

System and Organization Controls (SOC 2) Type 2 Report

Cloud Vendor Platform as a Service Built-On Cloud Vendor Cloud Infrastructure



For the Period April 1, 2022, to March 31, 2023

A Type 2 Independent Service Auditor’s Report on Controls Relevant to Security and Availability

Confidential - Cloud Vendor

# TABLE OF CONTENTS

[SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT 2](#_gjdgxs)

[SECTION II – CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE MANAGEMENT’S ASSERTION 5](#_30j0zll)

[SECTION III – DESCRIPTION OF CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE SYSTEM 6](#_1fob9te)

[SECTION IV – CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE CONTROLS, TEST PROCEDURES, AND](#_3znysh7) [RESULTS OF TESTING 19](#_3znysh7)

**1** System and Organization Controls (SOC 2) Type 2 Report | Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure Confidential - Cloud Vendor

# SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT

To Cloud Vendor, Inc. :

Scope

We have examined Cloud Vendor, Inc.’s (“Cloud Vendor” or the “service organization”) accompanying description of its Cloud Vendor Platform as a Service (PaaS) Built-On Cloud Vendor Cloud Infrastructure system, in Section 3, throughout the period April 1, 2022, to March 31, 2023 (the “description”), based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria)* (“description criteria”) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 20 22, to March 31, 2023, to provide reasonable assurance that Cloud Vendor’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability (“applicable trust services criteria”) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Cloud Vendor uses a subservice organization for cloud hosting services for monitoring data center hosting services, and network security services, including security list management. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cloud Vendor, to achieve Cloud Vendor’s service commitments and system requirements based on the applicable trust services criteria. The description presents Cloud Vendor’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cloud Vendor’s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

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

*Service Auditor’s Responsibilities*

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). 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 organiza tion’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Δ Obtaining an understanding of the system and the service organization’s service commitments and system requirements;

Δ 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;

Δ Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;

Δ Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the serv ice organization achieved its service commitments and system requirements based on the applicable trust services criteria;

Δ 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

Δ Evaluating the overall presentation of the description.

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

*Inherent Limitations*

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

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

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

*Description of Test of Controls*

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled “Testing Matrices.”

*Opinion*

In our opinion, in all material respects :

1. the description presents the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
2. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Cloud Vendor’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and the user entities applied the complementary controls assumed in the design of Cloud Vendor’s controls throughout that period; and
3. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Cloud Vendor’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and user entity controls assumed in the design of Cloud Vendor’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 Cloud Vendor; user entities of the Cloud Vendor PaaS Built-On Cloud Vendor Cloud Infrastructure system during some or all of the period April 1, 2022, to March 31, 2023, business partners of Cloud Vendor subject to risks arising from interactions with the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure 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:

Δ The nature of the service provided by the service organization;

Δ How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties;

Δ Internal control and its limitations;

Δ 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;

Δ User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services;

Location

April 20, 2023

# SECTION II – CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE MANAGEMENT’S ASSERTION

We have prepared the accompanying description of the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system , in Section 3, throughout the period April 1, 2022, to March 31, 2023 (the “description”) , based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria),* (“description criteria”). The description is intended to provide report users with information about the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system that may be useful when assessing the risks arising from interactions with Cloud Vendor’s system, particularly information about system controls that Cloud Vendor 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 and availability ( “applicable trust services criteria ”) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Cloud Vendor uses a subservice organization for cloud hosting services for monitoring data center hosting services, and network security services, including security list management. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cloud Vendor, to achieve Cloud Vendor’s service commitments and system requirements based on the applicable trust services criteria. The description presents Cloud Vendor’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cloud Vendor’s controls. The description does not disclose the actual controls at the subservice organization.

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

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

1. the description presents the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
2. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Cloud Vendor’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and the user entities applied the complementary controls assumed in the design of Cloud Vendor’s controls throughout that period; and
3. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023 , to provide reasonable assurance that Cloud Vendor ’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of Cloud Vendor’s controls operated effectively throughout that period.

# SECTION III – DESCRIPTION OF CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE SYSTEM

## Cloud Vendor Corporation Overview

Cloud Vendor provides products and services that address enterprise information technology (IT) environments. Cloud Vendor products and services include enterprise applications and infrastructure offerings that are delivered worldwide through a variety of flexible and interoperable IT deployment models. These models include on-premises deployments, cloud-based deployments, and hybrid deployments (an approach that combine s both on-premise and cloud-based deployment) such as the Cloud Vendor Cloud at Customer offering (an instance of Cloud Vendor Cloud in a customer’s own data center). Accordingly, Cloud Vendor offers choice and flexibility to their customers and facilitate the product, ser vice and deployment combinations that best suit their customers’ needs. Cloud Vendor customers include businesses of many sizes, government agencies, educational institutions, and resellers that Cloud Vendor markets and sells to directly through worldwide sales force and indirectly through the Cloud Vendor Partner Network. Using Cloud Vendor technologies, customers can build, deploy, run, manage, and support their internal and external products, services, and business operations.

Cloud Vendor Cloud Services offerings provide a comprehensive and fully integrated stack of applications and infrastructure services delivered via a cloud-based deployment model. Cloud Vendor Cloud Services integrate IT components, including software, hardware, and services, on a customer’s behalf in a cloud -based IT environment that Cloud Vendor deploys, manages, supports, and upgrades for the customer and may be accessed by the customer utilizing common web browsers via a broad spectrum of devices.

Cloud Vendor Cloud Services are designed to be rapidly deployable to enable customers toward innovation; intuitive for casual and experienced users; easily maintainable to reduce upgrade, integration and testing work; connectable among different deployment models to enable interchangeability and extendibility between IT environments ; compatible to easily move workloads between the Cloud Vendor Cloud and other IT environments; requiring lower upfront customer investment, secure, standards -based and reliable.

Cloud Vendor cloud license and on -premises license deployment offerings include Cloud Vendor Applications, Cloud Vendor Database and Cloud Vendor Middleware software offerings, among others, which customers deploy using IT infrastructure from the Cloud Vendor Cloud or their own cloud-based or on-premises IT environments. Substantially all customers, at their option, purchase license support contracts when they purchase a Cloud Vendor license.

Cloud Vendor hardware product offerings include Cloud Vendor Engineered Systems, servers, storage, and industry -specific products, among others. Cloud Vendor also offers services to assist customers and partners to help maximize the performance of their Cloud Vendor purchases.

Providing choice and flexibility to Cloud Vendor customers as to when and how customers deploy Cloud Vendor applications and infrastructure technologies is an important element of Cloud Vendor’s corpor ate strategy. Cloud Vendor believes that offering customers broad, comprehensive, flexible, and interoperable deployment models for Cloud Vendor applications and infrastructure technologies is important to growth strategies.

## Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure Overview

Cloud Vendor PaaS Built–On Cloud Vendor Cloud Infrastructure provides customers with various platforms to build and deploy applications within the public, private, or hybrid cloud. Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure provides cloud offerings in the areas of application development, data management, business analytics, integration, content, and collaboration, and mobile. The cloud offerings that are within the scope of this assessment are included in the Service Descriptions section below.

Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure cloud services support traditional workloads, however initiation, authorization, recording and processing of transactions is the responsibility of the customer. Transferring transactions to reports and correction of incorrect information presented to user entities are also the responsibility of the customer. Additionally, controls governing the related accounting records, supporting information, and specific accounts that are used to process transactions are the responsibility of the customer.

## Infrastructure and Software

Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure runs on Linux server operating systems and are supported by Cloud Vendor databases. The production servers supporting Cloud Vendor PaaS Built-On Cloud Vendor Cloud Infrastructure are located within a separate network segment that is dedicated to cloud services. Remote access to Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure production networks is required to pass through encrypted virtual private networks (VPNs). An intrusion detection system (IDS) is in place to monitor network traffic for potential security breaches.

The production infrastructure resides within Cloud Vendor Cloud Infrastructure regions.

## Subservice Organizations

Cloud Vendor utilizes the cloud hosting services provided by Cloud Vendor Cloud Infrastructure for monitoring data center hosting services, and network security services, including security list management.

Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting services, including the physical safeguarding of the IT infrastructure to mitigate the risk of unauthorized access to the IT infrastructure, as well as environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Cloud Vendor Cloud Infrastructure to achieve Cloud Vendor’s service commitments and system requirements based on the applicable trust services criteria.

| **CONTROL ACTIVITY EXPECTED TO BE IMPLEMENTED BY VENDOR CLOUD INFRASTRUCTURE.** | **APPLICABLE TRUST SERVICES CRITERIA** |
| --- | --- |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for restricting physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers. | CC6.4 CC6.5 |
| Cloud Vendor Cloud Infrastructure is responsible for implementing logical access security measures to protect against threats from sources outside the boundaries of the system. | CC6.6 |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for monitoring physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers. | CC7.2 |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for ensuring the data center facilities are equipped with environmental security safeguards and are utilizing environmental monitoring applications to monitor for environmental events. | A1.2 |

## Monitoring of Subservice Organizations

Cloud Vendor Cloud Services personnel monitor the performance of the cloud hosting services pr ovider on an ongoing basis as a component of normal business operations throughout the year. This includes obtaining and reviewing the applicable third -party attestations for Cloud Vendor Cloud Infrastructure.

# Service Descriptions

# The scope of this report includes the controls placed in operation specifically for the following Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure services to meet the Trust Services Criteria related to security and availability. These criteria are set for th in TSP section 100, of the 2017, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

# Services available to customers may include, but are not limited to, the offerings described below. The actual services provided by Cloud Vendor depends on both the contractual agreement with and the services provisioned by each individual customer.

# Cloud Vendor Analytics Cloud

# Cloud Vendor Analytics Cloud is a scalable and secure public cloud service that provides a full set of capabilities to explore and perform collaborative analytics for customers. The service offers flexible data storage and tools for deriving and sharing data insights. Key features of Cloud Vendor Analytics Cloud include, but are not limited to, the following:

# Δ Data preparation: Analysts can ingest, profile, and cleanse data using a variety of algorithms.

# Δ Data flow: Analysts can prepare, transform, and aggregate data, and then run machine- learning models at scale.

# Δ Data discovery: Subject matter experts can collaborate with other business users, blending intelligent analysis at scale, machine learning, and statistical modeling.

# Δ Data visualization: Analysts can visualize any data, on any device, on premises and in the cloud.

# Δ Data collaboration: Large organizations and small teams can share data more simply, without the need to manage or consolidate multiple versions of spreadsheets, and quickly perform ad hoc analysis of the spreadsheet data.

# Δ Data-driven: Application developers can utilize interfaces that enable them to extend, customize, and embed rich analytic experiences in the application flow.

# Cloud Vendor Application Program Interface (API) Platform Cloud Service

# Cloud Vendor API Platform Cloud Service is a complete lifecycle solution that supports agile API development and makes it easy to keep an eye on key performance indicators (KPIs). The service allows for creating, managing, securing, and advertising APIs to connect to new or existing services. Key features of the Cloud Vendor API Platform Cloud Service include, but are not limited to, the following:

# Δ Enables authorized and authenticated developers of mobile and web apps to access and consume an organization’s services.

# Δ Can be deployed on- premises or to any cloud service including Cloud Vendor Cloud, Alternate Vendor Cloud, and Alternate Vendor Cloud Cloud, thus allowing the API and services to reside in the same place.

# Δ Enables access to legacy applications and services without modifying the legacy code base.

# Δ Route requests to more than one service.

## Cloud Vendor Big Data Cloud Service – Compute Edition

Cloud Vendor Big Data Cloud Service gives customers access to the resources of a preconfigured Cloud Vendor Big Data environment, including a complete installation of the Alternate Vendor Distribution Including Alternate Vendor Hadoop (XXX) and Alternate Vendor Product. The service is used to capture and analyze massive volumes of data generated by social media feeds, email, web logs, photographs, smart meters, sensors, and similar devices.

