# Zoom Video Communications, Inc.

# SOC 2 Report

For

Zoom Unified Communications Platform

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security and Availability and CCM Criteria

October 16, 2021, to October 15, 2022

Attestation and Compliance Services

Quality, above all.

This report is intended solely for use by the management of Zoom Video Communications, Inc., user entities of Zoom Video Communications, Inc.’s services, and other parties who have sufficient knowledge and understanding of Zoom Video Communications, Inc.’s services covered by this report (e3ach referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

# Table of Contents

Section 1 Independent Service Auditor's Report .................................................... 1

Section 2 Management's Assertion .................. 5

Section 3 Description of the System ................ 7

Section 4 Testing Matrices ............................... 22

Section 5 Other Information Provided by Zoom.................................................. 186

# Section I

## Independent Service Auditor's Report

# Independent Service Auditor's Report

To Zoom Video Communications, Inc.:

*Scope*

We have examined Zoom Video Communications, Inc.'s ("Zoom" or the "service organization") accompanying description of its Zoom Unified Communications Platform, in Section 3, throughout the period October 16, 2021, to October 15, 2022, (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 October 16, 2021, to October 15, 2022, to provide reasonable assurance that Zoom'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).* We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 4.0 control specifications ("CCM criteria") throughout the period October 16, 2021, to October 15, 2022.

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

The information included in Section 5, "Other Information Provided by Zoom" is presented by Zoom management to provide additional information and is not a part of the description. Information about Zoom's management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve the CCM criteria and the Zoom's service commitments and system requirements based on the applicable trust services criteria.

*Service Organization's Responsibilities*

Zoom 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 Zoom's service commitments, system requirements, and CCM criteria were achieved. Zoom has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Zoom 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 CCM 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. 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 CCM criteria were achieved and the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

*Inherent Limitations*

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the CCM criteria are achieved or 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:

a. the description presents Zoom's Unified Communications Platform that was designed and implemented throughout the period October 16, 2021, to October 15, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 16, 2021, to October 15, 2022, to provide reasonable assurance that the CCM criteria would be met and the Zoom'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 applied the complementary controls assumed in the design of Zoom's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 16, 2021, to October 15, 2022, to provide reasonable assurance that the CCM criteria were achieved, and Zoom's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Zoom'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 Zoom; user entities of Zoom's Unified Communications Platform during some or all of the period October 16, 2021, to October 15, 2022, business partners of Zoom subject to risks arising from interactions with the Zoom Unified Communications Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Schellman & Company, LLC

Tampa, Florida
December 19, 2022

# SECTION 2

## MANAGEMENT'S ASSERTION

# Management's Assertion

We have prepared the accompanying description of Zoom's Unified Communications Platform, in Section 3, throughout the period October 16, 2021, to October 15, 2022, (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 Zoom Unified Communications Platform that may be useful when assessing the risks arising from interactions with Zoom's system, particularly information about system controls that Zoom has designed, implemented, and operated to provide reasonable assurance that the criteria set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 4.0 control specifications ("CCM criteria") were achieved and Zoom'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)*.

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

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

a. the description presents Zoom's Unified Communications Platform that was designed and implemented throughout the period October 16, 2021, to October 15, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 16, 2021, to October 15, 2022, to provide reasonable assurance that the CCM criteria would be met and the Zoom'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 applied the complementary controls assumed in the design of Zoom's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 16, 2021, to October 15, 2022, to provide reasonable assurance that the CCM criteria were achieved, and the Zoom's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Zoom's controls operated effectively throughout that period.

# SECTION 3

## DESCRIPTION OF THE SYSTEM

# Overview of Operations

### Company Background

Founded in 2011, Zoom is a public company headquartered in San Jose, California, with over 6,000 employees. Zoom's Unified Communications (UCaaS) platform connects people through frictionless video, voice, chat, and content sharing and enables face-to-face video experiences across mobile devices, desktops, telephones, and room systems. Zoom's unified communications (UC) solves the challenge of juggling multiple tools by combining business communications such as telephony, instant messaging, and video conferencing on one streamlined platform.

### Description of Services Provided

The Zoom UCaaS platform unifies cloud video conferencing, simple online meetings, phone conferencing, chat, and a software-defined conference room solution into one platform. The system offers video, audio, chat, and wireless screen-sharing across Windows, Mac OS, Linux, Chrome OS, iOS, Android, Blackberry, Zoom Rooms, and H.323/Session Initiation Protocol (SIP) room systems. Zoom Products include:

- **Zoom Meetings** - a cloud-based collaboration service which includes video, audio, chat, content sharing and collaboration capabilities.
- **Zoom Team Chat** - a cloud-based chat service that allows users streamline communications between team members.
- **Zoom Phone** – includes business phone system features that enable employees to talk and interact in new ways anytime, anywhere.
- **Zoom Webinars** – host reliable and scalable online events with up to 100 interactive video participants and 10,000+ attendees.
- **Zoom Rooms** – software-based group video conferencing for conference and huddle rooms that run off-the-shelf hardware including a dedicated Mac or PC, camera, and speaker with an iPad controller.
- **Zoom Conference Room Connector** – a gateway allowing H.323 and SIP systems to connect to Zoom meetings. Room Connector is available in both cloud computing and as a virtual machine for installation on the customer premise.
- **Zoom API & SDKs** – provides the ability for developers to easily add Video, Voice and Screen Sharing to your application. The API is a server-side implementation designed around representational state transfer (REST). The Zoom API manages the pre-meeting experience such as creating, editing, and deleting resources like users, meetings, and webinars.

# Principal Service Commitments and System Requirements

*Principal Service Commitments*

The principal service commitments Zoom makes to customers related to security and availability are documented and communicated in the Zoom customer contracts. Specific customer commitments communicated by Zoom for protecting customer data include, but are not limited to, the following:

- Zoom will maintain reasonable physical and technical safeguards to prevent unauthorized disclosure of or access to Customer Content.
- Zoom will notify Customer if it becomes aware of unauthorized access to Customer Content, in accordance with applicable laws.

- Zoom will take reasonable and appropriate measures to protect against the loss, misuse, unauthorized access, and alteration of data.
- Zoom commits to maintain a 99.9% uptime availability (excluding excused downtime i.e., maintenance).

*System Requirements*

Zoom establishes operational and system requirements to support achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements include the implementation of logical access, mandatory user access reviews, risk and vulnerability management, system monitoring, incident action planning and detection, and security incident response procedures. Additional requirements are the necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

Such requirements are communicated in Zoom's system policies and standards, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected – these policies and supporting standards address how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed.

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.

## COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

**System Boundaries**

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

**Infrastructure and Software**

Zoom's production environments consist of multiple instances running Linux operating systems. Zoom utilizes various private colocation datacenters, along with Amazon Web Services (AWS) and Oracle Cloud Infrastructure (OCI) for data center and cloud hosting services of the production environment. Zoom utilizes industry standard hardware in redundant configurations to minimize service interruptions.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

| Primary Infrastructure | | |
|---|---|---|
| **Production Application** | **Business Function Description** | **Physical Location** |
| Configuration management tool | Used to propagate security and system configurations from a central repository to the production environment. | Available in each colocation/data center |
| VPN | Secure remote access to the production environment. | San Jose, California; Denver, Colorado; Kansas City, Kansas; Amsterdam, Netherlands |

**Primary Infrastructure**

| Production Application | Business Function Description | Physical Location |
|---|---|---|
| Firewall / AWS Security Groups | Protects production servers from unapproved connections, both inbound and outbound. | **<u>Firewall:</u>**<br>(Corporate)<br>San Jose, California<br>(Colocations)<br>Australia, Brazil, Canada, Germany, Hong Kong, India, Japan, Malaysia, Mexico, Netherlands, United States<br>**<u>AWS Security Groups:</u>**<br>Hosted in AWS |
| Security information and event management (SIEM) | SIEM. | AWS Elastic Compute Cloud (EC2) |
| Vulnerability Scanner | Used to scan for vulnerabilities within the production environment. | On-premises scanner in colocation/datacenter and agent on each host |
| AWS Aurora Relational Database Services (RDS) | A distributed relational database service. | Hosted in AWS |
| AWS DynamoDB | NoSQL database. | |
| AWS Simple Storage Service (S3) | File storage used to store and protect data. | |
| AWS CloudFront | Global Content Delivery (facilitates playback for recording). | |
| AWS Key Management System (KMS) | Amazon KMS creates and manages keys and controls the use of encryption across a wide range of AWS services applications. | |
| OCI | OCI is utilized to manage production servers to provision services. | Hosted in OCI |
| OCI Compute | OCI Compute service is utilized to create compute instances to deploy and applications. | |
| OCI Containers and Artifacts | OCI Container Engine for Kubernetes is used to define and create Kubernetes clusters to enable the deployment, scaling, and management of containerized applications.<br>OCI Container Registry is used to store, share, and manage development artifacts in an Oracle-managed registry. | |

**People**

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Information Security Personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure.
- Developers – responsible for the secure development and deployment of code for the Zoom UCaaS platform.
- IT Operations – responsible for administrative processes, and support for hardware and software, for both internal and external clients including the network infrastructure; server and device management.

