user listing and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.
6.6.2	01.j 01.y	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.6.3		SSH keys are used to access all storage nodes.	**Inspection:** Obtained and reviewed the SSH configuration. Verified SSH keys were in place and used to access all storage nodes.	No exceptions noted.
6.6.4	08.f 01.m 01.n 01.o	Firewalls are in place to protect production systems and are configured to restrict unnecessary ports, protocols, and services. Logs are monitored to detect any potential security vulnerabilities or unauthorized access attempts.	**Inspection:** Obtained and reviewed the network diagram, firewall configuration and firewall logs. Verified firewalls were in place to protect production systems and were configured to restrict unnecessary ports, protocols, and services and logs were monitored to detect any potential security vulnerabilities or unauthorized access attempts.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.6.5	01.y 09.y	The Company uses Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the server TLS configuration. Verified TLS 1.1 or higher was used for transmitting sensitive data over public networks.	No exceptions noted.
6.6.6	09.v	All sensitive information (e.g., covered information, PANs, FTI) is encrypted when sent via end-user messaging technologies (e.g., email, instant messaging, and chat).	**Inspection:** Obtained and reviewed the encryption configuration. Verified sensitive information is encrypted when sent via end-user messaging technologies.	No exceptions noted.
6.6.7	09.m	A current network diagram documents all connections to systems storing, processing or transmitting covered information, including any wireless networks. The network diagram is reviewed and updated annually or any time a significant change is made to the environment.	**Inspection:** Obtained and reviewed the network diagram. Verified the network diagram documented all connections and was reviewed annually or any time a significant change was made to the environment.	No exceptions noted.
6.6.8	01.m	Wireless networks are segregated from internal and private networks. A firewall exists between the wireless networks and the production environment.	**Inspection:** Obtained and reviewed the wireless network diagram. Verified segregation exists between internal and private networks and a firewall existed between the wireless networks and the production environments.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.6.9		An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention (IDS/IPS) configuration and alerts. Verified an IDS/IPS was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	No exceptions noted.
6.6.10	01.x	The Company installs personal firewall software or equivalent functionality on any mobile and/or employee-owned computers with direct connectivity to the Internet which are used to access the organization's network.	**Inspection:** Obtained and reviewed the personal firewall console configuration. Verified personal firewall software on computers with direct connectivity to the Internet which are used to access the organization's network was installed.	No exceptions noted.
6.6.11	01.x	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed encryption screenshots for sampled employees during the audit period. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.				