## Cloud Vendor Management Cloud

Cloud Vendor Management Cloud is a suite of integrated monitoring, management, and analytics cloud offerings. This suite is designed for today’s heterogeneous environments: on- premises, Cloud Vendor Cloud, and third -party cloud serv ices. Cloud Vendor Management Cloud enables customers to store uploaded data in a single unified platform. It automatically analyzes data using matching learning, proactive monitoring, analysis, and correlations across its offerings. Cloud Vendor Management Cloud eliminates the existence of multiple information silos in end-user and infrastructure data and resolves application issues quickly.

## Cloud Vendor Mobile Hub

Cloud Vendor Mobile Hub is a suite of public cloud services that consists of a set of integrated components enabl ing developers, managers, and mobile cloud administrators to develop, maintain, monitor, and export mobile apps and the resources they rely on. Key features of the Cloud Vendor Mobile Hub include, but are not limited to, the following:

Δ Notifications for writing code to send notifications to mobile apps.

Δ My Profile to retrieve the current app user’s profile.

Δ Storage to work with collections and objects (such as images and documents) that are associated with a customer’s backend.

Δ Data Offline and Sync to build applications that cache REST resources for offline use and then synchronize all offline changes with the server when the device goes online again.

Δ Location to define location devices and places and query for them from mobile apps.

Δ Database Access and Database Management to access the database associated with a customer’s Mobile Hub instance.

Δ App policies to retrieve application configuration properties that you have set in the backend.

## Cloud Vendor Product Cloud Service

Cloud Vendor Product Cloud Service is a visual and declarative cloud environment for developing and hosting engaging mobile and web applications. Cloud Vendor Product Cloud Service provides easy access to data from any REST -based service and enables the creation of custom reusable business objects for storing and managing data. Using the cloud -based visual development tools, customers can create and test responsive web applications and native mobile apps without the need to install any additional software.

## Cloud Vendor Product Studio

Product Studio is an application development platform that helps customers plan and manage work through all stages of the application development lifecycle: design, build, test, and deploy. Product Studio enables developers to easily deploy their applications to their preferred target, whether it’s a staging or production instance of Cloud Vendor Cloud Applications or a Cloud Vendor Cloud Infrastructure service instance.

## Cloud Vendor Domain Name System (DNS)

Cloud Vendor Cloud Infrastructure is a set of complementary cloud services that enables customers to build and run a wide range of applications and services in a highly available hosted environment. Cloud Vendor Cloud Infrastructure offers high-performance compute capabilities (as physical hardware or virtual instances) and storage capacity in a flexible overlay virtual network that is securely accessible from customers’ on -premises networks. Cloud Vendor Cloud Infrastructure’s DNS Service helps customers to optimize performance and communication at the edge of the Cloud Vendor Cloud.

Services available to customers may include, but are not limited to, the offering described below. The actual services provided by Cloud Vendor depend on the contractual agreement with and the services provisioned by each individual customer.

Cloud Vendor DNS allows customers to create and manage their DNS zones. Customers can create zones, add records to zones, and allow the edge network to handle their domain's DNS queries.

Service components used to build a DNS zone and make it accessible from the internet include:

Δ Domain - Domain names identify a specific location or group of locations on the Internet as a whole. A common definition of "domain" is the complete portion of the DNS tree that has been delegated to a user's control. For example, example.com or Cloud Vendor.com.

Δ Zone - A zone is a is a portion of the DNS namespace. A Start of Authority record (SOA) defines a zone. A zone contains all labels underneath itself in the tree, unless otherwise specified.

Δ Label - Labels are prepended to the zone name, separated by a period, to form the name of a subdomain. For example, the "www" section of [www.example.com](http://www.example.com/) are labels. Records are associated with these domains.

Δ Child Zone - Child zones are independent subdomains with their own SOA and Name Server (NS) records. The parent zone of a child zone must contain NS records that refer DNS queries to the name servers responsible for the child zone. Each subsequent child zone creates another link in the delegation chain.

Δ Resource Records - A record contains specific domain information for a zone. Each record type contains information called record data (RDATA). For example, the RDATA of an A or AAAA record contains an IP address for a domain name, while MX records contain information about the mail server for a domain. Cloud Vendor Cloud Infrastructure normalizes all RDATA into the most machine -readable format. The returned presentation of RDATA may differ from its initial input.

Δ Delegation - The name servers where the customer’s DNS is hosted and managed.

## Principal Service Commitments and System Requirements

Cloud Vendor is committed to providing their clients a secure environment in which to conduct their business as pertains to the use of Cloud Vendor services. The commitment to security begins with the contract signed between Cloud Vendor and the client. The contract contains specific language around the security that Cloud Vendor will provide as part of their ongoing services. Contracts are communicated to external client users and are utilized by Cloud Vendor to create policy documents that put in place procedures to help ensure that the security commitments are met. Through a combination of policies, processes, and controls, Cloud Vendor operates in a manner that focuses on providing security in the user environment. In the event of a downgrade to security or an incident that may jeopardize their security commitment, Cloud Vendor has in place a security incident procedure by which they identify, investigate, and resolve the incident. Cloud Vendor communicates security incidents to external users as deemed necessary and based on the impact of the incident. Cloud Vendor policies, procedures, and controls establish and govern all areas of security applicable to Cloud Vendor services and to its customers’ use of Cloud Vendor services. Cloud Vendor personnel are subject to this security policy and any additional policies that govern their employment or the services they provide to Cloud Vendor.

Cloud Vendor communicates a 99.5% target uptime for the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure. Various monitoring capabilities are available for end users.

Cloud Vendor’s confidential information is a valuable corporate asset and protecting the confidential information of customers (user entities) and others with whom Cloud Vendor interacts (e.g., partners, suppliers, web site registrants, potential acquisitions, employment applicants) is a commitment Cloud Vendor makes. This commitment applies to data stored in a hard or electronic format. Cloud Vendor has defined groups of information as either public or confidential. Public information is accessible through ordinary means (marketing campaigns, brochures, business cards, press releases, etc.) and is not sensitive nor does it have value to Cloud Vendor or Cloud Vendor’s user entities. All other information is considered confidential. For the purposes of their commitments to customers, Cloud Vendor treats all customer data as confidential. Cloud Vendor commits to safeguarding confidential information by not transferring, publishing, using, or disclosing it other than as necessary in the ordinary course of business or as directed or authorized by Cloud Vendor. Upon commencement of employment with Cloud Vendor, employees must sign a Proprietary Information Agreement (PIA) document that includes acknowledgement of confidentiality requirements. The obligation to protect confidential information continues after the end of an employee’s tenure at Cloud Vendor. Cloud Vendor also requires customers to sign contracts acknowledging that they are aware of their obligations as it pertains to protecting confidential information.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system, and may therefore, not fully address the specific service commitments and requirements made to all system users, in each individual case.

## Relevant Aspects of the Control Environment

The control environment is embodied by the organization’s awareness of the need for controls and the emphasis given to the ap propriate controls as demonstrated by the organization’s policies, procedures, organizational structure, and management actions. The primary elements of the control environment include commitment to integrity and ethical values, oversight responsibility of the Board of Directors, assignment of authority and responsibility, commitment to competence, and account ability.

## Commitment to Integrity and Ethical Values

Cloud Vendor has a reputation for secure and reliable product offerings and related services, and it has invested a great deal of time and resources in protecting the integrity and security of products, services, and the internal and external data managed therein.

Cloud Vendor has a Compliance and Ethics Program that includes a Code of Ethics and Business Conduct (CEBC), which defines and implements the Company’s core values, that applies to all Cloud Vendor entities. Core values include integrity, ethics, compliance, mutual respect, teamwork, communication, innovation, customer satisfaction, quality, and fairness. The CEBC supplements and, in many cases, exceeds what is required to comply with laws and regulations. The Vendor CEBC applies to all personnel employed by or engaged to provide services to Cloud Vendor, including, but not limited to, Cloud Vendor’s employees, officers, temporary employees, workers (including agency workers), casual staff, and independent contractors (“employees”). Cloud Vendor also requires its partners and suppliers to adhere to the Partner Code of Ethics and Business Conduct and its suppliers to adhere to the Supplier Code of Ethics and Business Conduct a s well as the Cloud Vendor Supply Chain Security and Assurance guidance, which are available on the Cloud Vendor website.

The Global Anti -Corruption Policy and Business Courtesy Guidelines (ACP), which also applies to all employees, supplements the CEBC. Both documents are posted on both internal and external corporate websites.

Each new employee is required to complete and sign an employment agreement or equivalent and a Proprietary Information Agreem ent prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local procedures, la ws, and regulations. Additionally, all employees are required to take an Ethics and Business Conduct training upon hire and every two years therea fter.

A confidential ethics helpline has been established for Cloud Vendor employees and non -Cloud Vendor employees, such as business partners, customers, and other stakeholders, to field concerns, questions, or to report violations of the CEBC. The reporting site allows employees to report compliance and ethics situations confidentially and / or anonymously where allowed by local law. A summary of items communicated via the ethics helpline, including fraud, are presented to the Finance and Audit Committee with specific reference to items impacting the financial statements.

## Oversight Responsibility of the Board of Directors

A corporate governance framework is in place at Cloud Vendor for continuity and quality monitoring of the control environment that includes reviewing the results of external controls assessments reports annually. The control environment at Cloud Vendor Cloud Infrastructure originates with, and is the responsibility of, the Cloud Vendor Board of Directors. The Board of Directors provides oversight of Vendor Cloud Infrastructure operations and activities including oversight of the Finance and Audit Committee.

Cloud Vendor Legal reviews the profiles of Board members to ensure the board and committee members meet current regulatory and internal requirements, including independence and expertise.

Cloud Vendor maintains, and distributes externally via its website, its Corporate Governance Guidelines as well as charters for its Finance and Audit Committee, Independent Committee, Compensation Committee, and Nomination and Governance Committee.

## Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day -to-day basis. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Cloud Vendor has developed an organizational structure to meet its needs in support of its control obligations. Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel supporting system design, development, implementation, security, operation, maintenance, and monitoring. The current management structure has adequate diversification and segregation of responsibility across executive management to ensure no overriding influence exists within the current reporting structure. In addition, Cloud Vendor provides IT security oversight to identify and implement security controls and processes in the IT control environment that align with organizational objectives.

Cloud Vendor is supported by the following security groups, which provide oversight of internal IT resources and suppliers:

| **SECURITY GROUP** | **ROLES AND RESPONSIBILITIES** |
| --- | --- |
| Global Information Security (GIS) | GIS is responsible for security oversight, compliance, enforcement, and conducting information assessments leading to the development of information security policy and strategy, as well as training and awareness at the corporate level. This organization serves as the primary contact for security incident response, provid ing overall direction for incident prevention, identification, investigation, and resolution. |
| Global Product Security | Under the leadership of Cloud Vendor’s Chief Security Officer, Global Product Security promotes the use of Cloud Vendor Software Security Assurance s tandards throughout Cloud Vendor, acts as a central resource too help development teams improve the security of their products, and handles specialized security functions. |
| Global Physical Security | Responsible for defining, developing, implementing, and managing all aspects of physical security for the protection or Cloud Vendor’s employees, facilities, business enterprise, and assets. |
| Global Trade Compliance | Responsible for import and export oversight, guidance, enforcement to enable worldwide trade compliant business processes across Cloud Vendor, to uphold and protect Cloud Vendor’s global trade privileges and ensure the success of Cloud Vendor’s business. |
| Security Architecture | The Cloud Vendor corporate security architect helps set internal information- security technical directio n and guides Cloud Vendor’s IT departments and lines of business towards deploying information security and identity management solutions that advance Cloud Vendor's Information Security goals. The corporate security architect works with GIS and [Global Product Security ,](https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html) and the [development Security Leads](https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html) to develop, communicate, and implement corporate security architecture roadmaps. |
| Business Assessment and Audit | Cloud Vendor’s Business Assessment & Audit (BA&A) is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Cloud Vendor policies, standards and select laws and regulations across Cloud Vendor’s Lines of Business and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks or control gaps are confidential and shared with executive leadership and Cloud Vendor’s Board o f Directors. |

## Commitment to Competence

Cloud Vendor Cloud Infrastructure’s commitment to employee competence begins with formal hiring practices designed to help ensure that new employees are qualified for their job responsibilities. The hiring process also includes a robust background check, performed on candidates selected for hire, in accordance with local laws and regulations, and local Cloud Vendor policy.