**Procedures**

*Access, Authentication and Authorization*

AWS Virtual Private Cloud (VPC) security groups are configured to serve as a virtual firewall to restrict access to the application. Access to Zoom's production infrastructure hosted at AWS and at Zoom's colocation / data centers requires multi-factor authentication and access to servers hosted by AWS require secure shell (SSH) with private key utilizing a Zero-Trust authentication solution. Remote access to the data centers is only allowed through encrypted VPNs which utilize multi-factor authentication (MFA). Password controls such as minimum length, password history, password complexity, and account lockout settings are in place to reduce the risk of unauthorized activity. Zoom production systems utilize a Lightweight Directory Access Protocol system for authorized user access. Administrative access to the production systems are restricted to authorized personnel.

*Access Requests and Access Revocation*

Access to systems is role based and restricted to those who require access based on a business need. A formal provisioning process has been established for managing user accounts and controlling access to resources within the production environment. New employees are granted a standard level of access based on their role and a new hire ticket is used to guide the onboarding process. Prior to granting an individual access above the standard level of access, the specific system access must be added to the new hire ticket and approved by the designated approver(s).

The ability to create a new user or modify an existing user's access is limited to authorized personnel. Zoom has a formal offboarding process in place. Upon termination during the exit interview process, access to Zoom production systems, tools, and the network is removed in accordance with the policy. Zoom performs access reviews on a quarterly basis as a detective measure. In the event a user is terminated, a ticket is used to track and guide the termination process and help ensure the terminated user's logical and physical access is removed and/or disabled upon the individual's departure from the organization.

*Change Management*

Zoom's change management process establishes guidelines and standards to formally authorize, manage, test, document, monitor, and implement Zoom information system changes in the production environment. Documented policies and procedures are in place to guide personnel in the release management and change management process. A ticketing system is utilized to track and document application and system changes throughout the change management process. Proposed changes to production environments and applications require approval and testing prior to implementation into production. Backout procedures are documented for each change implementation to allow for rollback of changes when changes impair system operations.

Bi-weekly, a change management meeting is held to discuss, communicate, and approve the past, ongoing, and upcoming projects that affect the systems. Access privileges to promote application changes into the production environment are segregated from those with development responsibility and restricted to authorized personnel. The production environment is logically segmented from the development and test environments. In conjunction with Zoom's formal change management process, Zoom has established a formal software development lifecycle process that includes peer code review, testing, and security reviews, including static and dynamic analysis scans. Software also goes through a quality assurance process.

*Data Backup and Disaster Recovery*

Automated backup systems are in place to perform scheduled backups and/or geo-dispersed data center replication on at least a daily basis. The automated backup systems are configured to send alert notifications to infrastructure or operations engineering in the event of backup job completion or failure. Failover and restoration of backup files is performed as a component of business operations at least annually. Data is also replicated across geographically separate availability zones and stored in an encrypted format.

*Server Capacity Monitoring and Evaluation*

Management reviews availability trends and forecasts as compared to system commitments as a component of business operations as needed. The enterprise monitoring applications are configured to send alerts to operations personnel when predefined thresholds are exceeded.

*Disaster Recovery*

Disaster recovery plans are in place to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations. Disaster recovery plans are tested on an annual basis to ensure the system operation is in accordance with commitments and requirements. Failover and restoration of backup files are performed as a component of business operations on at least an annual basis.

*System Monitoring*

Formally documented standard build procedures for installation and maintenance of production servers and network devices are in place.

Monthly vulnerability assessments are performed to identify vulnerabilities and assess their potential impact to system security and availability. Identified vulnerabilities are tracked and monitored until mitigated. To provide additional insight into potential vulnerabilities, penetration tests of the production networks are performed by a third-party vendor on an annual basis to help ensure compliance with corporate policies. Securing the perimeter is a firewall system to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule.

In the event of a security incident, documented escalation procedures for reporting security and confidentiality incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints. Logging and monitoring software are configured to collect data from production servers to monitor system performance, potential security vulnerabilities, resource utilization and alert infrastructure operations personnel upon detection of usual system activity or service requests. Additionally, Zoom has implemented a next generation firewall which includes advanced threat protection to analyze network events and report possible or actual network security breaches and to alert security operations personnel when certain network security events are detected.

*Encryption*

Zoom encrypts customer data both in-transit and at-rest. Connections to the Zoom website utilize transport layer security (TLS) 1.3 where possible and 1.2 encryption and public key infrastructure (PKI) certificates issued by trusted commercial certificate authority. Through the web portal, individuals can access a range of features associated with their Zoom account, manage its operations, and integrate with other systems. The strength of encryption and specific ciphers used for connections to the website will depend on the browser used to access the site and the results of the common encryption method negotiated. When users connect to a meeting using the Zoom web client, leveraging web assembly, Zoom will send and receive meeting real-time content (video, voice, and content share) via UDP, directly from the meeting server encrypted with 256-bit AES-GCM. For at-rest data, Zoom utilizes AWS' SSE (Server Side Encryption) which, in the context of S3, uses AES-256 to encrypt data (e.g., recording files).

### Data

The following table describes the information used and supported by the system.

| Data Used and Supported by the System | | |
|---|---|---|
| **Data Description** | **Data Reporting** | **Classification** |
| Customer Data Processed by Zoom | Customer Content (i.e., customer recordings, customer transcriptions, any data shared by the customer through the use of Zoom's services / products) | Restricted |
| | • Customer Data (e.g., user account info, such as name, e-mail, address, phone, device ID, employer, meeting title, profile picture)<br>• Meeting metadata: metrics about end user meetings, e.g., when, and how meetings were conducted | Private |
| Operation Data | Technical information from Zoom's software or systems hosting the Services, and from the systems, applications and devices that are used to access the Services, such as:<br>• Production Logs – Internal-only and are not shared with customers<br>• Vulnerability Scans, Penetration Test Results – Internal-only and are not shared with customers | Confidential |

### Significant Changes During the Review Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

### Subservice Organizations

The data center hosting services provided by Digital Realty, Databank, eStruxture (formerly Aptum), Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, and Zayo and the cloud hosting services provided by AWS and OCI were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI alone or in combination with controls at Zoom, and the types of controls expected to be implemented at Digital Realty, Level 3, CoreSite, Aptum, Equinix, Telstra, Zayo, AWS, and OCI to achieve Zoom's service commitments and system requirements based on the applicable trust services criteria.

| Control Activities Expected to be Implemented by the Subservice Organizations | Applicable Trust Services Criteria |
|---|---|
| AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | CC6.1 – CC6.3,<br>CC6.5 – CC6.7,<br>CC7.1 – CC7.2 |
| Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | CC6.4 |
| Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | CC6.5 |
| AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | CC7.2 |
| AWS and OCI are responsible for ensuring capacity demand controls are in place to meet Zoom's availability commitments and requirements. | A1.1 |
| Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | A1.2 |

## Control Environment

The control environment at Zoom is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

### Integrity and Ethical Values

Integrity and ethical values are essential elements of Zoom's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Zoom's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

In order to maintain an atmosphere where these goals can be accomplished Zoom has provided a workplace where communications are open, and problems can be discussed and resolved in a mutually respectful atmosphere, considering individual circumstances and the individual employee. Zoom firmly believes that by communicating directly, difficulties that may arise can be resolved and that a mutually beneficial relationship can be developed.

Specific control activities that Zoom has implemented that demonstrate a commitment to integrity and ethical values are described below:

- Management formally documents and reviews the employee handbook on at least an annual basis that communicates entity values and commitments.
- A documented code of business conduct and ethics is in place to govern workplace behavior standards.
- Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources.
- Background screenings are performed for new employees for positions with access to non-public information as a component of the hiring process.

**Board of Directors and Audit Committee Oversight**

Zoom's control consciousness is influenced significantly by its board of directors. The board oversees organizational activities and meets on a formal and informal basis to discuss operations, ongoing and upcoming projects, operational concerns and strategic direction, and financial performance metrics. Specific control activities that Zoom has implemented that demonstrate that the board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control are described below:

- A board of directors' charter is in place that establishes board member responsibilities, mandates, for management oversight, and oversight of internal control.
- The board of directors, operating independently from management and exercising objectivity in evaluations and decision making, has established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance.
- Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the annual report for board review.

**Organizational Structure and Assignment of Authority and Responsibility**

Zoom's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing a relevant organizational structure includes consideration of key areas of authority, responsibility, and lines of reporting. Zoom develops an organizational structure suited to its needs which depends, in part, on its size and the nature of its activities.