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.7	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.			
6.7.1	10.f 06.f	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Data Classification, Transfer, and Handling Policy. Verified policies and procedures on the use of cryptographic controls for protection of information were documented.	No exceptions noted.
6.7.2	09.x	The confidentiality and integrity for electronic commerce is maintained.	**Inspection:** Obtained and reviewed the TLS certificate. Verified the confidentiality and integrity for electronic commerce was maintained.	No exceptions noted.
6.7.3	01.j 01.y	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.7.4	01.y 09.y	The Company uses Transport Layer Security (TLS 1.1 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the server TLS configuration. Verified TLS 1.1 or higher was used for transmitting sensitive data over public networks.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.7.5	01.x	Corporate laptops are encrypted in the event they are lost or stolen.	**Inspection:** Obtained and reviewed encryption screenshots for sampled employees during the audit period. Verified corporate laptops were encrypted in the event they were lost or stolen.	No exceptions noted.
6.7.6	09.o	Procedures are implemented to enforce controls around the management of removable media. The use of removable media is limited to those with a valid business need.	**Inspection:** Obtained and reviewed the Information Classification Policy and the USB Data Export Process. Verified the use of removable media was limited to those with a valid business need.	No exceptions noted.
6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
6.8.1	09.g 10.k	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the documented Change Management Policy addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.8.2	10.h	System and configuration management tools are used to maintain an inventory of installed applications and software and to monitor patch status. These tools log and alert IT of software installation or attempted software installation.	**Inspection:** Obtained and reviewed the application inventory, device enrolment configuration, and the configuration management system alert configuration. Verified system and configuration management tools were used to maintain an inventory of installed applications and software and to monitor patch status. These tools logged and alerted IT of software installation or attempted software installation.	No exceptions noted.
6.8.3	09.j 09.k	Anti-virus software is installed on all servers and workstations. Updates are pushed to the nodes as new updates and signatures become available.	**Inspection:** Obtained and reviewed the anti-virus configuration. Verified it is installed on all workstations and updates are pushed as new updates and signatures become available.	No exceptions noted.
6.8.4		Procedures are in place to wipe information assets that have been transferred or returned to the entity's custody prior to its implementation on the network.	**Inspection:** Obtained and reviewed the Asset Management Policy. Verified Procedures were in place to wipe information assets that had been transferred or returned to the entity's custody prior to its implementation on the network.	No exceptions noted.
6.8.5	01.w 01.m	Separate environments are used for development, testing, and production. Developers do not have the ability to migrate changes to production.	**Inspection:** Obtained and reviewed the network diagrams, developer listings and reconciled with the production access listing. Verified separate environments were used for development, testing, and production. Developers did not have the ability to migrate changes to production.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.1	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.			
7.1.1	10.m	An enterprise monitoring tool is in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts are sent to security personnel.	**Inspection:** Obtained and reviewed the monitoring dashboard and alert configuration. Verified an enterprise monitoring tool was in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts were sent to security personnel.	No exceptions noted.
7.1.2		Internal and external vulnerability scans are performed continually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the internal and external vulnerability scan report. Verified internal and external vulnerability scans were performed continually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
7.1.3		Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.1.4	06.h	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the Configuration Standards and the configuration compliance review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, annually.	No exceptions noted.
7.2	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.			
7.2.1		External parties are provided with instructions for communicating potential security breaches to the Company.	**Inspection:** Obtained and reviewed the Master Service Agreements (MSA) for the sampled customers obtained during the audit period. Verified external parties were provided with instructions for communicating potential security breaches to the Company.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.2.2	06.h	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the Configuration Standards and the configuration compliance review. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, annually.	No exceptions noted.
7.2.3		An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention (IDS/IPS) configuration and alerts. Verified an IDS/IPS was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.2.4	10.m	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Inspection:** Obtained and reviewed the security event tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution.	No exceptions noted.
7.2.5	11.c	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Security Incident Response Policy. Verified Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.2.6	11.d	Procedures are in place to monitor and quantify the types, volumes, and costs of information security incidents.	**Inspection:** Obtained and reviewed the Security Incident Response Policy. Verified procedures are in place to monitor and quantify the types, volumes, and costs of information security incidents.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.3	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.			
7.3.1	11.c	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Security Incident Response Policy. Verified Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.3.2	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.3.3	10.m	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Inspection:** Obtained and reviewed the security event tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution.	No exceptions noted.
7.3.4	11.d	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inspection:** Obtained and reviewed the incident ticket for the sampled critical security incident during the audit period. Verified management performed an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	No exceptions noted.
7.3.5		The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inspection:** Obtained and reviewed the Disaster Recovery Plan test report. Verified the Business Continuity and Disaster Recovery Plan was tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan was updated based on the test results.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.3.6	09.l	Backup restore testing is performed annually, at minimum, to test the integrity of the backup data and the effectiveness of the Business Continuity and Disaster Recovery plan.	**Inspection:** Obtained and reviewed the backup restore test report. Verified backup restore testing was performed annually to test the integrity of the backup data and the effectiveness of the Business Continuity and Disaster Recovery plan.	No exceptions noted.
7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
7.4.1	11.c	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Security Incident Response Policy. Verified Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.4.2	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.4.3	11.d	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inspection:** Obtained and reviewed the incident ticket for the sampled critical security incident during the audit period. Verified management performed an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	No exceptions noted.
7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.			
7.5.1		The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inspection:** Obtained and reviewed the Disaster Recovery Plan test report. Verified the Business Continuity and Disaster Recovery Plan was tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan was updated based on the test results.	No exceptions noted.
7.5.2	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.5.3	11.d	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inspection:** Obtained and reviewed the incident ticket for the sampled critical security incident during the audit period. Verified management performed an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	No exceptions noted.