New employees are supported by a new hire web site and orientation courses. Ongoing training is available to all employees through a variety of courses delivered through web learning and external courses. Training for each employee is tailored to support his or her job role.

Employees are required to complete the Ethics and Business Conduct, Informa tion Protection Awareness (IPA), and the Anti - Corruption & Foreign Corrupt Practices Act online courses upon hire. All Cloud Vendor employees are required to complete IPA training every two years. The Human Resources (HR) Training team runs exception reports monthly to identify any employees or managers not in compliance with these courses and follows up with those individuals by email.

Cloud Vendor Cloud Infrastructure employees must complete security awareness training specific to the services annually. This training includes Cloud Vendor Cloud Infrastructure requirements, the process to report and respond to potential incidents and specific security training tailored to the System. Additionally, employees with access to source code are required to complete annual secure code training. The Cloud Vendor Cloud Infrastructure Security Training team runs exception reports on a periodic basis to identify employees not in compliance with the requirement to complete the annual training and follows up with those individuals’ managers by email.

Critical information is disseminated via email throughout the Company. Employees are also informed about company events, security updates and other matters through the company website "In the Know".

In addition, Cloud Vendor conducts annual appraisal and performance management process for all Cloud Vendor employees. The performance management process follows a performance evaluation framework and clarifies how employees are expected to perform, how they will be measured, and how their work fits into the larger business context.

## Accountability

Cloud Vendor Cloud Infrastructure’s commitment to an effective system of internal control begins with the Cloud Vendor Board of Directors and Finance and Audit Committee. The primary functions of the Finance and Audit Committee ( the “Committee”) are to assist the Board of Directors (the “Board”) of Cloud Vendor Corporation with the Board’s oversight of: management’s conduct of the Corporation’s financial accounting and reporting processes; the integrity of the Corporation’s financial statements; the Corporation’s compliance with legal and regulatory requirements; its independent registered public accounting firm’s qualifications, performance and independence; the performance of the Corporation’s internal audit function; and the evaluation of merger and acquisition transactions and investment transactions proposed by the Corporation’s management. The Finance and Audit Committee holds regular meetings as necessary, but not less than quarterly, and special meetings as may be called by the Chairman of the Committee.

Cloud Vendor has developed internal policies outlining corporate requirements to hold individuals accountable for their internal control responsibilities. The policies are managed centrally, reviewed at least annually and are available to all personnel. Per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers are required to comply with all laws, regulations, contractual obligations, and Cloud Vendor policies. Non -compliance with laws, regulations, and Cloud Vendor policies may result in disciplinary action up to and including termination. Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process.

In addition to corporate policies, Cloud Vendor Cloud Infrastructure has designed and implemented a set of robust standards outlining detailed requirements for various processes undertaken and managed by Cloud Vendor personnel and provide direction for all activities performed.

## Information and Communication

### MyCloud Vendor Support (MOS)

Cloud Vendor customers can access information online through MOS, which is Cloud Vendor Corporation’s portal for technical support services, the primary means of logging electronic Service Requests (SRs), and the source of a variety of support services and information for Cloud Vendor customers.

Cloud Vendor Cloud Infrastructure customers may use MOS to view the knowledge base and technical support services information; search for updates, alerts, and other information about products and releases; and set automated notification preferences regarding newly available information.

Customers may use MOS to log electronic SRs, or they can report incidents to their customer account manager, who is responsible for opening a SR ticket within the Cloud Vendor Cloud Infrastructure system tool for tracking and resolution.

### External Communication

Cloud Vendor Cloud Infrastructure maintains a description of the System, including Cloud Vendor commitments and obligations, detailed information relating to customer responsibilities and customer support guides on the Cloud Vendor public website. The process for external parties to report incidents to Cloud Vendor is also outlined on the Cloud Vendor public website. Customers have access to information about Cloud Vendor corporate security via Cloud Vendor’s publicly available Security Practices document, Cloud Hosting and Delivery Policies, Global Customer Support Security Practices, Consulting Security Practices, and Advanced Customer Services Security Practices.

Cloud Vendor has standard terms and conditions that govern the use of Cloud Services that are publicly available and indicates the date of its most recent update. During the customer order process, customers are required to acknowledge the Cloud Vendor Cloud Services Agreement, which outlines customer responsibilities and Cloud Vendor’s responsibilities, objectives, and commitments. Amendments to the standard Cloud Vendor Cloud Services Agreement require advanced approval.

Cloud Vendor Cloud Infrastructure service release notes are publicly available. Incidents that cause a customer outage are reviewed and communicated to the impacted customer.

### Security Practices

Cloud Vendor has corporate security practices that encompass all the functions related to security, safety, and business continuity for Cloud Vendor’s internal operations and its provision of services to customers. These security practices include a suite of internal information security policies as well as customer -facing security practices that apply to different service lines.

Cloud Vendor’s security practices are designed to protect the confidentiality, integrity, and availability of both customer and Cloud Vendor data. Cloud Vendor continually works to strengthen and improve the security controls and practices for Cloud Vendor internal operations and ser vices offered to customers.

### Data Classification

When new service offerings are available to customers, the data gathered by the service is classified and documented according to the Cloud Vendor corporate policy. The Cloud Vendor Data Processing Agreement, which is publicly available, defines h ow to handle personal data. Additionally, the Cloud Vendor Services Privacy Policy describes the conditions under which Cloud Vendor may access, collect, and / or us e services data, which includes customers' development, test, or production environments. The policy is publicly available and indicates the date of the most recent update.

## Risk Assessment

Cloud Vendor values the necessary balance between risk and control and that the intent of risk management is to reduce risk to an acceptable level. Risk is integral to the p ursuit of value, which is a function of risk and return. Cloud Vendor seeks to manage risk exposures to incur just enough of the right kinds of risk to effectively pursue strategic goals.

Cloud Vendor BA&A conducts an annual Global Risk Assessment of key business pro cesses at Cloud Vendor. Upon request, members of management across the Company update their risk assessment of each process against two factors: likelihood of control / process issues a nd importance to business strategy. In addition, BA&A meets with senior management, Executive Committee members, the Finance and Audit Committee Chair, and the Board Chair to discuss Company risk.

The Cloud Vendor Cloud Infrastructure Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating/responding to, and monitoring risk specific to the Cloud Vendor Cloud Infrastructure organization. Risk assessments are performed annually across Cloud Vendor Cloud Infrastructure to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after National Institute of Standards and Technology (NIST) Special Publication 800 -30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO / IEC 27001:2013 standard. This includes ex ternal and internal risk factors such as new legislation, types of fraud, fraud incentives and pressures for employees, fraud opportunities and employee attitudes and rationalizations for fraud.

Risks are reviewed, assigned an owner, and remediated in line with the Cloud Vendor Cloud Infrastructure risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activities are collated and form inputs into Cloud Vendor Cloud Infrastructure’s risk assessment process.

## Monitoring

At least annually, Cloud Vendor Cloud Infrastructure completes an internal audit of the system. The internal audit is conducted by qualified auditors and as per the requirements set out in Clause 9 of ISO / IEC 27001:2013.

Cloud Vendor designed control activities in its day -to-day operations to support the Cloud Vendor Cloud Infrastructure environment. The sections below describe different control activities in various processes within Cloud Vendor Cloud Infrastructure.

## Significant Changes During the Period

No significant changes to the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system occurred during the period.

## Procedures

### Personnel Procedures

HR is a corporate function at Cloud Vendor. The controls in this section apply to the global employee population, including Cloud Vendor Cloud Infrastructure employees. HR uses several corporate HR management systems for their operations, and HR procedures vary according to local laws, regulations, and Vendor policies. HR representatives are assigned to business areas within Cloud Vendor.

Hiring of new employees – traditional new hire or through a merger or acquisition – occurs using formal procedures that follow corporate directives and in- country regulations and processes. A manager who needs a new employee accesses a HR self -service application, creates the job requisition, and forwards it to the Recruitment team for review and approval in accordance with the local process.

Cloud Vendor advertises job postings for a minimum of two weeks, in accordance with local policy. Submitted résumés or curricula vitae (CVs) are assessed and qualified candidates are selected for interviews. The hiring manager and a recruiter, if requested by the manager, initially interview potential candidates. Then multiple interviewers, selected based on their experience, role, and subject matter expertise, speak with the candidate regarding qualifications.

After a candidate has been identified, Cloud Vendor initiates the offer process using a formal Global Approval Matrix (GAM) that indicates the level of approval required for offers and transfers based on the terms of the transaction (e.g., position, salary). The HR recruitment team maintains this GAM. Cloud Vendor HR systems are configured to automatically route requests based on the terms specified in the GAM.

After a candidate is selected for the job opening, the candidate’s offer request is automatically routed using the GAM. On occasion, hiring approvals may also be obtained via email in accordance with the GAM.

Cloud Vendor, or a third party acting on behalf of Cloud Vendor, performs background checks on candidates selected for hire in accordance with local laws, regulations, and Cloud Vendor policies. Cloud Vendor’s supplier agreements require the suppliers of contract personnel to perform background screening of non -direct Cloud Vendor workers (sub-contractors) to the extent permitted by local laws, regulations, and Vendor policies before assigning them to Cloud Vendor. In the event a non- direct worker is hired as a direct Cloud Vendor employee, Cloud Vendor will re-perform the same location- based background checks on the individual. A candidate’s offer may be released contingent upon satisfactory completion of Cloud Vendor's pre -employment background check process.

After a candidate accepts the offer, local HR reviews the appropriate documents to ascertain an applicant’s right to work, in accordance with local laws and regulations and policy. HR requires each new employee to complete and sign a core set of new hire forms for their location, such as an employment agreement or equivalent and Propriety Information Agreement (PIA), prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local laws, regulations, and Cloud Vendor policies. Employees are assigned a job description upon hire that defines their role and the necessary qualifications for their position.

Cloud Vendor has developed an employee performance evaluation framework for use by its lines of business. Global HR supports the performance management process by providing guidance and tools to help facilitate individual and team success. The performance management process largely covers goal setting, continuous feedback and conversations with management, and performance evaluations. This process seeks to define what Cloud Vendor employees are expected to do, how work goals can be accomplished and how these contribute to the strategic objectives of the organization.

Cloud Vendor uses a formal process for terminations. For voluntary terminations, the manager is responsible for ensuring the voluntary termination action is initiated after an employee initiated his or her resignation. HR manages involuntary terminations. HR systems process involuntary terminations and issue automated notifications based on the effective date of termination. The recipient list for the alert includes all necessary parties, such as the employee’s manager and HR representative.

When an employee is terminated, Cloud Vendor HR updates the employee's status in the HR database and that data is then synchronized with the Cloud Vendor Cloud Infrastructure Permissions system using Cloud Vendor Corporate lightweight directory access protocol (LDAP). Permissions uses data attained from HR to revoke Cloud Vendor Cloud Infrastructure access for terminated personnel. When necessary, a person's access may be revoked in the Permissions system prior to HR processing their termination.

HR termination transactions are monitored quarterly to identify transactions where the termination date entered in the HR system is more than 14 days after the actual termination date. The risks associated with possible extended access are evaluated and risk mitigation performed, as needed. Documentation of review procedures and results are maintained in a secure Cloud Vendor repository.

### Operations

Cloud Vendor Cloud Infrastructure Operations is responsible for overall product availability. Cloud Vendor Cloud Infrastructure Operations includes the network operations; operations systems engineering; operations tooling; region build; operational readiness; security operations; infrastructure engineering; and customer operations areas of focus.