Zoom's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at helping to ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that Zoom has implemented that demonstrate that management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives are described below:

- Organizational charts are in place to communicate the areas of authority, responsibility, and lines of reporting related to the design, implementation, operation, and maintenance of the system. The organizational charts are available and communicated to employees via the HR system and updated as needed.
- Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities.
- The responsibility for planning, implementing, operating, assessing, and improving the Information Security governance program is assigned to the Chief Information Security Officer (CISO).

### Commitment to Competence

Zoom defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific controls that Zoom has implemented that demonstrate a commitment to attract, develop, and retain competent individuals in alignment with objectives are described below:

- Training materials are available to new and existing employees to maintain and advance the skill level of personnel.
- Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies.
- Management monitors the completion of security awareness training for employees.
- Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities.

### Accountability

Zoom's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Zoom's human capital policies and practices relate to employee hiring, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Zoom has implemented that demonstrate accountability for internal control responsibilities in the pursuit of objectives are described below:

- Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities.
- Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures.
- The board of directors, operating independently from management and exercising objectivity in evaluations and decision making, has established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance.
- Management provides internal control performance metrics to the board of directors on an annual basis. These metrics are formally documented in the annual report for board review.

## Risk Assessment

### Objective Setting

Management holds quarterly business review meetings that discuss and align internal control responsibilities, performance measures and incentives with company business objectives. The CISO formally documents an organization strategy and updates it on at least an annual basis to align internal control responsibilities, performance measures and incentives with company business objectives. Management also formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's mission.

Management performs a risk assessment on at least an annual basis to identify, assess, and respond to information security risks. Documented policies and procedures are in place for conducting risk assessments and monitoring and responding to identified risks. The risk assessment includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies.

### Risk Identification and Analysis

Zoom has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to protect the confidentiality, integrity, and availability of customer data. A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review. Risks are reported to and reviewed by executive management in accordance with the company’s risk management standards. Beyond assessing the risks germane to hardware and software that comprise the cloud service offering, the organization continuously develops its understanding of the various challenges to the Zoom security posture through studying operational trends uncovered by automated vulnerability assessments of the production network, and annual network penetration testing.

### Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

*External Factors*

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

*Internal Factors*

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

### Risk Analysis

Risk analysis is an essential process to the entity’s success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Trust Services Criteria and Related Control Activities section below.

*Likelihood of Threat Occurrence*

Zoom's risk assessment assesses the likelihood that a given threat is capable of exploiting a given vulnerability (or vulnerabilities). The risk factor is determined by the likelihood of a threat event resulting in an adverse impact to the organization.

*Impact Analysis*

The impact magnitude for the risk assessment is guided by utilizing the potential exposure to Zoom, should the risk or the event occur. The impact of each threat identified is assigned to account for financial, compliance, operational effects to the business and reputational damage. The result of the likelihood and impact analysis will yield an overall risk rating.

### Potential for Fraud

A formal security risk assessment is performed on at least an annual basis that considers the potential for fraud and includes the evaluation of pressures, opportunities, and rationalization. Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures including fraudulent activity.

### Risk Mitigation

Commercial and professional liability insurance policies are in place to offset the financial impact of risks relating to security and availability commitments. Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. A security risk assessment is performed on at least an annual basis that includes an evaluation of risk mitigation control activities for risks to the confidentiality, integrity, and availability of data.

Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. The entity's established vendor requirements, scope of services, roles and responsibilities, and service levels are documented in vendor contracts. Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.

## Trust Services Criteria, CCM Criteria and Related Control Activities

### Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability categories and the requirements set forth in the CSA's CCM matrix version 3.0.1.

### Selection and Development of Control Activities

The applicable trust services criteria, CCM criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria, CCM criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Zoom's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

### Trust Services Criteria and CCM Criteria Not Applicable to the In-Scope System

The Trust Services criteria and CCM criteria presented below, are not applicable to the Zoom UCaaS platform within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted trust services criterion or CCM criteria. The following table presents the trust services criterion and CCM criteria that are not applicable for the Zoom UCaaS platform at Zoom. The not applicable trust services criteria are also described within Section 4.

| Criteria # | Reason for Omitted Criteria |
|---|---|
| CCC-02 | **Not applicable**. Zoom does not outsource development |
| IPY-02 | **Not applicable**. Customers maintain control over their access and any access to their data. |

## INFORMATION AND COMMUNICATION SYSTEMS

Zoom has implemented security awareness training to ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated. These include formal and informal training programs and the use of e-mail to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Zoom has systems and processes for detecting and managing fraud and security incidents. These methods include, but are not limited to, the following:

- Documented policies and standards are in place to set the minimum baseline requirements with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and standards are communicated to internal personnel via the company’s intranet.
- Employees are required to complete security awareness training, upon hire, and during the review period, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management monitors the completion of security awareness training for employees on an ongoing basis.
- Management formally documents and reviews the employee handbook on at least an annual basis that communicates entity values and commitments.
- Responsibility and accountability are defined through formal job descriptions.
- The engineering team sends release announcements to communicate planned changes to system components.
- Management holds quarterly business review meetings to discuss and align on internal control responsibilities, performance measures and incentives with company business objectives.

*External Communications*

Zoom has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in the use of their services and communication of significant events. These methods include, but are not limited to, the following:

- The entity’s security and availability commitments and the associated system requirements are documented in customer contracts.
- Guidelines for reporting failures, incidents, concerns, and other complaints are communicated to users via contractual terms.

- Information regarding the design and operation of the systems and its boundaries is communicated to external users via the company website.

## Monitoring

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

### Ongoing Monitoring

Operational and security metrics are tracked and reviewed on an ongoing basis. Monitoring includes, but is not limited to, progress on information security objectives and key results, risk assessment metrics, vulnerability metrics, patch compliance metrics, and incident metrics.

Zoom has deployed various intrusion detection system (IDS) / intrusion prevention system (IPS) and file integrity monitoring (FIM) tools within the production system to detect any anomalies or unusual activities. The IDS / IPS and FIM tools are configured to alert security personnel when certain security events are detected.

### Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the required competence and authority.

### Subservice Organization Monitoring

Zoom has a vendor due diligence program that includes assessing vendors against Zoom's privacy, security, compliance, financial and architectural requirements. Ongoing monitoring of Zoom's subservice organizations is conducted in accordance with the assessed risk.

Zoom incorporates relevant security and privacy obligations into its contractual agreements with subservice organizations. To facilitate ongoing monitoring, the company's standard privacy contractual provisions also include reporting requirements and audit rights.

### Internal and External Auditing

Zoom conducts various internal and external audits to assess the design and operating effectiveness of its control environment. Audit findings are tracked, and remediation plans are implemented in accordance with the company's standards.

### Evaluating and Communicating Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented by the self-assessors in an internal tracking tool, for management review. Deviations or deficiencies associated with controls with a level High risk assignment are immediately escalated to management for immediate corrective action. Other self-assessment results are reviewed within a week of the self-assessment test procedures, and corrective action, if required, is assigned to an individual and documented once those required actions are complete. Management reviews the deviations and corrective actions during the annual risk assessment meeting.

## Complementary Control Responsibilities at User Entities

Zoom’s controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the Zoom UCaaS platform and its controls, the following responsibilities should be considered by user entities:

| # | Customer Responsibility |
|---|---|
| 1. | Customers are responsible for ensuring that appropriate logging for security events is in place to support monitoring and incident response processes. |
| 2. | Customers are responsible for utilizing multi-factor authentication for controlling access to the Zoom UCaaS platform. |
| 3. | Customers are responsible for restricting access to the Zoom UCaaS platform in accordance with the principle of least privilege. |
| 4. | Customers are responsible for ensuring the Zoom UCaaS platform client is kept up-to-date with the most current release. |

# SECTION 4

## TESTING MATRICES

# Tests of Operating Effectiveness and Results of Tests

### Scope of Testing

This report on the controls relates to the Zoom Video Communications System provided by Zoom. The scope of the testing was restricted to the Zoom Video Communications System and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 16, 2021, to October 15, 2022.

### 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 and CCM criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- 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, e-mails, 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 relevant 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 American Institute of Certified Public Accountants (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 subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the "Subservice Organizations" section within Section 3.