8.0 CHANGE MANAGEMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
8.1.1	10.a	The Company has adopted a formal Systems Development Life Cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC takes into account Security requirements.	**Inspection:** Obtained and reviewed the System Development Life Cycle (SDLC) methodology. Verified the Company had adopted a formal SDLC methodology that governed the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC took into account Security requirements	No exceptions noted.
8.1.2	09.g 10.k	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the documented Change Management Policy addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.

8.0 CHANGE MANAGEMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1.3	10.b 10.l	Applications are developed based on secure coding guidelines to prevent common coding vulnerabilities in software development processes. During system development (e.g., applications, databases), checks are applied to the input of business transactions, standing data, and parameter tables.	**Inspection:** Obtained and reviewed the Database Best Practices, General Coding Best Practices, and the software development lifecycle. Verified applications were developed based on secure coding guidelines to prevent common coding vulnerabilities in software development processes. During system development (e.g., applications, databases), checks were applied to the input of business transactions, standing data, and parameter tables.	No exceptions noted.
8.1.4	09.b	System changes are documented, tested, and approved prior to migrating the change to production as part of the change management process.	**Inspection:** Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified system changes were documented, tested, and approved prior to the change being moved to production.	No exceptions noted.
8.1.5		Emergency changes are documented, authorized, tested, and approved following the Change Management Policy.	**Inspection:** Obtained and reviewed the change tickets for the sampled emergency changes during the audit period. Verified emergency changes were documented, authorized, tested, and approved following the Change Management Policy.	No exceptions noted.
8.1.6		Changes made to systems are communicated to appropriate users.	**Inspection:** Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified system changes were communicated to appropriate users.	No exceptions noted.

8.0 CHANGE MANAGEMENT				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1.7	10.k	Vendor security patches are evaluated, and critical patches are applied to key systems and applications within 30 days of release.	**Inspection:** Obtained and reviewed the update configuration. Verified vendor security patches were evaluated, and critical patches were applied to key systems and applications within 30 days of release.	No exceptions noted.

9.0 RISK MITIGATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
9.1.1	03.a	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Management Policy. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
9.1.2		Risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	**Inspection:** Obtained and reviewed the insurance policy. Verified risk management activities considered the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	No exceptions noted.
9.1.3	00.a 07.c	The Company maintains an Information Security Management Program that is defined in terms of the characteristics of the business, and is established and managed including monitoring, maintenance, and improvement. The Company establishes implements, maintains and continually improves the Information Security Management System, in accordance with the requirements of the standards.	**Inspection:** Obtained and reviewed the Information Security Policy and the Employee Training Plan. Verified the Company maintained an Information Security Management Program that was defined in terms of the characteristics of the business, and was established and managed including monitoring, maintenance, and improvement. Verified the Company established, implemented, maintained and continually improves the Information Security Management System, in accordance with the requirements of the standards.	No exceptions noted.

9.0 RISK MITIGATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.2	The entity assesses and manages risks associated with vendors and business partners.			
9.2.1		The Company has a Vendor Management Policy, which provides guidance regarding the identification and management of critical vendors and business partners.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified the Company had a Vendor Management Policy, which provided guidance regarding the identification and management of critical vendors and business partners.	No exceptions noted.
9.2.2		Executed agreements are maintained for sub-service organizations. These agreements define the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	**Inspection:** Obtained and reviewed service agreements for the sub-service organizations utilized during the audit period. Verified executed agreements were maintained for vendors and business partners. These agreements defined the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	No exceptions noted.
9.2.3	09.f	SOC audit reports of key sub-service organizations are reviewed for appropriateness, including complementary user entity controls.	**Inspection:** Obtained and reviewed the SOC Report for the sub-service organization. Verified the SOC Report was reviewed for appropriateness, including complementary user entity controls.	No exceptions noted.