### System Monitoring

Documented incident response policies and procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities. The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team du ring the process. These policies and procedures are reviewed by senior management on at least an annual basis and are made available to employees via the corporate intranet.

Monitoring tools are used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds that impact availability and operational system metrics. Alerts received from the monitoring tools are recorded within a ticketing system and are assigned to IT and operations personnel for resolution. The ticketing system is utilized to manage system incidents, response, and resolution.

Patch management processes are in place to apply patches to production devices. Production devices are patched on at least an annual basis.

Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure services include a customer managed service. As part of this service offering, customers are responsible for the patching, maintenance, and monitoring of the service, including controls to help ensure that systems are maintained in a manner that helps ensure system availability. The computer operations controls described above are not applicable to customer managed service. The customer managed service is Big Data Cloud Service.

### Incident Response

Incidents are reported via MOS where SR tickets are generated and assigned to Cloud Vendor personnel for resolution. Each SR is assigned a severity level in order to direct the appropriate resources to issues depending on the impact to the customer and other system components. SR reports can be generated from MOS and are used by Cloud Vendor to determine volume, response time and resolution of reported incidents.

Cloud Vendor has documented escalation procedures that include conta ct and notification lists. The escalation procedures guide personnel to report failures, incidents, concerns, and other complaints to the appropriate individuals at Cloud Vendor and / or the customer.

### Disaster Recovery

Cloud Vendor maintains a Business Impact Analysi s (BIA) and Service Resiliency Plan (SRP) for each service. The plans outline procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and are reviewed annually. Cloud Vendor exercises each service’s SRP at least annually.

### Access Authentication and Authorization

Authentication to Cloud Vendor Identity Management (OIM), the production environment including databases, requires an authorized user account and password and occurs through the following procedures:

Δ Cloud services personnel attempting to access the OIM system are required to authenticate via an authorized user account and password. The OIM system is configured to enforce minimum password length and password complexity.

Δ Cloud services personnel attempting to access the production environment are required to connect via OCNA, which enforces two-factor authentication, including an individual token. Once users have authenticated successfully to OCNA, they are then required to authenticate to a bastion host utilizing a multifactor authentication process that includes YubiKey universal serial bus (USB) tokens. After connection to the bastion host has been established, users are able to authenticate to the production server operating systems via Secure Shell (SSH).

Δ Database users authenticate to the production databases after first establishing connections to OCNA, the bastion hosts, and the production server operation system. The database requires a user to have an authorized user account and password, which is granted via membership in the OIM / LDAP group. Therefore, access to the infrastructure and services supporting the in- scope systems requires multi -factor authentication, a VPN connection, SSH connection with a user account and password / private key, and a personal identification number (PIN) / Individual token generator.

Δ IDCS users authenticate to the production environment after first establishing connections to OCNA, then by having been provisioned the appropriate permissions from the Cloud Vendor Cloud Infrastructure Permissions access management system users log in to the bastion hosts using two -factor authentication, and then the production server operating system. After connection to the bastion host has been established, users are able to authenticate to the production server operating systems via SSH.

Administrative access within the OIM system, OCNA, bastion hosts, production server operating systems and databases is restricted to user accounts accessible by authorized IT and systems administration personnel. Administrative access within the Cloud Vendor Cloud

Infrastructure Permissions access management system is controlled by Cloud Vendor Cloud Infrastructure, who enforces the information n security controls described above.

Cloud Vendor Big Data Cloud Service – Compute Edition is considered a customer managed service. As part of this service offering, customers are responsible for the implementation, operation, and monitoring of the service, including controls to help ensure that system information is protected from unauthorized or unintentional use, modification, addition, or deletion. The information security controls described above are not applicable to this customer managed service.

### Access Requests and Access Revocation

Cloud Vendor GIS establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. These policies and procedures are made available to employees via the corporate intranet.

To grant user access a customized automated provisioning system, Cloud Vendor Identity Management system (OIM), is in place and configured to grant user access, upon request and approval from management to the production environment.

As part of the employee onboarding process, H R feeds new hire data to the OIM system which automatically provisions new employees an OIM system account. Once an OIM system account exists, employees and / or their managers can self-serve and request access to the VPN, Cloud Vendor Cloud Network Access (OCNA) and any production systems required to perform their job functions. The request requires approval by various levels of product management in OIM, depending on the access requested. The approval process is automated in OIM and is configured based on pre- defined rulesets: level one approval is required from the employees’ manager, level two approval from cloud operations senior management, and level three approval from security services. OIM automatically notifies product management via email when access requests are submitted and require approval. Additionally, OIM automatically provisions user access privileges once appropriate approvals are received, required trainings have been completed, and confidentiality agreements have been executed.

The ability to approve access to OCNA, bastion hosts, production server operating systems, and databases is restricted to user accounts accessible by authorized IT and operations management personnel. Subsequently, upon employee termination, HR feeds termination data to the OIM system which is configured to automatically revoke access to the production environment or Cloud Vendor Corporate LDAP which synchs to Cloud Vendor Cloud Infrastructure Permissions and revokes user access upon termination.

Continuous monitoring of employee access appropriateness occurs on a quarterly basis. Cloud operations personnel send email notifications to management personnel to initiate a network user access review for members within their organization. Management personnel are responsible for initiating changes to their employees’ access, as necessary. Additionally, user privileges to in- scope systems that are assigned to employees via the OIM system or Cloud Vendor Cloud Infrastructure Permissions are configured to expire at intervals that do not exceed 90 days. Users must submit an access request ticket following the standard user access administration process via OIM to have their access reinstated.

## Production Server Operating System Logging

Centralized logging is in place as a detective measure to identify inappropriate access and / or activities within the system. Production servers are configured to log authentication attempts, security administration and user commands on the operating system, which are then forwarded to a centralized security information and event monitoring (SIEM) solution in each region which ingests and stores security-related logs and alerts from networking devices, hosts, and other components within the infrastructure. Cloud Vendor Cloud Infrastructure’s Detection and Response team (DART) monitors the SIEM for event correlations and other relevant detection scenarios on a 24x7 basis to defend and protect against unauthorized intrusions and activity in the production environment.

## Network Security

Documented data communication policies and procedures are in place to guid e personnel in network security practices that include network device security, network device logging and monitoring, incident reporting and response, and remote access administration. These policies and procedures are reviewed by senior management on at least an annual basis and are made available to employees via the corporate intranet.

Network security monitoring is accomplished via the use of an IDS. An IDS is in place within the production network to analyze Internet traffic and report possible or actual network security breaches. The IDS is configured to alert network personnel of possible network security breaches. Network event logs from the IDS are available for review. A ticketing system is utilized to manage, track, and respond to system and network problems and incidents.

Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. A penetration test of the system is conducted at least annually. Operations and IT management personnel review and analyze the results of the vulnerability scans and penetration assessments and create remediation and mitigation plans where required.

To protect data while in transit, web servers utilize transport layer security (TLS) encryption for web communication sessions. Connections to a Cloud Vendor web-based cloud management console must be made over an encrypted protocol using hypertext transfer protocol secure (HTTPS) and TLS 1.2 or above.

## Change Management

Documented change management policies and procedures are in place to guide personnel in systems development, maintenance, and documentation of activities. These change management policies and procedures are applicable to configuration changes, software code, and patching.

Changes to infrastructure configurations and services supporting the in- scope systems are documented in a ticketing system, tested, peer reviewed and approved prior to release or deployment. After changes have been developed, code review is performed to verify that newly developed code satisfies the requested objective and that changes adhere to coding standards. Alongside code review, functional testing and / or regression testing is completed for changes. If testing is unsuccessful, the development team amends the change as needed before resubmitting to quality assurance (QA) personnel for a further round of testing. Once functional testing and / or regression testing has passed, change management leadership is responsible for providing final approval prior to the software change implementation.

Development and testing environments are separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. The source code management tool for services supporting the in -scope systems is configured to store current and prior versions of source code to support rollback to prior versions. Write access to the source code management tool is authenticated, restricted, and authorized to development personnel. Users are authenticated via an authorized user account and password before being granted access to the source code in the source code management tool. Additionally, changes to source code result in the creation of a new version of the software code. The ability to implement changes into the production environment is restricted to user accounts accessible by authorized IT and systems administration personnel.

Cloud Vendor Big Data Cloud Service – Compute Edition is considered a customer managed service. As part of this service offering, customers are responsible for the implementation, operation, and monitoring of this service. Cloud Vendor develops, tests, and approves changes for the service, and makes the changes available to customers in a centralized location; however, customers are responsible for implementing changes. The change management controls specific to implementing changes described above are not applicable to customer mana ged services.

## Complimentary Controls at User Entities

Cloud Vendor’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the applicable trust services criteria related to Vendor’s services to be solely achieved by Cloud Vendor’s control procedures. Accordingly, user entities, in conjunction with the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system and related services, should establish their own internal controls or procedures to complement those of Cloud Vendor.

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

| **COMPLEMENTARY USER ENTITY CONTROL** | **RELATED APPLICABLE TRUST SERVICES CRITERIA** |
| --- | --- |
| User entities are expected to implement controls that ensure data backup and restoration processes are in place to help ensure the recoverability of their data. | A1.2 |
| User entities are responsible for submitting incident tickets through the customer portal, MOS, and reviewing incident response details provided by Cloud Vendor. Customers should initiate inquiry or follow -up as appropriate. | CC7.3 CC7.4 CC7.5 |
| User entities are expected to implement controls that ensure the confidentiality of any user accounts and passwords assigned to them for use with Cloud Vendor’s systems. | CC6.1 CC6.2 |

| **COMPLEMENTARY USER ENTITY CONTROL** | **RELATED APPLICABLE TRUST SERVICES CRITERIA** |
| --- | --- |
| User entities are expected to implement controls that ensure they immediately notify Cloud Vendor of any actual or suspected information security breaches, including compromised user accounts. | CC6.3 |
| User entities are expected to implement controls that ensure the secure management of SSH keys for use with Cloud Vendor’s systems. | CC6.1 CC6.2 CC6.3 |

# SECTION IV – CLOUD VENDOR PAAS BUILT-ON CLOUD VENDOR CLOUD INFRASTRUCTURE CONTROLS, TEST PROCEDURES, AND RESULTS OF TESTING

## Scope of Testing

This report on the controls relates to the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system provided by Cloud Vendor. The scope of the testing was restricted to the Cloud Vendor PaaS Built -On Cloud Vendor Cloud Infrastructure system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period April 1, 2022, to March 31, 2023.

## Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

Δ The nature of the control and the frequency with which it operates;

Δ The control risk mitigated by the control;

Δ The effectiveness of entity -level controls, especially controls that monitor other controls;

Δ The degree to which the control relies on the effectiveness of other controls; and

Δ Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

| **TEST APPROACH** | **DESCRIPTION** |
| --- | --- |
| Inquiry | Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in- person interviews, telephone calls, emails, web-based conferences, or a combination of the preceding. |
| Observation | Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations re levant to the performance of control policies and procedures. |
| Inspection | Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.). |

## Sampling

Consistent with AICPA authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

## Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system -generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

## Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non -occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by user entities and subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the “Complementary Controls at User Entities” and “Subservice Organizations” sections, respectively, within Section 3.