## Audit and Assurance

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: A&A-01:** *Audit and Assurance Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| **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. | | | |
| **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. | | | |
| A&A-01.01 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained that defined the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A&A-01.02 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| A&A-01.03 | An information security management program is in place to guide employees and contractors in security practices and achievement of objectives. Security policies and standards are made available on the company intranet. | Inspected the information security policies and an example objective update to determine that an information security management program was in place to guide employees and contractors in security practices and achievement of objectives and that security policies and standards were made available on the company intranet. | No exceptions noted. |
| **CCM: A&A-02:** *Independent Assessments* - Conduct independent audit and assurance assessments according to relevant standards at least annually. | | | |
| **CC4.1** The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | | |
| A&A-02.01 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-02.02 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-02.03 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| A&A-02.04 | Independent audit and assurance assessments are performed according to risk-based plans and security policies. | Inspected the annual information security management system (ISMS) internal audit report to determine that independent audit and assurance assessments were performed according to risk-based plans and security policies. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A&A-02.05 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected the security meetings held for a sample of months to determine that security management meetings were held for each month sampled to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| **CCM: A&A-03:** *Risk Based Planning Assessment* - Perform independent audit and assurance assessments according to risk-based plans and policies. | | | |
| **CC4.1** The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | | |
| A&A-03.01 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| A&A-03.02 | Independent audit and assurance assessments are performed according to risk-based plans and security policies. | Inspected the annual ISMS internal audit report to determine that independent audit and assurance assessments were performed according to risk-based plans and security policies. | No exceptions noted. |
| A&A-03.03 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected the security meetings held for a sample of months to determine that security management meetings were held for each month sampled to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| **CCM: A&A-04:** *Requirements Compliance* - Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| A&A-04.01 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A&A-04.02 | Independent audit and assurance assessments are performed according to risk-based plans and security policies. | Inspected the annual ISMS internal audit report to determine that independent audit and assurance assessments were performed according to risk-based plans and security policies. | No exceptions noted. |
| A&A-04.03 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected the security meetings held for a sample of months to determine that security management meetings were held for each month sampled to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| **CCM: A&A-05:** *Audit Management Process* - Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| **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. | | | |
| A&A-05.01 | Penetration testing is conducted by an independent third party on an annual basis.  Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-05.02 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-05.03 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| A&A-05.04 | Independent audit and assurance assessments are performed according to risk-based plans and security policies. | Inspected the annual ISMS internal audit report to determine that independent audit and assurance assessments were performed according to risk-based plans and security policies. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A&A-05.05 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected the security meetings held for a sample of months to determine that security management meetings were held for each month sampled to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| **CCM: A&A-06:** *Remediation* - Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders. | | | |
| **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. | | | |
| A&A-06.01 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-06.02 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| A&A-06.03 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| A&A-06.04 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected the security meetings held for a sample of months to determine that security management meetings were held for each month sampled to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |

# Application and Interface Security

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: AIS-01:** *Application and Interface Security Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| **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. | | | |
| **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. | | | |
| AIS-01.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| AIS-01.02 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | No exceptions noted. |
| AIS-01.03 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained that defined the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| AIS-01.04 | The entity’s security, availability, and privacy commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual non-disclosure agreement (NDA), and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-01.05 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that a documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| **CCM: AIS-02:** *Application Security Baseline Requirements* - Establish, document and maintain baseline requirements for securing different applications. | | | |
| **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. | | | |
| **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. | | | |
| **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. | | | |
| AIS-02.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| AIS-02.02 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | No exceptions noted. |
| AIS-02.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| AIS-02.04 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-02.05 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via file integrity monitoring (FIM). | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| AIS-02.06 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. These policies and procedures are communicated to internal personnel via the company intranet. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation and that the policies and procedures were communicated to internal personnel via the company intranet. | No exceptions noted. |
| AIS-02.07 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| AIS-02.08 | Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures. | Inspected the employee handbook to determine that policies were documented and maintained that addressed disciplinary actions for lack of compliance with policies, standards, and procedures. | No exceptions noted. |
| **CCM: AIS-03:** *Application Security Metrics* - Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| AIS-03.01 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| AIS-03.02 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-03.03 | Penetration testing is conducted by an independent third party on an annual basis.  Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| AIS-03.04 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| **CCM: AIS-04:** *Secure Application Design and Development* - Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. | | | |
| **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. | | | |
| **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. | | | |
| AIS-04.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| AIS-04.02 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | No exceptions noted. |
| AIS-04.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-04.04 | Production system, application, and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| AIS-04.05 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| **CCM: AIS-05:** *Automated Application Security Testing* - Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals.  Automate when applicable and possible. | | | |
| **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. | | | |
| **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. | | | |
| AIS-05.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| AIS-05.02 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | No exceptions noted. |
| AIS-05.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-05.04 | Production system, application, and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| AIS-05.05 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| AIS-05.06 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |
| **CCM: AIS-06:** *Automated Secure Application Deployment* - Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment.  Automate where possible. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| AIS-06.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| AIS-06.02 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-06.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| AIS-06.04 | Production system, application, and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| AIS-06.05 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| **CCM: AIS-07:** *Application Vulnerability Remediation* - Define and implement a process to remediate application security vulnerabilities, automating remediation when possible. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| **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. | | | |
| AIS-07.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-07.02 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| AIS-07.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| AIS-07.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| AIS-07.05 | Policies and standards are in place for identifying and remediating vulnerabilities in production operation systems. | Inspected the automated patching tool configuration and an example patch applied during the period to determine that policies and standards were in place for identifying and remediating vulnerabilities in production operation systems. | No exceptions noted. |
| AIS-07.06 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| AIS-07.07 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| AIS-07.08 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

## Business Continuity Management & Operational Resilience

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: BCR-01:** *Business Continuity Management Policies and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| BCR-01.01 | Policies and standards are documented and maintained defining the requirements for business continuity management and operational resilience. | Inspected the business continuity plan to determine that policies and standards were documented and maintained that defined the requirements for business continuity management and operational resilience. | No exceptions noted. |
| BCR-01.02 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| BCR-01.03 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-01.04 | Policies and procedures are in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | Inspected the data retention policy to determine that policies and procedures were in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | No exceptions noted. |
| BCR-01.05 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |
| BCR-01.06 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation.  These policies and procedures are communicated to internal personnel via the company intranet. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation and that the policies and procedures were communicated to internal personnel via the company intranet. | No exceptions noted. |
| BCR-01.07 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| BCR-01.08 | Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures. | Inspected the employee handbook to determine that policies were documented and maintained that addressed disciplinary actions for lack of compliance with policies, standards, and procedures. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom’s availability commitments and requirements. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: BCR-02:** *Risk Assessment and Impact Analysis* - Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| **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. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| BCR-02.01 | Business continuity plans are tested on an annual basis or upon significant changes to the document and lessons learned are documented in the summary report. | Inspected the results of the most recent tabletop exercise to determine that business continuity plans were tested during the period and lessons learned were documented in the summary report. | No exceptions noted. |
| BCR-02.02 | Disaster recovery plans are tested on an annual basis to help ensure the system operation is in accordance with commitments and requirements. | Inspected evidence of the most recently completed disaster recovery plan testing to determine that disaster recovery plans were tested during the period to help ensure the system operation was in accordance with commitments and requirements. | No exceptions noted. |
| BCR-02.03 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| BCR-02.04 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| BCR-02.05 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-02.06 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| BCR-02.07 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that a documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| BCR-02.08 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: BCR-03:** *Business Continuity Strategy* - Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| BCR-03.01 | Policies and standards are documented and maintained defining the requirements for business continuity management and operational resilience. | Inspected the business continuity plan to determine that policies and standards were documented and maintained that defined the requirements for business continuity management and operational resilience. | No exceptions noted. |
| BCR-03.02 | Policies and procedures are in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | Inspected the data retention policy to determine that policies and procedures were in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-03.03 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |
| BCR-03.04 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| BCR-03.05 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| BCR-03.06 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that a documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| BCR-03.07 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: BCR-04:** *Business Continuity Planning* - Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| BCR-04.01 | Policies and standards are documented and maintained defining the requirements for business continuity management and operational resilience. | Inspected the business continuity plan to determine that policies and standards were documented and maintained that defined the requirements for business continuity management and operational resilience. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-04.02 | Policies and procedures are in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | Inspected the data retention policy to determine that policies and procedures were in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | No exceptions noted. |
| BCR-04.03 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |
| BCR-04.04 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| BCR-04.05 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| BCR-04.06 | Business continuity plans are tested on an annual basis or upon significant changes to the document and lessons learned are documented in the summary report. | Inspected the results of the most recent tabletop exercise to determine that business continuity plans were tested during the period and lessons learned were documented in the summary report. | No exceptions noted. |
| BCR-04.07 | Disaster recovery plans are tested on an annual basis to help ensure the system operation is in accordance with commitments and requirements. | Inspected evidence of the most recently completed disaster recovery plan testing to determine that disaster recovery plans were tested during the period to help ensure the system operation was in accordance with commitments and requirements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-04.08 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom’s availability commitments and requirements. | | |
| **CCM: BCR-05:** *Documentation* - Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically. | | | |
| **CC2.1** COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| **PI1.1** The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | | |
| BCR-05.01 | Policies and standards are documented and maintained defining the requirements for business continuity management and operational resilience. | Inspected the business continuity plan to determine that policies and standards were documented and maintained that defined the requirements for business continuity management and operational resilience. | No exceptions noted. |
| BCR-05.02 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| BCR-05.03 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| BCR-05.04 | Policies and procedures are in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | Inspected the data retention policy to determine that policies and procedures were in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-05.05 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |
| BCR-05.06 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| **CCM: BCR-06:** *Business Continuity Exercises* - Exercise and test business continuity and operational resilience plans at least annually or upon significant changes. | | | |
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| BCR-06.01 | Business continuity plans are tested on an annual basis or upon significant changes to the document and lessons learned are documented in the summary report. | Inspected the results of the most recent tabletop exercise to determine that business continuity plans were tested during the period and lessons learned were documented in the summary report. | No exceptions noted. |
| | Disaster recovery plans are tested on an annual basis to help ensure the system operation is in accordance with commitments and requirements. | Inspected evidence of the most recently completed disaster recovery plan testing to determine that disaster recovery plans were tested during the period to help ensure the system operation was in accordance with commitments and requirements. | No exceptions noted. |
| | IT personnel perform failover and restoration of backup files as a component of business operations on at least an annual basis. | Inspected the database testing report to determine that IT personnel performed failover and restoration of backup files as a component of business operations during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: BCR-07:** *Communication* - Establish communication with stakeholders and participants in the course of business continuity and resilience procedures. | | | |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| BCR-07.01 | Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website. | Inspected the company website overview page to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website. | No exceptions noted. |
| BCR-07.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| BCR-07.03 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that a documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| BCR-07.04 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| **CCM: BCR-08:** *Backup* - Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| BCR-08.01 | IT personnel perform failover and restoration of backup files as a component of business operations on at least an annual basis. | Inspected the database testing report to determine that IT personnel performed failover and restoration of backup files as a component of business operations during the period. | No exceptions noted. |
| BCR-08.02 | Data is replicated across geographically separate availability zones. | Inspected the data replication configurations to determine that data was replicated across geographically separate availability zones. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: BCR-09:** *Disaster Response Plan* - Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **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. | | | |
| BCR-09.01 | Policies and standards are documented and maintained defining the requirements for business continuity management and operational resilience. | Inspected the business continuity plan to determine that policies and standards were documented and maintained that defined the requirements for business continuity management and operational resilience. | No exceptions noted. |
| BCR-09.02 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| BCR-09.03 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| BCR-09.04 | Policies and procedures are in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | Inspected the data retention policy to determine that policies and procedures were in place to support business processes and technical measures implemented and to define and adhere to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. | No exceptions noted. |
| BCR-09.05 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-09.06 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: BCR-10:** *Response Plan Exercise* - Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities. | | | |
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| BCR-10.01 | Business continuity plans are tested on an annual basis or upon significant changes to the document and lessons learned are documented in the summary report. | Inspected the results of the most recent tabletop exercise to determine that business continuity plans were tested during the period and lessons learned were documented in the summary report. | No exceptions noted. |
| BCR-10.02 | Disaster recovery plans are tested on an annual basis to help ensure the system operation is in accordance with commitments and requirements. | Inspected evidence of the most recently completed disaster recovery plan testing to determine that disaster recovery plans were tested during the period to help ensure the system operation was in accordance with commitments and requirements. | No exceptions noted. |
| BCR-10.03 | IT personnel perform failover and restoration of backup files as a component of business operations on at least an annual basis. | Inspected the database testing report to determine that IT personnel performed failover and restoration of backup files as a component of business operations during the period. | No exceptions noted. |
| **CCM: BCR-11:** *Equipment Redundancy* - Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **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. | | | |
| BCR-11.01 | Data is replicated across geographically separate availability zones. | Inspected the data replication configurations to determine that data was replicated across geographically separate availability zones. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| BCR-11.02 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |

## Change Control and Configuration Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CCC-01:** *Change Management Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually. | | | |
| **CC3.1** The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| **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. | | | |
| CCC-01.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| CCC-01.02 | Backout procedures are documented for system, application, and maintenance changes to allow for the rollback of changes that impair system operation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that backout procedures were documented for system, application, and maintenance changes to allow for the rollback of changes that impaired system operation for each change sampled. | No exceptions noted. |
| CCC-01.03 | Policies and standards for the secure disposal of equipment are documented and maintained. | Inspected the data classification and media disposal policies to determine that policies and standards for the secure disposal of equipment were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CCC-01.04 | Documented change management policies and procedures are in place to guide personnel in monitoring outsourced development and to help ensure code review is performed by Zoom management for code developed by external business partners. | Inspected the change management policies and procedures to determine that documented change management policies and procedures were in place to guide personnel in monitoring outsourced development and to help ensure code review was performed by Zoom management for code developed by external business partners. | No exceptions noted. |
| **CCM: CCC-02:** *Quality Testing* - Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards. | | | |
| **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. | | | |
| CCC-02.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| CCC-02.02 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| CCC-02.03 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| CCC-02.04 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CCC-03:** *Change Management Technology* - Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). | | | |
| **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. | | | |
| CCC-03.01 | A change management meeting is held weekly to discuss and communicate the ongoing and upcoming projects that affect the system. | Inspected the meeting minutes for a sample of change management meetings held during the period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affect the system for each week sampled. | No exceptions noted. |
| CCC-03.02 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| CCC-03.03 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| CCC-03.04 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |
| CCC-03.05 | Test and development environments do not use live production data. | Inspected the release procedure and example test data to determine that test and development environments did not use live production data. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CCC-04:** *Unauthorized Change Protection* - Restrict the unauthorized addition, removal, update, and management of organization assets. | | | |
| **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. | | | |
| CCC-04.01 | The system is configured to automatically enforce peer review and approval for software changes prior to implementation into the production environment. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that the system was configured to automatically enforce peer review and approval for application changes to be reviewed prior to implementation into the production environment for each change sampled. | No exceptions noted. |
| CCC-04.02 | Version control software is utilized to restrict access to application source code and provide rollback capabilities. | Inspected the branch directory to determine that version control software was utilized to restrict access to application source code and provide rollback capabilities. | No exceptions noted. |
| CCC-04.03 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inspected the listing of users with ability to promote production changes and the user access review performed for a sample of quarters during the period to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| CCC-04.04 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |
| **CCM: CCC-05:** *Change Agreements* - Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs. | | | |
| **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. | | | |
| CCC-05.01 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CCC-05.02 | The system is configured to automatically enforce peer review and approval for software changes prior to implementation into the production environment. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that the system was configured to automatically enforce peer review and approval for application changes to be reviewed prior to implementation into the production environment for each change sampled. | No exceptions noted. |
| **CCM: CCC-06:** *Change Management Baseline* - Establish change management baselines for all relevant authorized changes on organization assets. | | | |
| **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. | | | |
| CCC-06.01 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| CCC-06.02 | A change management meeting is held weekly to discuss and communicate the ongoing and upcoming projects that affect the system. | Inspected the change release meeting minutes for a sample of weeks during the period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled. | No exceptions noted. |
| CCC-06.03 | The system is configured to automatically enforce peer review and approval for software changes prior to implementation into the production environment. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that the system was configured to automatically enforce peer review and approval for application changes to be reviewed prior to implementation into the production environment for each change sampled. | No exceptions noted. |
| CCC-06.04 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inspected the listing of users with ability to promote production changes and the user access review performed for a sample of quarters during the period to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CCC-06.05 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| **CCM: CCC-07:** *Detection of Baseline Deviation* - Implement detection measures with proactive notification in case of changes deviating from the established baseline. | | | |
| **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. | | | |
| CCC-07.01 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| CCC-07.02 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| **CCM: CCC-08:** *Exception Management* - Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process.  Align the procedure with the requirements of GRC-04: Policy Exception Process. | | | |
| **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. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| **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. | | | |
| **C9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| CCC-08.01 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CCC-08.02 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| CCC-08.03 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |
| CCC-08.04 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| **CCM: CCC-09:** *Change Restoration* - Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns. | | | |
| **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. | | | |
| CCC-09.01 | Backout procedures are documented for system, application, and maintenance changes to allow for the rollback of changes that impair system operation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that backout procedures were documented for system, application, and maintenance changes to allow for the rollback of changes that impaired system operation for each change sampled. | No exceptions noted. |
| CCC-09.02 | Version control software is utilized to restrict access to application source code and provide rollback capabilities. | Inspected the rollback and branch protection rules to determine that version control software was utilized to restrict access to application source code and provide rollback capabilities. | No exceptions noted. |