9.0 RISK MITIGATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.2.4		Management requires all critical vendors without a SOC report to fill out a questionnaire to evaluate risk.	**Inquiry, Observation and Inspection:** Inquired of client management, observed the generation of a list of critical vendors during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, inquired with Management that all critical vendors without a SOC report to fill out a questionnaire to evaluate risk.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
9.2.5	09.f	A periodic review of service level agreements (SLAs) is conducted annually, at minimum, and compared against the monitoring records.	**Inspection:** Obtained and reviewed the SLA review. Verified the review is completed annually against monitoring records.	No exceptions noted.

9.0 RISK MITIGATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.2.6	05.i	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy and vendor review. Verified the Company maintained a formal process that assessed the potential threats and vulnerabilities from vendors providing goods and services. Additionally, the Company assessed, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	No exceptions noted.
9.2.7	05.i	Vendors and third-parties are not provided access to the Company's information until the appropriate controls have been implemented and a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.	**Inquiry, Observation and Inspection:** Inquired of management, observed the generation of a list of new vendors during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Vendor Management Policy, and verified vendors and third-parties are not provided access to the Company's information until the appropriate controls were implemented and a contract is signed.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

9.0 RISK MITIGATION				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.2.8	00.a 07.c	The Company maintains an Information Security Management Program that is defined in terms of the characteristics of the business, and is established and managed including monitoring, maintenance, and improvement. The Company establishes implements, maintains and continually improves the Information Security Management System, in accordance with the requirements of the standards.	**Inspection:** Obtained and reviewed the Information Security Policy and the Employee Training Plan. Verified the Company maintained an Information Security Management Program that was defined in terms of the characteristics of the business, and was established and managed including monitoring, maintenance, and improvement. Verified the Company established, implemented, maintained and continually improves the Information Security Management System, in accordance with the requirements of the standards.	No exceptions noted.

Additional Criteria for Availability

AVAILABILITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A 1.1.1	10.m	An enterprise monitoring tool is in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts are sent to security personnel.	**Inspection:** Obtained and reviewed the monitoring dashboard and alert configuration. Verified an enterprise monitoring tool was in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts were sent to security personnel.	No exceptions noted.
AWS is responsible for ensuring capacity demand controls are in place to meet availability commitments and requirements.				
A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A 1.2.1	06.c	The Company maintains recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	**Inspection:** Obtained and reviewed the Backup and Recovery Policy. Verified the Company maintained recovery strategies, such as data replication, offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	No exceptions noted.
AWS is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.				

AVAILABILITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A 1.3.1	11.d	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inspection:** Obtained and reviewed the incident ticket for the sampled critical security incident during the audit period. Verified management performed an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	No exceptions noted.
A 1.3.2	02.e 11.a	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Incident Response Policy and training report for the sampled employees during the audit period. Verified the Company had a comprehensive Incident Response Plan that was communicated to staff and was regularly updated. Incident response training was held annually.	No exceptions noted.

AVAILABILITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
A 1.3.3		Incident recovery plan testing is performed annually, at minimum. The testing includes: • development of testing scenarios based on threat likelihood and magnitude; • consideration of relevant system components from across the Company that can impair availability; • scenarios that consider the potential for the lack of availability of key personnel; and • revision of continuity plans and systems based on test results.	**Inspection:** Obtained and reviewed the Business Continuity Plan Test, which included Incident Recovery Plan testing. Verified testing was performed annually and included: • development of testing scenarios based on threat likelihood and magnitude; • consideration of relevant system components from across the Company that can impair availability; • scenarios that consider the potential for the lack of availability of key personnel; and • revision of continuity plans and systems based on test results.	No exceptions noted.
A 1.3.4		The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inspection:** Obtained and reviewed the Disaster Recovery Plan test report. Verified the Business Continuity and Disaster Recovery Plan was tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan was updated based on the test results.	No exceptions noted.

AVAILABILITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
A 1.3.5	09.l	Backup restore testing is performed annually, at minimum, to test the integrity of the backup data and the effectiveness of the Business Continuity and Disaster Recovery plan.	**Inspection:** Obtained and reviewed the backup restore test report. Verified backup restore testing was performed annually to test the integrity of the backup data and the effectiveness of the Business Continuity and Disaster Recovery plan.	No exceptions noted.
A 1.3.6	09.l	Inventory records for the backup copies, including content and current location, is maintained.	**Inspection:** Obtained and reviewed the inventory records of the backup files. Verified inventory records for the backup copies, including content and current location, was maintained.	No exceptions noted.

Additional Criteria for Confidentiality

CONFIDENTIALITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C 1.1.1		Procedures are in place to identify and designate confidential information when it is received or created, and to determine the period over which the confidential information is to be retained.	**Inspection:** Obtained and reviewed the Data Classification and Handling Policy, the Record Retention and Destruction Policy, and the Personal Data Management and Protection Policy. Verified procedures were in place to identify and designate confidential information when it was received or created, and to determine the period over which the confidential information was to be retained.	No exceptions noted.
C 1.1.2		Procedures are in place to protect confidential information from erasure or destruction during the specified retention period.	**Inspection:** Obtained and reviewed the Data Classification and Handling Policy, the Record Retention and Destruction Policy, and the Personal Data Management and Protection Policy. Verified procedures were in place to protect confidential information from erasure or destruction during the specified retention period.	No exceptions noted.

CONFIDENTIALITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
C 1.1.3		Executed agreements are maintained for sub-service organizations. These agreements define the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	**Inspection:** Obtained and reviewed service agreements for the sub-service organizations utilized during the audit period. Verified executed agreements were maintained for vendors and business partners. These agreements defined the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	No exceptions noted.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C 1.2.1		Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	**Inspection:** Obtained and reviewed the Record Retention and Destruction Policy. Verified procedures were in place to identify confidential information requiring destruction when the end of the retention period was reached.	No exceptions noted.
C 1.2.2	09.q	Formal data retention and disposal procedures are in place to guide the secure disposal of data that has been identified for destruction in a manner that prevents loss, theft, misuse, or unauthorized access.	**Inspection:** Obtained and reviewed the Record Retention and Disposal Procedures and Schedule. Verified formal data retention and disposal procedures were in place to guide the secure disposal of data that had been identified for destruction in a manner that prevented loss, theft, misuse, or unauthorized access.	No exceptions noted.

CONFIDENTIALITY				
Control #	**HITRUST CSF 9.4 Control #**	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
C 1.2.3		On an as-needed basis, confidential information is identified either through data retention requirements, contractual obligations, or customer requests, and the data is securely sanitized, wiped, or destroyed.	**Inquiry, Observation and Inspection:** Inquired of management, observed the generation of a list of destruction requests during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Study Closeout Policy, and verified confidential information would be identified either through data retention requirements, contractual obligations, or customer requests, and the data would be securely sanitized, wiped, or destroyed.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
C 1.2.4	08.l 09.p	Prior to disposal, all electronic media is securely wiped and sanitized to remove all data and software.	**Inquiry, Observation and Inspection:** Inquired of Management, observed the generation of a list of data disposals during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Record Retention and Disposal Policy, and verified all electronic media is securely wiped and sanitized to remove all data and software, prior to disposal.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

SECTION FIVE

Other Information Provided by THREAD

OTHER INFORMATION PROVIDED BY THREAD

The information included in this section of the report is presented by THREAD to provide additional information to user entities and is not part of THREAD's description of controls placed in operation. The information in this section has not been subjected to the procedures applied in the examination of the description of controls related to the security, availability and confidentiality principles and specific criteria and, accordingly, CyberGuard Compliance, LLP expresses no opinion on it.

1 Management's Response to Testing Exceptions

Control Number	Criteria	Control Description	Test Results
6.1.7	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.	Modified user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inquiry:** Inquired with management regarding user access modifications during the audit period and determined a population of access modifications during the audit period could not be provided. Therefore, we were unable to verify that modified user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.
Management's Response: listings were unable to be provided for users whose access was modified after initial onboarding. Access changes were recorded but not in a format that was requested by the auditor. **Remediation Plan:** THREAD ensures to identify modified users going forward.			