## Security Category

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **Control Environment** | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | |
| CC1.1.1: Each new employee is required to complete and sign an employment agreement (or equivalent) and a PIA prior to or on the day of hire (or as otherwise required under applicable law) in accordance with local procedures, laws, and regulations. | Inquired of a principle regulatory compliance specialist regarding the employment agreement and the PIA to determine that each new employee was required to complete and sign an employment agreement (or equivalent) and a PIA prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local procedures, laws and regulations. | No exceptions noted. |
| Inspected the completed employment agreement and P IA documentation for a sample of employees hired during the period to determine that each employee sampled completed and signed an employment agreement and PIA. | No exceptions noted. |
| CC1.1.2: Employees are required to complete the Ethics and Business Conduct, IPA, and the Anti-Corruption and Foreign Corrupt Practices Act online courses upon hire. New hires who do not complete these courses in the allotted time frames are identified on an  exception list for follow -up by the Cloud Vendor Global Training Team. | Inquired of a princip regulatory compliance specialist regarding training requirements to determine that employees were required to complete the Ethics and Business Conduct, IPA, and  the Anti -Corruption and Foreign Corrupt Practices Act online courses upon hir e and new hires who did not complete these courses in the allotted time frames were identified on an exception list for follow-up by the Cloud Vendor Global Training Team. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the training documentation and evidence of Ethics and Business Conduct, IPA, and Anti-Corruption and Foreign Corrupt Practices Act training completion for a sample of employees hired during the period to determine that each employee sampled completed the Ethics and Business Conduct, IPA, and  the Anti-Corruption and Foreign Corrupt Practices Act online courses. | No exceptions noted. |
| Inspected the training exception report configurations and an example training exception report generated during the period to determine that new hires who did not complete the Ethics and Business Conduct, IPA, and the Anti-Corruption and Foreign Corrupt Practices Act online courses were identified on an exception list. | No exceptions noted. |
| CC1.1.3: Cloud Vendor performs background checks on candidates for hire in accordance with local laws and regulations as well as local Cloud Vendor policy. | Inquired of a HR manager regarding background checks to determine that Cloud Vendor performed background checks on candidates for hire in accordance with local laws and regulations as well as local Cloud Vendor policy. | No exceptions noted. |
| Inspected the completed background check documentation for a sample of employees hired during the period to determine that background checks were performed for each employee sampled. | No exceptions noted. |
| CC1.1.4: Per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers are required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies. Non -compliance with laws, regulations, and Cloud Vendor policies may result in disciplinary action up to and including termination.  Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process. | Inspected the Authority, Enforcement, Exceptions, and Violations Policy to determine that per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers were required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies and non- compliance with laws, regulations, and Cloud Vendor policies could result in disciplinary action up to and including termination and requests for an exception to an information security policy were required to be made as directed in the Corporate Security Exception  Management Process. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC1.2** COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
| CC1.2.1: The Cloud Vendor Corporation Board of Directors maintains a charter for the Committee on Independence Issues, which defines responsibilities and duties for evaluating the independence of members of the Board. | Inspected the board of directors’ charter to determine that the Cloud Vendor Corporation Board of Directors maintained a charter for the Committee on Independence Issues, which defined responsibilities and duties for evaluating the independence of members of the Board. | No exceptions noted. |
| Inspected the organizational charts to determine that members of the board of directors were independent of management and exercised oversight of the development and performance of internal control. | No exceptions noted. |
| CC1.2.2: Management personnel provide the results of external controls assessment reports to the board of directors on at least an annual basis.  Evidence of the board of director’s review is documented in the board of directors meeting minutes. | Inquired of a principal regulatory compliance specialist regarding board reviews of external controls assessment reports to determine that management personnel provided external controls assessment reports to the board of directors on at least an annual basis and evidence of the board of director’s review was documented in the board of directors meeting minutes. | No exceptions noted. |
| Inspected the board of directors’ meeting minutes evidencing the board review of external control assessment reports to determine that management personnel provided external controls assessment reports to the board of directors and that evidence of the board of director s’ review was documented in the board of directors meeting minutes during the period. | No exceptions noted. |
| **CC1.3** COSO Princip le 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
| CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of the system. | Inquired of a principal regulatory compliance specialist regarding the organizational structure to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of the system. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the organizational charts on the company intranet to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| CC1.3.2: Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inquired of a principal regulatory compliance specialist regarding employee job descriptions to determine that documented position descriptions were  in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | No exceptions noted. |
| Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled. | No exceptions noted. |
| CC1.3.3: GIS establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. | Inquired of a principal regulatory compliance specialist regarding information security policies and procedures to determine that GIS established and maint ained corporate information security policies and policies were reviewed and revised by GIS at least annually. | No exceptions noted. |
| Inspected the information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS during the period. | No exceptions noted. |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | |
| CC1.4.1: Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for p articular jobs. | Inquired of a principal regulatory compliance specialist regarding employee job descriptions to determine that documented position descriptions were  in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled. | No exceptions noted. |
| CC1.4.2: Training courses are available to new and existing employees to maintain and advance the skill level of personnel. | Inspected available training courses from Cloud Vendor University to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel. | No exceptions noted. |
| CC1.4.3: Per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers are required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies. Non -compliance with laws, regulations, and Cloud Vendor policies may result in disciplinary action up to and including termination.  Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process. | Inspected the Authority, Enforcement, Exceptions, and Violations Policy to determine that per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers were required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies and non- compliance with laws, regulations, and Cloud Vendor policies could result in disciplinary action up to and including termination and requests for an exception to an information security policy were required to be made as directed in the Corporate Security Exception Management Process. | No exceptions noted. |
| CC1.4.4: Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | Inquired of a principal regulatory compliance specialist regarding security awareness training to determine that employees were required to complete security training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| Inspected the training documentation and evidence of training completion for a sample of current employees to determine that security awareness training was completed during the period for each employee sampled. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC1.4.5: Cloud Vendor performs background checks on candidates for hire in accordance with local laws and regulations as well as local Cloud Vendor policy. | Inquired of a HR manager regarding background checks to determine that Cloud Vendor performed background checks on candidates for hire in accordance with local laws and regulations as well as local Cloud Vendor policy. | No exceptions noted. |
| Inspected the completed background check documentation for a sample of employees hired during the period to determine that background checks were performed for each employee sampled. | No exceptions noted. |
| **CC1.5** COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
| CC1.5.1: Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particu lar jobs. | Inquired of a principal regulatory compliance specialist regarding employee job descriptions to determine that documented position descriptions were  in place to define the skills, responsibilities, and knowledge levels required for particular job s. | No exceptions noted. |
| Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled. | No exceptions noted. |
| CC1.5.2: Per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers are required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies. Non -compliance with laws, regulations, and Cloud Vendor policies may result in disciplinary action up to and including termination.  Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process. | Inspected the Authority, Enforcement, Exceptions, and Violations Policy to determine that per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers were required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies and non- compliance with laws, regulations, and Cloud Vendor policies could result in disciplinary action up to and including termination and requests for an exception to an information security policy were required to be made as directed in the Corporate Security Exception Management Process. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC1.5.3: Management personnel provide the results of external controls assessment reports to the board of directors on at least an annual basis.  Evidence of the board of director’s review is documented in the board of directors meeting minutes. | Inquired of a principal regulatory compliance specialist regarding board reviews of external controls assessment reports to determine that management personnel provided external controls assessment reports to the board of directors on at least an annual basis and evidence of the board of director’s review was documented in the board of directors meeting minutes. | No exceptions noted. |
| Inspected the board of directors’ meeting minutes evidencing the board review of external control assessment reports to determine that management personnel provided external controls assessment reports to the board of directors and that evidence of the board of director s’ review was documented in the board of directors meeting minutes during the period. | No exceptions noted. |
| **Communication and Information** | | |
| **CC2.1** COSO Princip le 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | |
| CC2.1.1: The Information Security Policy outlines the principles to protect and manage the security of information assets in accordance with business, legal, regulatory, and contractual requirements, and obligations, as well as organizational objectives and strategic targets. | Inspected the Information Security Policy to determine that the Information Security Policy outlined the principles to protect and manage the security of information assets in accordance with business, legal, regulatory, and contractual requirements, and obligations, as well as organizational objectives and strategic targets. | No exceptions noted. |
| CC2.1.2: Monitoring tools are used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds that impact availability and operational system metrics. | Inspected the enterprise monitoring tool configurations to determine that monitoring tools were used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. | No exceptions noted. |
| Inspected the enterprise monitoring tool alert notification configurations and an example alert notification generated during the period to determine that the monitoring tools were configured to trigger alerts upon reaching or exceeding specified thresholds that impacted availability and operational system metrics. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC2.1.3: Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at lea st a quarterly basis. | Inquired of a principal regulatory compliance specialist regarding internal network vulnerability scans to determine that Cloud Vendor performed internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | No exceptions noted. |
| Inspected the network vulnerability scan reports for a sample of quarters during the period to determine that Cloud Vendor performed internal network vulnerability scans of the production network for each quarter sampled. | No exceptions noted. |
| CC2.1.4: A penetration test of the in - scope systems is conducted at least annually. | Inspected the results of the most recently completed penetration test to determine that a penetration test of the in -scope systems was conducted during the period. | No exceptions noted. |
| **CC2.2** COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | |
| CC2.2.1: Cloud Vendor requirements and operating procedures are documented and shared with relevant internal stakeholders. | Inspected the Cloud Vendor policies and procedures on the company intranet to determine that Cloud Vendor requirements and operating procedures were documented and shared with relevant internal stakeholders. | No exceptions noted. |
| CC2.2.2: Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to co mply with the corporate and business unit security policies. | Inquired of a principal regulatory compliance specialist regarding security awareness training to determine that employees were required to complete security training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| Inspected the training documentation and evidence of training completion for a sample of current employees to determine that security awareness training was completed during the period for each employee sampled. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC2.2.3: Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inquired of a principal regulatory compliance specialist regarding employee job descriptions to determine that documented position descriptions were  in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | No exceptions noted. |
| Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled. | No exceptions noted. |
| CC2.2.4: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, manag ing, and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team during the process. | Inspected the incident response policies and procedures to determine th at the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notificati on of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
| CC2.3.1: Cloud Vendor maintains a description of the in -scope services on the Cloud Vendor website. | Inspected the product descriptions on the Cloud Vendor external website to determine that Cloud Vendor maintained a description of  the in -scope services on the Cloud Vendor website. | No exceptions noted. |
| Inspected the Cloud Vendor Cloud Services Agreement and Cloud Vendor corporate security practices on the external website to determine that the entity’s security and availability commitments and the associated requirements were  document ed in externally facing customer documents. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC2.3.2: The process for external parties to report incidents to Cloud Vendor is outlined on the Cloud Vendor website. For Cloud Vendor customers and partners, MOS portal provides an interface to search for solutions, access support tools, and create service requests regarding the in -scope services. | Inspected the escalation procedures on the Cloud Vendor website to determine that the process for external parties to report incidents to Cloud Vendor was outlined on the Cloud Vendor website. | No exceptions noted. |
| Inspected the MOS portal to determine that the MOS portal provided an interface to search for solutions, access  support tools, and create service requests regarding the in -scope services. | No exceptions noted. |
| **Risk Assessment** | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risk s relating to objectives. | | |
| CC3.1.1: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the ach ievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |
| **CC3.2** COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | | |
| CC3.2.1: Production assets are tracked in an inventory system. | Inspected the in- scope system inventory listing to determine that production assets were tracked in an inventory system. | No exceptions noted. |
| CC3.2.2: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |
| **CC3.3** COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
| CC3.3.1: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
| CC3.4.1: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |
| CC3.4.2: Cloud Vendor monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. | Inquired of a principal regulatory compliance specialist regarding security monitoring to determine that Cloud Vendor monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management. | No exceptions noted. |
| Inspected an example security update and notification during the period to determine that Cloud Vendor monito red the security impact of emerging technologies during the period. | No exceptions noted. |
| **Monitoring Activities** | | |
| **CC4.1** COSO Principle 16: The entity selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning. | | |
| CC4.1.1: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy als o outlines the responsibilities of each team during the process. | Inspected the incident response policies and procedures to determine that the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification,  prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notification of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC4.1.2: The Cloud Vendor Corporation Board of Directors maintains a charter for the Committee on Independence Issues, which defines responsibilities and duties for evaluating the independence of members of the Board. | Inspected the board of directors’ chart er to determine that the Cloud Vendor Corporation Board of Directors maintained a charter for the Committee on Independence Issues, which defined responsibilities and duties for evaluating the independence of members of the Board. | No exceptions noted. |
| Inspected the organizational charts to determine that members of the board of directors were independent of management and exercised oversight of the development and performance of internal control. | No exceptions noted. |
| CC4.1.3: Management personnel provide the results of external controls assessment reports to the board of directors on at least an annual basis.  Evidence of the board of director’s review is documented in the board of directors meeting minutes. | Inquired of a principal regulatory compliance specialist regarding board reviews of external controls assessment reports to determine that management personnel provided external controls assessment reports to the board of directors on at least an annual basis and evidence of the board of director’s r eview was documented in the board of directors meeting minutes. | No exceptions noted. |
| Inspected the board of directors’ meeting minutes evidencing the board review of external control assessment reports to determine that management personnel provided external controls assessment reports to the board of directors and that evidence of the board of directors’ review was documented in the board of directors meeting minutes during the period. | No exceptions noted. |
| CC4.1.4: Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | Inquired of a principal regulatory compliance specialist regarding internal network vulnerability scans to determine that Cloud Vendor performed internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | No exceptions noted. |
| Inspected the network vulnerability scan reports for a sample of quarters during the period to determine that Cloud Vendor performed internal network vulnerability scans of the production network for each quarter sampled. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC4.1.5: A penetration test of the in - scope systems is conducted at least annually. | Inspected the results of the most recently completed penetration test to determine that a penetration test of the in-scope systems was conducted during the period. | No exceptions noted. |
| CC4.1.6: An internal audit of the in- scope systems is conducted by an independent party on an annual basis. Cloud Vendor evaluates and communicates internal control findings to those parties responsible for taking corrective action.  Findings are reviewed and tracked through resolution. | Inquired of a principal regulatory compliance specialist regarding internal audits to determine that an internal audit of the in -scope systems was conducted by an independent party on an annual basis and Cloud Vendor evaluated and communicated internal control findings to the parties responsible for taking action and findings were reviewed and tracked through resolution. | No exceptions noted. |
| Inspected the results of the most recently completed internal audit to determine  that an internal audit of the in-scope systems was conducted by an independent party during the period and Cloud Vendor evaluated and communicated internal control findings to the parties responsible for taking action and findings were reviewed and tracked through resolution. | No exceptions noted. |
| CC4.1.7: Cloud Vendor reviews in- scope data center provider attestation reports, or internationally recognized certifications, at least annually. Identified issues are evaluated and tracked through resolution. In the event that a site does not have an attestation report, or internationally recognized certification, Cloud Vendor performs an assessment annually of the site’s control environment, including physical security controls and environmental safeguards. | Inquired of a principal regulatory compliance specialist regarding data center vendor monitoring to determine that Cloud Vendor reviewed in -scope data center provider attestations reports, or internationally recognized certifications, at least annually and identified issues were evaluated and tracked through resolution and in the event that a site did not have an attestation report, or internationally recognized certification, Cloud Vendor performed an assessment annually of the site’s control environment, including physical security controls and environmental safeguards. | No exceptions noted. |