## Cryptography, Encryption and Key Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CEK-01:** *Encryption and Key Management Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| CEK-01.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-01.02 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and bring your own device (BYOD) policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: CEK-02:** *CEK Roles and Responsibilities* - Define and implement cryptographic, encryption and key management roles and responsibilities. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-02.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CEK-02.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| CEK-02.03 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| **CCM: CEK-03:** *Data Encryption* - Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards. | | | |
| **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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| CEK-03.01 | Backups of in-scope systems are encrypted. | Inspected the automated backup system encryption configurations for a sample of database clusters to determine that backups of in-scope systems were encrypted for each database cluster sampled. | No exceptions noted. |
| CEK-03.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| CEK-03.03 | Encrypted VPNs are required for remote access to production which require authentication through multi-factor authentication protocols. | Inspected the VPN encryption and multi-factor authentication configurations to determine that encrypted VPNs were required for remote access to production which required authentication through multi-factor authentication protocols. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CEK-04:** *Encryption Algorithm* - Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology. | | | |
| **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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| CEK-04.01 | Backups of in-scope systems are encrypted. | Inspected the automated backup system encryption configurations for a sample of database clusters to determine that backups of in-scope systems were encrypted for each database cluster sampled. | No exceptions noted. |
| CEK-04.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| CEK-04.03 | Encrypted VPNs are required for remote access to production which require authentication through multi-factor authentication protocols. | Inspected the VPN encryption and multi-factor authentication configurations to determine that encrypted VPNs were required for remote access to production which required authentication through multi-factor authentication protocols. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: CEK-05:** *Encryption Change Management* - Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-05.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-05.02 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CEK-05.03 | Test and development environments do not use live production data. | Inspected the release procedure and example test data to determine that test and development environments did not use live production data. | No exceptions noted. |
| **CCM: CEK-06:** *Encryption Change Cost Benefit Analysis* - Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-06.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-06.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| CEK-06.03 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| **CCM: CEK-07:** *Encryption Risk Management* - Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-07.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-08:** *CSC Key Management Capability* - CSPs must provide the capability for CSCs to manage their own data encryption keys. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-08.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-09:** *Encryption and Key Management Audit* - Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s). | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-09.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-09.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CEK-09.03 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| **CCM: CEK-10:** *Key Generation* - Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-10.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-11:** *Key Purpose* - Manage cryptographic secret and private keys that are provisioned for a unique purpose. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-11.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-12:** *Key Rotation* - Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-12.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-13:** *Key Revocation* - Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-13.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-14:** *Key Destruction* - Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-14.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-14.02 | Policies and standards for the secure disposal of equipment are documented and maintained. | Inspected the data classification and media disposal policies to determine that policies and standards for the secure disposal of equipment were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CEK-14.03 | Requests to dispose of media devices containing confidential information are entered and tracked via the ticketing system. Requests to dispose of media devices containing confidential information are entered via the ticketing system | Inspected an example list of media disposals and example certificates of deletion with the assistance of senior compliance analyst to determine that requests to dispose of media devices containing confidential information were entered and tracked via the ticketing system. | No exceptions noted. |
| **CCM: CEK-15:** *Key Activation* - Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-15.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| **CCM: CEK-16:** *Key Suspension* - Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-16.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-16.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CEK-17:** *Key Deactivation* - Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-17.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-17.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| **CCM: CEK-18:** *Key Archival* - Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-18.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-18.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CEK-19:** *Key Compromise* - Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-19.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-19.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| **CCM: CEK-20:** *Key Recovery* - Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-20.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-20.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: CEK-21:** *Key Inventory Management* - Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| CEK-21.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| CEK-21.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| CEK-21.03 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| CEK-21.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |

# Data Center Security

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DCS-01:** *Off-Site Equipment Disposal Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually. | | | |
| **P5.1** The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy. | | | |
| **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. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| **CC3.3** COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | | |
| **P1.1** The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |
| **P2.1** The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. | | | |
| **P4.1** The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. | | | |
| **P4.2** The entity retains personal information consistent with the entity's objectives related to privacy. | | | |
| **P4.3** The entity securely disposes of personal information to meet the entity's objectives related to privacy. | | | |
| DCS-01.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DCS-02:** *Off-Site Transfer Authorization Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **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. | | | |
| **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. | | | |
| DCS-02.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: DCS-03:** *Secure Area Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually. | | | |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| **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. | | | |
| **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. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| DCS-03.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DCS-03.02 | Documented policies and procedures are in place to guide personnel in designing and applying safe and secure office areas. | Inspected the employee handbook and clean desk standard to determine that documented policies and procedures were in place to guide personnel in designing and applying safe and secure office areas. | No exceptions noted. |
| DCS-03.03 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: DCS-04:** *Secure Media Transportation Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| DCS-04.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| **CCM: DCS-05:** *Assets Classification* - Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. | | | |
| **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. | | | |
| DCS-05.01 | An inventory of physical and logical assets (e.g., applications) is documented, classified, and maintained according to the organizational business risk. | Inspected the asset inventory to determine that an inventory of physical and logical assets (e.g., applications) was documented, classified, and maintained according to the organizational business risk. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DCS-05.02 | A systems inventory is developed and maintained to track physical devices and systems, virtual devices, and external information systems that are used to store and access company data. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that a systems inventory was developed and maintained to track physical devices and systems, virtual devices, and external information systems that were used to store and access company data. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DCS-06:** *Assets Cataloguing and Tracking* - Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system. | | | |
| **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. | | | |
| DCS-06.01 | An inventory of physical and logical assets (e.g., applications) is documented, classified, and maintained according to the organizational business risk. | Inspected the asset inventory to determine that an inventory of physical and logical assets (e.g., applications) was documented, classified, and maintained according to the organizational business risk. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DCS-07:** *Controlled Access Points* - Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas. | | | |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| **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. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives. | | | |
| DCS-07.01 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DCS-07.02 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems and the user access reviews for a sample of quarters to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| DCS-07.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| DCS-07.04 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |
| DCS-07.05 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| DCS-07.06 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: DCS-08:** *Equipment Identification* - Use equipment identification as a method for connection authentication. | | | |
| **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. | | | |
| DCS-08.01 | An inventory of physical and logical assets (e.g., applications) is documented, classified, and maintained according to the organizational business risk. | Inspected the asset inventory to determine that an inventory of physical and logical assets (e.g., applications) was documented, classified, and maintained according to the organizational business risk. | No exceptions noted. |
| DCS-08.02 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems and the user access reviews for a sample of quarters to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| DCS-08.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| DCS-08.04 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DCS-08.05 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| DCS-08.06 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DCS-09:** *Secure Area Authorization* - Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization. | | | |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| **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. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| DCS-09.01 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| DCS-09.02 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems and the user access reviews for a sample of quarters to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| DCS-09.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| DCS-09.04 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |
| DCS-09.05 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| DCS-09.06 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| DCS-09.07 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| DCS-09.08 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DCS-10:** *Surveillance System* - Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| DCS-10.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| DCS-10.02 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| DCS-10.03 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| **CCM: DCS-11:** *Unauthorized Access Response Training* - Train datacenter personnel to respond to unauthorized ingress or egress attempts. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| **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. | | | |
| DCS-11.01 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DCS-11.02 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: DCS-12:** *Cabling Security* - Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| DCS-12.01 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |
| DCS-12.02 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DCS-13:** *Environmental Systems* - Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| DCS-13.01 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |
| DCS-13.02 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: DCS-14:** *Secure Utilities* - Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| DCS-14.01 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |
| DCS-14.02 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DCS-15:** *Equipment Location* - Keep business-critical equipment away from locations subject to high probability for environmental risk events. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| **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. | | | |
| DCS-15.01 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |
| DCS-15.02 | Zoom reviews documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider is in compliance with security and availability policies and commitments. | Inspected most recent evidence of compliance verification for the cloud hosting provider to determine that Zoom reviewed documentation provided by the cloud hosting provider on an annual basis to help ensure that the cloud hosting provider was in compliance with security and availability confidentiality policies and commitments. | No exceptions noted. |
| | AWS and OCI are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |

# Data Security and Privacy Lifecycle Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-01:** *Security and Privacy Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually. | | | |
| **PI1.1** The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | | |
| **PI1.5** The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives. | | | |
| **P4.1** The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. | | | |
| **P4.2** The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. | | | |
| **P4.3** The entity securely disposes of personal information to meet the entity's objectives related to privacy. | | | |
| **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. | | | |
| DSP-01.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| DSP-01.02 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| DSP-01.03 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and BYOD policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DSP-01.04 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| DSP-01.05 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| DSP-01.06 | Information classifications and data ownership are defined in policies and procedures, which are reviewed annually for accuracy. | Inspected the data retention policy and data handling principles to determine that information classifications and data ownership was defined in the policies and procedures and were reviewed annually for accuracy. | The test of the control activity disclosed that the data protection and loss standard was not updated annually. |
| DSP-01.07 | Documented data classification policies and procedures are in place to guide personnel in classifying data by the data owner based on data type, value, sensitivity, and criticality to the organization. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that documented data classification policies and procedures were in place to guide personnel in classifying data by the data owner based on data type, value, sensitivity, and criticality to the organization. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-02:** *Secure Disposal* - Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means. | | | |
| **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. | | | |
| **CC6.2** 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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| **CC6.4** 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. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| **P4.3** The entity securely disposes of personal information to meet the entity's objectives related to privacy. | | | |
| DSP-02.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: DSP-03:** *Data Inventory* - Create and maintain a data inventory, at least for any sensitive data and personal data. | | | |
| **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. | | | |
| DSP-03.01 | Data flow diagrams and topology maps that cover the processing, storing, and transmission of data are documented and maintained. | Inspected the information security data flow document to determine that data flow diagrams and topology maps that covered the processing, storing, and transmission of data were documented and maintained. | No exceptions noted. |
| DSP-03.02 | Backups of in-scope systems are encrypted. | Inspected the automated backup system encryption configurations for a sample of database clusters to determine that backups of in-scope systems were encrypted for each database cluster sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DSP-03.03 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| DSP-03.04 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| DSP-03.05 | Data is replicated across geographically separate availability zones. | Inspected the data replication configurations to determine that data was replicated across geographically separate availability zones. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DSP-04:** Data Classification - Classify data according to its type and sensitivity level. | | | |
| **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. | | | |
| **C1.1** The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality. | | | |
| DSP-04.01 | Data flow diagrams and topology maps that cover the processing, storing, and transmission of data are documented and maintained. | Inspected the information security data flow document to determine that data flow diagrams and topology maps that covered the processing, storing, and transmission of data were documented and maintained. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DSP-05:** *Data Flow Documentation* - Create data flow documentation to identify what data is processed, stored, or transmitted where.  Review data flow documentation at defined intervals, at least annually, and after any change. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| DSP-05.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |

<table>
<tr><th>Control #</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td colspan="4"><b>CCM: DSP-06:</b> <i>Data Ownership and Stewardship</i> - Document ownership and stewardship of all relevant documented personal and sensitive data.  Perform review at least annually.</td></tr>
<tr><td colspan="4"><b>CC1.1</b> COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</td></tr>
<tr><td colspan="4"><b>CC1.3</b> COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</td></tr>
<tr><td colspan="4"><b>CC1.5</b> COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</td></tr>
<tr><td colspan="4"><b>P2.1</b> The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice.  Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required.  Such consent is obtained only for the intended purpose of the information to meet the entity’s objectives related to privacy.  The entity’s basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.</td></tr>
<tr><td colspan="4"><b>P3.2</b> For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity’s objectives related to privacy.</td></tr>
<tr><td colspan="4"><b>CC6.7</b> The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.</td></tr>
<tr><td>DSP-06.01</td><td>The entity’s security and availability commitments and the associated system requirements are documented in customer contracts.</td><td>Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts.</td><td>No exceptions noted.</td></tr>
<tr><td>DSP-06.02</td><td>Users are assigned unique user IDs.</td><td>Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs.</td><td>No exceptions noted.</td></tr>
<tr><td rowspan="2">DSP-06.03</td><td rowspan="2">Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager.</td><td>Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege.</td><td>No exceptions noted.</td></tr>
<tr><td>Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td colspan="3">AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside.</td></tr>
</table>

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-07:** *Data Protection by Design and Default* - Develop systems, products, and business practices based upon a principle of security by design and industry best practices. | | | |
| **PI1.2** The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. | | | |
| **PI1.3** The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. | | | |
| DSP-07.01 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and BYOD policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |
| DSP-07.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| **CCM: DSP-08:** *Data Privacy by Design and Default* - Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices.  Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations. | | | |
| **P1.1** The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | | |
| DSP-08.01 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and BYOD policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |
| DSP-08.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| **CCM: DSP-09:** *Data Protection Impact Assessment* - Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity, and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices. | | | |
| **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. | | | |
| DSP-09.01 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-10:** *Sensitive Data Transfer* - Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| DSP-10.01 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: DSP-11:** *Personal Data Access, Reversal, Rectification and Deletion* - Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations. | | | |
| **P2.1** The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. | | | |
| DSP-11.01 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and BYOD policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |
| DSP-11.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| DSP-11.03 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-12:** *Limitation of Purpose in Personal Data Processing* - Define, implement, and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject. | | | |
| **P2.1** The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice.  Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required.  Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy.  The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. | | | |
| DSP-12.01 | Policies and standards are in place requiring sensitive information to be encrypted over the Internet or other public communication paths. | Inspected the encryption policy and BYOD policy to determine that policies and standards were in place that required sensitive information to be encrypted over the Internet or other public communications paths. | No exceptions noted. |
| DSP-12.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| **CCM: DSP-13:** *Personal Data Sub-processing* - Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations. | | | |
| **P2.1** The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. | | | |
| DSP-13.01 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| DSP-13.02 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-14:** *Disclosure of Data Sub-processors* - Define, implement, and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing. | | | |
| **P6.1** The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. | | | |
| DSP-14.01 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| DSP-14.02 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual non-disclosure agreement (NDA), and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| **CCM: DSP-15:** *Limitation of Production Data Use* - Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| DSP-15.01 | Test and development environments do not use live production data. | Inspected the release procedure and example test data to determine that test and development environments did not use live production data. | No exceptions noted. |
| DSP-15.02 | Production data is not utilized for change development and testing efforts. | Inspected example testing data to determine that production data was not utilized for change development and testing efforts. | No exceptions noted. |
| **CCM: DSP-16:** *Data Retention and Deletion* - Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws, and regulations. | | | |
| **C1.1** The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | | |
| **C1.2** The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | | |
| **C3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| **P4.2** The entity retains personal information consistent with the entity's objectives related to privacy. | | | |
| DSP-16.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: DSP-17:** *Sensitive Data Protection* - Define and implement, processes, procedures, and technical measures to protect sensitive data throughout its lifecycle. | | | |
| **CC2.1** COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| **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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| **C1.1** The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | | |
| **P2.1** The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. | | | |
| **P3.1** Personal information is collected consistent with the entity's objectives related to privacy. | | | |
| **P3.2** For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy. | | | |
| **P4.1** The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. | | | |
| **P4.2** The entity retains personal information consistent with the entity's objectives related to privacy. | | | |
| **P4.3** The entity securely disposes of personal information to meet the entity's objectives related to privacy. | | | |
| **P5.1** The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy. | | | |
| **P5.2** The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy. | | | |
| **P6.1** The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. | | | |
| **P6.2** The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy. | | | |
| **P6.3** The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy. | | | |
| **P6.4** The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary. | | | |
| **P6.5** The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy. | | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **P6.6** The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy. | | | |
| **P6.7** The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy. | | | |
| DSP-17.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: DSP-18:** *Disclosure Notification* - The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation. | | | |
| **P4.1** The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. | | | |
| DSP-18.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| **CCM: DSP-19:** *Data Location* - Define and implement, processes, procedures, and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| DSP-19.01 | Policies and standards that define the requirements for the classification, protection, and handling of data throughout its lifecycle are documented, maintained, and are reviewed at least annually. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that policies and standards that defined the requirements for the classification, protection, and handling of data throughout its lifecycle were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. | | |