| Inspected the results of the most recently completed data center provider attestation report review to determine that Cloud Vendor reviewed in-scope data center provider attestation reports during the period and identified issues were evaluated and tracked through resolution. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC4.1.8: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was  performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed ris ks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC4.2** COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | | |
| CC4.2.1: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team during the process. | Inspected the incident response policies and procedures to determine that the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notification of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |
| CC4.2.2: An internal audit of the in- scope systems is conducted by an independent party on an annual basis. Cloud Vendor evaluates and communicates internal control findings to those parties responsible for taking corrective action.  Findings are reviewed and t racked through resolution. | Inquired of a principal regulatory compliance specialist regarding internal audits to determine that an internal audit of the in -scope systems was conducted by an independent party on an annual basis and Cloud Vendor evaluated and communicated internal control findings to the parties responsible for taking action and findings were reviewed and tracked through resolution. | No exceptions noted. |
| Inspected the results of the most recently completed internal audit to determine  that an internal audit of the in- scope systems was conducted by an independent party during the period and Cloud Vendor evaluated and communicated internal control findings to the parties responsible for taking action and findings were reviewed and tracked through resolution. | No exceptions noted. |
| CC4.2.3: Management personnel provide the results of external controls assessment reports to the board of directors on at least an annual basis.  Evidence of the board of director’s review is documented in the board of directors meeting minutes. | Inquired of a principal regulatory compliance specialist regarding board reviews of external controls assessment reports to determine that management personnel provided external controls assessment reports to the board of directors on at least an annual basis and  evidence of the board of director’s review was documented in the board of directors meeting minutes. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the board of directors’ meeting minutes evidencing the board review of external control assessment reports to determine that management personnel provided external controls assessment reports to the board of directors and that evidence of the board of directors’ review was documented in the board of directors meeting minutes during the perio d. | No exceptions noted. |
| **Control Activities** | | |
| **CC5.1** COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | |
| CC5.1.1: Documented policies and procedures are in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | Inspected the risk assessment policies and procedures to determine that  document ed policies and procedures were in place to guide personnel in selecting and developing control activities that contributed to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | No exceptions noted. |
| CC5.1.2: Risks related to services or data centers with an overall risk rating of high or critical are reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | Inspected the risk assessment  methodology and the results of the most recently completed risk assessment to determine that risks related to services or data centers with an overall risk rating of high or critical were reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk m anagement assessment program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that control activities, including general control activities over technology were selected and developed that contributed to the mitigation of risks to the achievement of objectives to acceptable levels. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | |
| CC5.2.1: Risks related to services or data centers with an overall risk rating of high or critical are reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that risks related to services or data centers with an overall risk rating of high or critical were reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that control activities, including general control activities over technology were selected and developed that contributed to the mitigation of risks to the achievement of objectives to acceptable levels. | No exceptions noted. |
| **CC5.3** COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
| CC5.3.1: Cloud Vendor requirements and operating procedures are documented and shared with relevant inter nal stakeholders. | Inspected the Cloud Vendor policies and procedures on the company intranet to determine that Cloud Vendor requirements and operating procedures were documented and shared with relevant internal stakeholders. | No exceptions noted. |
| CC5.3.2: GIS establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. | Inquired of a principal regulatory compliance specialist regarding information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS at least annually. | No exceptions noted. |
| Inspected the information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS during the period. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC5.3.3: Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | Inquired of a principal regulatory compliance specialist regarding security awareness training to determine that employees were required to complete security training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| Inspected the training documentation and evidence of training completion for a sample of current employees to determine that security awareness training was completed during the period for each employee sampled. | No exceptions noted. |
| CC5.3.4: Per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers are required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies. Non -compliance with laws, regulations, and Cloud Vendor policies may result in disciplinary action up to and including termination.  Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process. | Inspected the Authority, Enforcement, Exceptions, and Violations Policy to determine that per the Authority, Enforcement, Exceptions, and Violations Policy, Cloud Vendor employees and contingent workers were required to comply with laws, regulations, contractual obligations, and Cloud Vendor policies and non- compliance with laws, regulations, and Cloud Vendor policies could result in disciplinary action up to and including termination and requests for an exception to an information security policy were required to be made as directed in the Corporate Security Exception Management Process. | No exceptions noted. |
| CC5.3.5: Documented policies and procedures are in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in selecting and developing control activities that contributed to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **Logical and Physical Access Controls** | | |
| **CC6.1** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | | |
| CC6.1.1: GIS establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. | Inquired of a principal regulatory compliance specialist regarding information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS at least annually. | No exceptions noted. |
| Inspected the information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS during the period. | No exceptions noted. |
| CC6.1.2: User access requests are approved in the OIM system prior to access provisioning. | Inquired of a principal regulatory compliance specialist regarding the provisioning process for production system access to determine that user access requests were approved in the OIM system prior to access provisioning. | No exceptions noted. |
| Inspected the OIM production environment access reports and production environment approver user access listings for a sample of production environment user access requests processed during the period to determine that each user access request sampled was approved in the OIM system. | No exceptions noted. |
| CC6.1.3: Upon termination access to the in-scope systems is revoked. | Inspected the system production environment access removal reports and the production environment user access listings for a sample of employees terminated during the period to determine that upon termination of each terminated employee sampled, access to the in-scope systems was revoked. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC6.1.4: Cloud operations personnel send out an email notification to management personnel on a quarterly basis to perform a network user access review for members within their organization. | Inquired of a principal regulatory compliance specialist regarding the network user access review process to determine that cloud operations personnel sent an email notification to management personnel on a quarterly basis to perform a network user access review for members within their organization. | No exceptions noted. |
| Inspected the network user access review email notification configuration and the network user access review email notification for a sample of quarters during the period to determine that cloud operations personnel sent an email notification to management personnel for each quarter sampled. | No exceptions noted. |
| CC6.1.5: Users require an authorized user account and password in order to access  the OIM system. | Inspected the OIM system authentication configurations and user access listings to determine that users required an authorized user account and password in order to access the OIM system. | No exceptions noted. |
| CC6.1.6: The OIM system is configured to enforce minimum password length and password complexity for user accounts with access to the OIM system. | Inspected the OIM system authentication configurations to determine that the OIM system was configured to enforce minimum password length and password complexity for user accounts with access to the OIM system. | No exceptions noted. |
| CC6.1.7: Access to the infrastructure and services supporting the in -scope systems requires multi -factor authentication, a VPN connection, SSH connection with a user account and password / private key,  and a PIN / Individual token generator. | Inspected the OCNA authentication configurations and user access listing to determine that authentication to OCNA required users to connect via two -factor authentication that included the  following: | No exceptions noted. |
|  | Δ Authorized user account |  |
|  | Δ PIN |  |
|  | Δ Individual token generator |  |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the bastion host authentication configurations and user access listings for a sample of bastion hosts to determine  that authentication to each bastion host sampled required users to connect via two-factor authentication that included the following:  Δ Authorized user account  Δ PIN  Δ Individual token generator | No exceptions noted. |
| Inspected the operating system authentication configurations and user access listings for a sample of production servers to determine that authentication to the operating system required users to authenticate via an authorized user account and SSH private key pair for each server sampled. | No exceptions noted. |
| Inspected the database authentication configurations and user access listings for a sample of production databases to determine that authentication to the database required users to authenticate via an authorized user account and password for each database sampled. | No exceptions noted. |
| Inspected the VPN system configurations and user access listing to determine that  the VPN system was configured to require users to connect to the  production environment via a two -factor authentication that included the following:  Δ Authorized user account  Δ PIN  Δ YubiKey USB device | No exceptions noted. |
| CC6.1.8: Administrative access to in - scope systems is restricted to user accounts accessible by authorized IT and systems administration personnel. | Inspected the OIM system administrator user access listing with assistance of a principal regulatory compliance specialist to determine that administrative access within the OIM system was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the OCNA administrator user access listing with the assistance of a principal regulatory compliance specialist to determine that administrative access within OCNA was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |
| Inspected the bastion host administrator user access listings for a sample of bastion hosts with the assistance of a principal regulatory compliance specialist to determine that administrative access to each bastion host sampled was restricted to user accounts accessible by authorized IT and systems administ ration personnel. | No exceptions noted. |
| Inspected the operating system administrator user access listings for a sample of production servers with the assistance of a principal regulatory compliance specialist to determine that administrative access within the operating system was restricted to user accounts accessible by authorized IT and systems administration personnel for each server sampled. | No exceptions noted. |
| Inspected the database administrator user access listings for a sample of productio n databases with the assistance of a principal regulatory compliance specialist to determine that administrative access within the database was restricted to user accounts accessible by authorized IT and systems administration personnel for each database sampled. | No exceptions noted. |
| Inspected the VPN administrator user access listing with the assistance of a principal regulatory compliance specialist to determine that administrative access within the VPN system was restricted to user accounts accessible by authorized IT and system administration personnel. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC6.1.9: Authentication logs for production servers are configured to log authentication attempts, security administration and user commands on the operating system and then forwarded to a centralized log repository. | Inspected the logging configurations for a sample of production servers and an example log generated during the period to determine that each server sampled was configured to log authentication  attempts, security administration and user commands on the operating system and were then forwarded to the centralized log repository. | No exceptions noted. |
| **CC6.2** Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | | |
| CC6.2.1: User access requests are approved in the OIM system prior to access provisioning. | Inquired of principal regulatory compliance specialist regarding the provisioning process for production system access to determine that user access requests were approved in the OIM system prior to access provisioning. | No exceptions noted. |
| Inspected the OIM production environment access reports and production environment approver user access listings for a sample of production environment user access requests processed during the period to determine that each user access request sampled was approved in the OIM system. | No exceptions noted. |
| CC6.2.2: Upon termination access to the in-scope systems is revoked. | Inspected the system production environment access removal reports and the production environment user access listings for a sample of employees terminated during the period to determine that upon termination of each terminated employee samp led, access to the in -scope systems was revoked. | No exceptions noted. |
| CC6.2.3: Cloud operations personnel send out an email notification to management personnel on a quarterly basis to perform a network user access review for members within their organization. | Inquired of a principal regulatory compliance specialist regarding the network user access review process to determine that cloud operations personnel sent an email notification to management personnel on a quarterly basis to perform a networ k user access review for members within their organization. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the network user access review email notification configuration and the network user access review email notification for a sample of quarters during the period to determine that cloud operations personnel sent an email notification to management personnel for each quarter sampled. | No exceptions noted. |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and seg regation of duties, to meet the entity’s objectives. | | |
| CC6.3.1: User access requests are approved in the OIM system prior to access provisioning. | Inquired of principal regulatory compliance specialist regarding the provisioning process for production system access to determine that user access requests were approved in the OIM system prior to access provisioning. | No exceptions noted. |
| Inspected the OIM production environment access reports and production environment approver user access listings for a sample of production environment user access requests processed during the period to determine that each user access request sampled was approved in the OIM system. | No exceptions noted. |
| CC6.3.2: Upon termination access to the in-scope systems is revoked. | Inspected the system production environment access removal reports and the production environment user access listings for a sample of employees terminated during the period to determine that upon termination of each terminated employee sampled, access to the in -scope systems was revoked. | No exceptions noted. |
| CC6.3.3: Cloud operations personnel send out an email notification to management personnel on a quarterly basis to perform a network user access review for members within their organization. | Inquired of a principal regulatory compliance specialist regarding the network u ser access review process to determine that cloud operations personnel sent an email notification to management personnel on a quarterly basis to perform a network user access review for members within their organization. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected t he network user access review email notification configuration and the network user access review email notification for a sample of quarters during the period to determine that  cloud operations personnel sent an email notification to management personnel for each quarter sampled. | No exceptions noted. |
| CC6.3.4: Users require an authorized user account and password in order to access  the OIM system. | Inspected the OIM system authentication configurations and user access listings to determine that users required an authorized user account and password in order to access the OIM system. | No exceptions noted. |
| CC6.3.5: The OIM system is configured to enforce minimum password length and password complexity for user accounts with access to the OIM system. | Inspected the OIM system authentication configurations to determine that the OIM system was configured to enforce minimum password length and password complexity for user accounts with access to the OIM system. | No exceptions noted. |
| CC6.3.6: Access to the infrastructure and services supporting the in -scope systems requires multi -factor authentication, a VPN connection, SSH connection with a user account and password / private key,  and a PIN / Individual token generator. | Inspected the OCNA authentication configurations and user access listing to determine that authentication to OCNA required users to connect via two -factor authentication that included the  following: | No exceptions noted. |
|  | Δ Authorized user account |  |
|  | Δ PIN |  |
|  | Δ Individual token generator |  |
|  | Inspected the bastion host authentication configurations and user access listings for a sample of bastion hosts to determine  that authentication to each bastion host sampled required users to connect via two-factor authentication that included  the following: | No exceptions noted. |
|  | Δ Authorized user account |  |
|  | Δ PIN |  |
|  | Δ Individual token generator |  |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the operating system authentication configurations and user access listings for a sample of production servers to determine that authentication to the operating system required users to authenticate via an authorized user account and SSH private key pair for each server sampled. | No exceptions noted. |
| Inspected the database authentication configurations and user access listings for a sample of production databases to determine that authentication to the database required users to authenticate via an authorized user account and password for each database sampled. | No exceptions noted. |
| Inspected the VPN system configurations and user access listing to determine that  the VPN system was configured to require users to connect to the  production environment via a two -factor authentication that included the following:  Δ Authorized user account  Δ PIN  Δ YubiKey USB device | No exceptions noted. |
| CC6.3.7: Administrative access to in - scope systems is restricted to user accounts accessible by authorized IT and systems administration personnel. | Inspected the OIM system administrator user access listing with assistance of a principal regulatory compliance specialist to determine that administrative access within the OIM system was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |
| Inspected the OCNA administrator user access listing with the assistance of a principal regulatory compliance specialist to determine that administrative access within OCNA was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the bastion host administrator user access listings for a sample of bastion hosts with the assistance of a principal regulatory compliance specialist to determine that administrative access to each bastion host sampled was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |
| Inspected the operating system administrator user access listings for a sample of production servers with the assistance of a principal regulatory compliance specialist to determine that administrative access within the operating system was restricted to user accounts accessible by authorized IT and systems administration personnel for each server sampled. | No exceptions noted. |
| Inspected the database administrator user access listings for a sample of production databases with the assistance of principal regulatory compliance specialist to determine that administrative access  within the database was restricted to user accounts accessible by authorized IT and systems administration personnel for each database sampled. | No exceptions noted. |
| Inspected the VPN administrator user access listing with the assistance of a principal regulatory compliance specialist to determine that administrative access within the VPN system was restricted to user accounts accessible by authorized IT and system administration personnel. | No exceptions noted. |
| **CC6.4** 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. | | |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for restricting physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers. | | |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC6.5** The entity discontinues lo gical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives. | | |
| CC6.5.1: GIS establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. | Inquired of a principal regulatory compliance specialist regarding information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS at least annually. | No exceptions noted. |
| Inspected the information security policies and procedures to determine that GIS established and maintained corporate information security policies and policies were reviewed and revised by GIS during the period. | No exceptions noted. |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for restricting physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers. | | |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | |
| CC6.6.1: IDS is configured to alert network personnel of possible network security breaches. Network event logs from the IDS are available for review. | Inspected the IDS configurations and an example alert notification generated during the period to determine that an IDS was in place to analyze network device logs and alert network personnel of possible network security breaches. | No exceptions noted. |
| Inspected the IDS configurations and example network event logs generated during the period to determine that network event logs from the IDS were available for review. | No exceptions noted. |
| CC6.6.2: Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | Inquired of a principal regulatory compliance specialist regarding internal network vulnerability scans to determine that Cloud Vendor performed internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a qu arterly basis. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the network vulnerability scan reports for a sample of quarters during the period to determine that Cloud Vendor performed internal network vulnerability scans of the production network for each quarter sampled. | No exceptions noted. |
| CC6.6.3: A penetration test of the in - scope systems is conducted at least annually. | Inspected the results of the most recently completed penetration test to determine that a penetration test of the in -scope systems was conducted during the period. | No exceptions noted. |
| CC6.6.4: An encrypted VPN is required for remote access to the production environment to help ensure the security and integrity of the data passing over the public network. | Inquired of a principal regulatory compliance specialist regarding remote access to determine that an encrypted VPN was required for remote access to the production environment to help ensure the security and integrity of the data passing over the public network. | No exceptions noted. |
| Inspected the VPN encryption configurations to determine that an encrypted VPN was utilized for remote access. | No exceptions noted. |
| CC6.6.5: Connections to console must be made over an encrypted protocol using HTTPS and TLS 1.2. | Inspected the TLS encrypti on configurations to determine that connections to console were made over an encrypted protocol using HTTPS and TLS 1.2. | No exceptions noted. |
| Cloud Vendor Cloud Infrastructure is responsible for implementing logical access security measures to protect against threats from sources outside the boundaries of the system. | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and ex ternal users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives. | | |
| CC6.7.1: An encrypted VPN is required for remote access to the production environment to help ensure the security and integrity of the d ata passing over the public network. | Inquired of a principal regulatory compliance specialist regarding remote access to determine that an encrypted VPN was required for remote access to the production environment to help ensure the security and integrity of the data passing over the public network. | No exceptions noted. |
| Inspected the VPN encryption configurations to determine that an encrypted VPN was utilized for remote access. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC6.7.2: Connections to console must be made over an encrypted protocol using HTTPS and TLS 1.2. | Inspected the TLS encryption configurations to determine that connections to console were made over an encrypted protocol using HTTPS and TLS 1.2. | No exceptions noted. |
| **CC6.8** The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives. | | |
| CC6.8.1: Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | Inquired of a principal regulatory compliance specialist regarding security awareness training to determine that employees were required to complete security training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| Inspected the training documentation and evidence of training completion for a sample of current employees to determine that security awareness training was completed during the period for each employee sampled. | No exceptions noted. |
| CC6.8.2: The source code management tool for services supporting in -scope systems is configured to store current and prior versions of source code to support rollback to prior versions. Write access to the source code management tool is authenticated, restricted, and authorized to development personnel. | Inquired of a principal regulatory compliance specialist regarding the source code management tool to determine that the source code management tool for services supporting in-scope systems was configured to store current and prior versions of source code to support rollback to prior versions and write access to the source code management tool was authenticated,  restricted, and authorized to development personnel. | No exceptions noted. |
| Inspected the source code management tool configurations, authentication configurations, and version control activity logs generated during the period to determine that users were authenticated via an authorized user account and password before being granted access to the source code in the source code management tool and the source code management tool was configured to store current and prior versions of source code to support rollback to prior versions. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the listing of users with write access within the source code management tool with the assistance of principal regulatory compliance specialist to determine that write access to the source code management tool was restricted to authorized development personnel. | No exceptions noted. |
| CC6.8.3: The ability to implement changes into the production environment is restricted to user accounts accessible by authorized IT and systems administration personnel. | Inspected the listing of users with the ability to implement infrastructure configuration and software changes with the assistance of a principal regulatory compliance specialist to determine that the ability to implement software changes was restricted to user accounts accessible by authorized IT and systems administration personnel. | No exceptions noted. |
| **System Operations** | | |
| **CC7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | |
| CC7.1.1: Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | Inquired of a principal regulatory compliance specialist regarding internal network vulnerability s cans to determine that Cloud Vendor performed internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | No exceptions noted. |
| Inspected the network vulnerability scan reports for a sample of quarters during the period to determine that Cloud Vendor performed internal network vulnerability scans of the production network for each quarter sampled. | No exceptions noted. |
| CC7.1.2: A penetration test of the in - scope systems is conducted at least annually. | Inspected the results of the most recently completed penetration test to determine that a penetration test of the in -scope systems was conducted during the period. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of  malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed t o determine whether they represent security events. | | |
| CC7.2.1: Monitoring tools are used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds that impact availability and operational system metrics. | Inspected the enterprise monitoring tool configurations to determine that monitoring tools were used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. | No exceptions noted. |
| Inspected the enterprise monitoring tool alert notification configurations and an example alert notification generated during the period to determine that the monitoring tools were configured to trigger alerts upon reaching or exceeding specified thresholds that impacted availability and operational system metrics. | No exceptions noted. |
| CC7.2.2: Cloud Vendor performs internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | Inquired of a principal regulatory compliance specialist regarding internal network vulnerability scans to determine that Cloud Vendor performed internal network vulnerability scans of the production network to identify potential security vulnerabilities on at least a quarterly basis. | No exceptions noted. |
| Inspected the network vulnerability scan reports for a sample of quarters during the period to determine that Cloud Vendor performed internal network vulnerability scans of the production network for each quarter sampled. | No exceptions noted. |
| CC7.2.3: A penetration test of the in - scope systems is conducted at least annually. | Inspected the results of the most recently completed penetration test to determine that a penetration test of the in- scope systems was conducted during the period. | No exceptions noted. |
| CC7.2.4: IDS is configured to alert network personnel of possible network security breaches. Network event logs from the IDS are available for review. | Inspected the IDS configurations and an example alert notification generated during the period to determine that an IDS was in place to analyze network device logs and alert network personnel of possible network security breaches. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the IDS configurations and example network event logs generated during the period to determine that network event logs from the IDS were available for review. | No exceptions noted. |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for monitoring physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers. | | |
| **CC7.3** The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | | |
| CC7.3.1: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy a lso outlines the responsibilities of each team during the process. | Inspected the incident response policies and procedures to determine that the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notification of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |
| CC7.3.2: A ticketing system is utilized to manage system incidents, response, and resolution. | Inquired of a technical program manager regarding the incident management process to determine that a ticketing system was utilized to manage system incidents, response, and resolution. | No exceptions noted. |
| Inspected the ticketing system configurations and an example incident ticket resolved during the period to determine that a ticketing system was utilized. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | |
| CC7.4.1: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team during the process. | Inspected the incident response policies and procedures to determine that the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification,  prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notification of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |
| CC7.4.2: A ticketing system is utilized to manage system incidents, response, and resolution. | Inquired of a technical program manager regarding the incident management process to determine that a ticketing system was utilized to manage system incidents, response, and resolution. | No exceptions noted. |
| Inspected the ticketing system configurations and an example incident ticket resolved during the period to determine that a ticketing system was utilized. | No exceptions noted. |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
| CC7.5.1: The Cloud Vendor Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team during the process. | Inspected the incid ent response policies and procedures to determine that the Cloud Vendor Information Security Incident Reporting and Response Policy specified the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including notification of affected customers and the policy outlined the responsibilities of each team during the process. | No exceptions noted. |
| CC7.5.2: A ticketing system is utilized to manage system incidents, response, and resolution. | Inquired of a technical program manager regarding the incident management process to determine that a ticketing system was utilized to manage system incidents, response, and resolution. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the ticketing system configurations and an example incident ticket resolved during the period to determine that a ticketing system was utilized. | No exceptions noted. |
| **Change Management** | | |
| **CC8.1** The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | | |
| CC8.1.1: Documented change management policies and procedures are in place to guide personnel in systems development, maintenance, and documentation activities. | Inspected the change management policies and procedures to determine that documented change management policies and procedures were in place to guide personnel in systems development, maintenance, and documentation activities. | No exceptions noted. |
| CC8.1.2: Changes to infrastructure configurations and services supporting in-scope systems are documented in a ticketing system, tested, peer reviewed and approved prior to release or deployment. | Inquired of a principal regulatory compliance specialist regarding changes to infrastructure configurations and services supporting in- scope systems to determine that changes to infrastructure configurations and ser vices supporting in-scope systems were documented in a ticketing system, tested, peer reviewed and approved prior to release or deployment. | No exceptions noted. |
| Inspected the ticketing system dashboards and change request tickets for a sample of infrastructure configuration and software changes implemented during the period to determine that each change sampled was documented in a ticketing system, tested, peer reviewed, and approved. | No exceptions noted. |
| CC8.1.3: Development and testing environments are separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. | Inquired of a principal regulatory compliance specialist regarding the development and testing environments to determine that the development and testing environments were separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the development, test, and production environment IP addresses to determine that the development and testing environments were logically separated from the production environment. | No exceptions noted. |
| CC8.1.4: The source code management tool for services supporting in -scope systems is configured to store current and prior versions of source code to support rollback to prior versions. Write access to the source code management tool is authenticated, restricted, and authorized to development personnel. | Inquired of a principal regulatory compliance specialist regarding the source code management tool to determine that the source code management tool for services supporting in-scope systems was configured to store current and prior versions of source code to support rollback to prior versions and write access to the source code management tool was authenticated, restricted and authorized to development personnel. | No exceptions noted. |
| Inspected the source code management tool configurations, authentication configurations, and version control activity logs generated during the period to determine that users were authenticated via an authorized user account and password before being granted access to the source code in the source code management tool and the source code management tool was configured to store current and prior versions of source code to support rollback to prior versions. | No exceptions noted. |
| Inspected the listing of users with write access within the source code management tool with the ass istance of management personnel to determine that write access to the source code management tool was restricted to authorized development personnel. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC8.1.5: The ability to implement changes into the production environment is restricted to user accounts accessible by authorized IT and systems administration personnel. | Inspected the listing of users with the ability to implement infrastructure configuration and software changes for a sample of production servers and databases supporting the in -scope services with the assistance of a principal regulatory compliance specialist to determine that the ability to implement software changes was restricted to user accounts accessible by authorized IT and systems administration personnel for each production server and database sampled. | No exceptions noted. |
| CC8.1.6: Production devices are patched on at least an annual basis. | Inquired of a principal regulatory compliance specialist regarding the patch management process to determine that production devices were patched on at least an annual basis. | No exceptions noted. |
| Inspected the patch management history logs generated during the period for a sample of production servers to determine that operating system patches were deployed during the period for each server sampled. | No exceptions noted. |
| **Risk Mitigation** | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | |
| CC9.1.1: Documented policies and procedures are in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in selecting and developing control activities that contributed to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. | No exceptions noted. |
| CC9.1.2: Risk assessments ar e performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |
| CC9.1.3: Risks related to services or data centers with an overall risk rating of high or critical are reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that risks related to services or data centers with an overall risk rating of high or critical were reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that control activities, including general control activities over technology were selected and developed that contributed to the mitigation of risks to the achievement of objectives to acceptable levels. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC9.1.4: Cloud Vendor maintains a BIA and SRP for each service. The plans outline procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and are reviewed annually. | Inquired of a principal regulatory compliance specialist regarding BIA and SRP reviews to determine that Cloud Vendor maintained a BIA and SRP for each service and the plans outlined procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and were reviewed annually. | No exceptions noted. |
| Inspected the BIA and SRP for each in- scope service to determine that Cloud Vendor maintained a BIA and SRP for each service and the plans outlined procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and were reviewed during the period. | No exceptions noted. |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | |
| **CC9.2.1**: The Supplier Code of Ethics and Business Conduct and the Supplier and Physical Security Standards sets out the requirements that suppliers and vendors are required to adhere to. | Inspected the third -party management policies and procedures, the master service agreement template, the Supplier Information and Physical Security Standards the Supplier Security Management Policy to determine that the Supplier Code of Ethics and Business Conduct and the Supplier and Physical Security Standards set out the requirements that suppliers and vendors were required to adhere to. | No exceptions noted. |
| CC9.2.2: Cloud Vendor reviews in- scope data center provider attestation reports, or internationally recognized certifications, at least annually. Identified issues are evaluated and tracked through resolution. In the event that a site does not have an attestation report, or internationally recognized certification, Cloud Vendor performs an assessment annually of the site’s control environment, including physical security controls and environmental safeguards. | Inquired of a principal regulatory compliance specialist regarding data center vendor monitoring to determine that Cloud Vendor reviewed in -scope data center provider attestations reports, or internationally recognized certifications, at least annually and identified issues were evaluated and tracked through resolution and i n the event that a site did not have an attestation report, or internationally recognized certification, Cloud Vendor performed an assessment annually of the site’s control environment, including physical security controls and environmental safeguards. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the results of the most recently completed data center provider attestation report review to determine that Cloud Vendor reviewed in -scope data center provider attestation reports during the period and identified issues were evaluated and tracked through resolution. | No exceptions noted. |
| CC9.2.3: Risk assessments are performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. Risk checkpoints ensure critical service teams are directed to onboard to the Service Resiliency Program. | Inquired of a principal risk manager regarding the risk assessment process to determine that risk assessments were performed annually across Cloud Vendor to identify threats and risks that could impact the security, confidentiality, or availability of the in -scope systems and risk checkpoints ensured critical service teams were directed to onboard to the Service Resiliency Program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that a risk assessment was performed during the period for each in - scope service that identified threats and risks that could impact the security, confidentiality, or availability of the in - scope systems. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that the entity specified objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives, identified and assessed risks to the achievement of objectives, considered the potential for fraud, assessed changes that could significantly impact the system of internal control, assessed risks arising from potential business disruptions, and assessed risks associated with vendors and business partners as part of the risk assessment process during the period. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| CC9.2.4: Risks related to services or data centers with an overall risk rating of high or critical are reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that risks related to services or data centers with an overall risk rating of high or critical were reviewed, assigned an owner, and remediated in line with the Cloud Vendor risk management assessment program. | No exceptions noted. |
| Inspected the risk assessment methodology and the results of the most recently completed risk assessment to determine that control activities, including general control activities over technology were selected and developed that contributed to the mitigation of risks to the achievement of objectives to acceptable levels. | No exceptions noted. |

**Additional Criteria for Availability**

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
| **A1.1** The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | |
| A1.1.1: Monitoring tools are used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds tha t impact availability and operational system metrics. | Inspected the enterprise monitoring tool configurations to determine that monitoring tools were used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. | No exceptions noted. |
| Inspected the enterprise monitoring tool alert notification configurations and an example alert notification generated during the period to determine that the monitoring tools were configured to trigger alerts upon rea ching or exceeding specified thresholds that impacted availability and operational system metrics. | No exceptions noted. |
| A1.1.2: A ticketing system is utilized to manage system incidents, response, and resolution. | Inquired of a technical program manager regarding the incident management process to determine that a ticketing system was utilized to manage system incidents, response, and resolution. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the ticketing system configurations and an example incident ticket resolved during the period to determine that a ticketing system was utilized. | No exceptions noted. |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data b ack-up processes, and recovery infrastructure to meet its objectives. | | |
| A1.2.1: Monitoring tools are used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds that impact availability and operational system metrics. | Inspected the enterprise monitoring tool configurations to determine that monitoring tools were used to collect metrics relating to the status and load of network devices and servers supporting the in -scope services. | No exceptions noted. |
| Inspected the enterprise monitoring tool alert notification configurations and an example alert notification generated during the period to determine that the monitoring tools were configured to trigger alerts upon reaching or exceeding specified thresholds that impacted availability and operational system metrics. | No exceptions noted. |
| A1.2.2: A ticketing system is utilized to manage system incidents, response, and resolution. | Inquired of a technical program manager regarding the incident management process to determine that a ticketing system was utilized to manage system incidents, response, and resolution. | No exceptions noted. |
| Inspected the ticketing system configurations and an example incident ticket resolved during the period to determine that a ticketing system was utilized. | No exceptions noted. |
| A1.2.3: Cloud Vendor maintains a BIA and SRP for each service. The plans outline procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and are reviewed annually. | Inquired of a principal regulatory compliance specialist regarding BIA and SRP reviews to determine that Cloud Vendor maintained a BIA and SRP for each service and the plans outlined procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and were reviewed annually. | No exceptions noted. |

| **CONTROL ACTIVITY SPECIFIED BY THE SERVICE ORGANIZATION** | **TEST APPLIED BY THE SERVICE AUDITOR** | **TEST RESULTS** |
| --- | --- | --- |
|  | Inspected the BIA and SRP for each in- scope service to determine that Vendor maintained a BIA and SRP for each service and the plans outlined procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and were reviewed during the period. | No exceptions noted. |
| Cloud Vendor Cloud Infrastructure is responsible for monitoring data center hosting providers responsible for ensuring the data center facilities are equipped with environmental security safeguards and are utilizing environmental monitoring applications to monitor for environ mental events. | | |
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | |
| A1.3.1: Cloud Vendor exercises each service’s SRP at least annually. | Inquired of a principal regulatory compliance specialist regarding SRP testing to determine that Cloud Vendor exercised each service’s SRP at least annually. | No exceptions noted. |
| Inspected the results of the most recently completed SRP test for each in -scope service to determine that each in- scope service’s SRP was exercised duri ng the period. | No exceptions noted. |