# Governance and Risk Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: GRC-01:** *Governance Program Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually. | | | |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| **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. | | | |
| GRC-01.01 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| GRC-01.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| GRC-01.03 | Documented policies and procedures are in place to guide personnel in supporting the entity's ISMS and include, but are not limited to, the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | Inspected the security policies and procedures to determine that documented policies and procedures were in place to guide personnel in supporting the entity's ISMS and included the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-01.04 | The board of directors, operating independently from management and exercising objectivity in evaluations and decision making, has established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | Inspected organizational strategic plans to determine that the board of directors, operating independently from management and exercising objectivity in evaluations and decision making, had established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | No exceptions noted. |
| **CCM: GRC-02:** *Risk Management Program* - Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks. | | | |
| **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. | | | |
| **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. | | | |
| **A1.2** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| GRC-02.01 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| GRC-02.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| GRC-02.03 | External parties and relevant authorities are leveraged to identify current threats, vulnerabilities, and new technologies. | Inspected security updates and example notification generated during the period to determine that external parties and relevant authorities were leveraged to identify current threats, vulnerabilities, and new technologies. | No exceptions noted. |
| GRC-02.04 | The board of directors, operating independently from management and exercising objectivity in evaluations and decision making, has established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | Inspected organizational strategic plans to determine that the board of directors, operating independently from management and exercising objectivity in evaluations and decision making, had established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-02.05 | Disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations are documented and maintained. | Inspected the disaster recovery plans to determine that disaster recovery plans to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations were documented and maintained. | No exceptions noted. |
|  | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring environmental protection controls are in place to meet Zoom's availability commitments and requirements. |  |  |
| **CCM: GRC-03:** *Organizational Policy Reviews* - Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization. |  |  |  |
| **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. |  |  |  |
| GRC-03.01 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| GRC-03.02 | Policies and standards are in place for identifying and remediating vulnerabilities in production operation systems. | Inspected the automated patching tool configuration and an example patch applied during the period to determine that policies and standards were in place for identifying and remediating vulnerabilities in production operation systems. | No exceptions noted. |
| GRC-03.03 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-03.04 | Documented policies and procedures are in place to guide personnel in supporting the entity's ISMP and include, but are not limited to, the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | Inspected the security policies and procedures to determine that documented policies and procedures were in place to guide personnel in supporting the entity's ISMP and included the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | No exceptions noted. |
| GRC-03.05 | Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures. | Inspected the employee handbook to determine that policies were documented and maintained that addressed disciplinary actions for lack of compliance with policies, standards, and procedures. | No exceptions noted. |
| **CCM: GRC-04:** *Policy Exception Process* - Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs. | | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| GRC-04.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-04.02 | Documented policies and procedures are in place to guide personnel in supporting the entity's ISMP and include, but are not limited to, the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | Inspected the security policies and procedures to determine that documented policies and procedures were in place to guide personnel in supporting the entity's ISMP and included the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | No exceptions noted. |
| GRC-04.03 | Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures. | Inspected the employee handbook to determine that policies were documented and maintained that addressed disciplinary actions for lack of compliance with policies, standards, and procedures. | No exceptions noted. |
| **CCM: GRC-05:** *Information Security Program* - Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| GRC-05.01 | An ISMC comprised of security personnel and executive staff has been established to guide the organization in managing security, availability, and confidentiality risks.  The ISMC meets at least annually to discuss results of risk assessments and status of risk mitigation plans. | Inspected the risk register, most recently completed risk assessment, and evidence of management's review of risk assessment results to determine that the ISMC met during the period to discuss results of risk assessments and status of risk mitigation plans. | No exceptions noted. |
| | | Inspected the security assessment and authorization policy to determine that an ISMC comprised of security personnel and executive staff had been established to guide the organization in managing security, availability, and confidentiality risks. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-05.02 | Documented policies and procedures are in place to guide personnel in supporting the entity's ISMP and include, but are not limited to, the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | Inspected the security policies and procedures to determine that documented policies and procedures were in place to guide personnel in supporting the entity's ISMP and included the following:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• Information systems acquisition, development, and maintenance | No exceptions noted. |
| **CCM: GRC-06:** *Governance Responsibility Mode* - Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs. | | | |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| GRC-06.01 | The responsibility for planning, implementing, operating, assessing, and improving the Information Security governance program is assigned to the CISO. | Inspected the information security management and governance standard to determine that the responsibility for planning, implementing, operating, assessing, and improving the Information Security governance program was assigned to the CISO. | No exceptions noted. |
| GRC-06.02 | Organizational charts are in place to communicate the areas of authority, responsibility, and lines of reporting related to the design, implementation, operation, and maintenance of the system. The organizational charts are available and communicated to employees via the HR system and updated as needed. | Inspected the organizational charts within the HR system to determine that organizational charts were in place to communicate the areas of authority, responsibility, and lines of reporting related to the design, implementation, operation, and maintenance of the system and that the organizational charts were available and communicated to employees via the HR system and updated as needed. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-06.03 | Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities. | Inspected the job descriptions for a sample of employment positions to determine that position descriptions were documented and included the required behaviors and skills required to perform the job functions and responsibilities. | No exceptions noted. |
| GRC-06.04 | The board of directors, operating independently from management and exercising objectivity in evaluations and decision making, has established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | Inspected organizational strategic plan to determine that the board of directors operated independently from management and exercised objectivity in evaluations and decision making, had established strategic plans to guide management personnel in achieving business objectives, including measures for evaluating management performance. | No exceptions noted. |
| **CCM: GRC-07:** *Information System Regulatory Mapping* - Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. | | | |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| **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. | | | |
| GRC-07.01 | The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. | Inspected security updates and example notifications generated during the period to determine that the entity's information technology security group 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. |
| GRC-07.02 | Management performs a risk assessment on an annual basis to identify and analyze the business and security risks, changes to the system, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of assessed changes that could significantly impact the system of internal control. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that management performed a risk assessment during the period that identified and analyzed the business and security risks, changes to the system, vulnerabilities, laws, and regulations, and that the risk assessment included the analysis of assessed changes that could significantly impact the system of internal control, and others with access to the entity's information system, and that risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| GRC-07.03 | The entity's security, availability, and privacy commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| GRC-07.04 | MSAs are in place to define security and confidentiality requirements for third parties with which confidential information is shared. | Inspected the MSAs for a sample of vendors to determine that MSAs were in place and defined security and confidentiality requirements for third parties with which confidential information was shared for each vendor sampled. | No exceptions noted. |
| **CCM: GRC-08:** *Special Interest Groups* - Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| GRC-08.01 | External parties and relevant authorities are leveraged to identify current threats, vulnerabilities, and new technologies. | Inspected security updates and example notification generated during the period to determine that external parties and relevant authorities were leveraged to identify current threats, vulnerabilities, and new technologies. | No exceptions noted. |

## Human Resources

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: HRS-01:** *Background Screening Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually. | | | |
| **CC1.4** The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| **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. | | | |
| HRS-01.01 | Background screenings are performed for new employees for positions with access to non-public information as a component of the hiring process. | Inspected the background screening documentation for a sample of employees hired during the period to determine that background screenings were performed for new employees for positions with access to non-public information as a component of the hiring process for each newly hired employee sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-01.02 | Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities. | Inspected the job descriptions for a sample of employment positions to determine that position descriptions were documented and included the required behaviors and skills required to perform the job functions and responsibilities. | No exceptions noted. |
| **CCM: HRS-02:** *Acceptable Use of Technology Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| HRS-02.01 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| HRS-02.02 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period and a sample of current employees to determine that employees were required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies for each newly hired and current employee sampled. | No exceptions noted. |
| HRS-02.03 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| HRS-02.04 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-02.05 | Policies are documented and maintained that define the requirements for endpoint device security. | Inspected the mobile device and access control policies to determine that policies were documented and maintained that defined the requirements for endpoint device security. | No exceptions noted. |
| HRS-02.06 | Zoom has established policies and procedures supporting business processes and technical measures implemented to manage business risks associated with permitting mobile device access to corporate resources and requires the implementation of higher assurance compensating controls and acceptable-use policies and procedures. | Inspected the employee handbook, access control policy, and the mobile device policy to determine that Zoom established policies and procedures supporting business processes and technical measures implemented to manage business risks associated with permitting mobile device access to corporate resources and required the implementation of higher assurance compensating controls and acceptable-use policies and procedures. | No exceptions noted. |
| **CCM: HRS-03:** *Clean Desk Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| HRS-03.01 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| **CCM: HRS-04:** *Remote and Home Working Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **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. | | | |
| HRS-04.01 | Policies are documented and maintained that define the requirements for endpoint device security. | Inspected the mobile device and access control policies to determine that policies were documented and maintained that defined the requirements for endpoint device security. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-04.02 | Zoom has established policies and procedures supporting business processes and technical measures implemented to manage business risks associated with permitting mobile device access to corporate resources and requires the implementation of higher assurance compensating controls and acceptable-use policies and procedures. | Inspected the employee handbook, access control policy, and the mobile device policy to determine that Zoom established policies and procedures supporting business processes and technical measures implemented to manage business risks associated with permitting mobile device access to corporate resources and required the implementation of higher assurance compensating controls and acceptable-use policies and procedures. | No exceptions noted. |
| HRS-04.03 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of employees hired during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| HRS-04.04 | Policies and standards that define the acceptable use of organizationally owned or managed assets are documented, maintained, and are reviewed at least annually. | Inspected the acceptable use policy to determine that policies and standards that defined the acceptable use of organizationally owned or managed assets were documented, maintained, and were reviewed during the period. | No exceptions noted. |
| HRS-04.05 | A mobile computing policy is in place to manage business risks associated with permitting mobile device access to corporate resources. | Inspected the mobile device and access control policies to determine that a mobile computing policy was in place to manage business risks associated with permitting mobile device access to corporate resources. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: HRS-05:** *Asset returns* - Establish and document procedures for the return of organization-owned assets by terminated employees. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| HRS-05.01 | Documented policies and procedures are in place to enforce the process that organizationally owned assets be returned within an established period upon termination of workforce personnel and / or expiration of external business relationships. | Inspected the personnel security policy to determine that policies and procedures were in place to enforce the process that organizationally owned assets be returned within an established period upon termination of workforce personnel and / or expiration of external business relationships. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-05.02 | Policies and standards for the secure disposal of equipment are documented and maintained. | Inspected the data classification and media disposal policies to determine that policies and standards for the secure disposal of equipment were documented and maintained. | No exceptions noted. |
| HRS-05.03 | Upon termination of workforce personnel and/or expiration of external business relationships, organizationally owned assets shall be returned and sanitized within an established period. | Inspected the termination support ticket for a sample of employees terminated during the period to determine that organizationally owned assets were returned and sanitized upon termination of workforce personnel and/or expiration of external business relationships for each terminated employee sampled. | No exceptions noted. |
| **CCM: HRS-06:** *Employment Termination* - Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment. | | | |
| **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. | | | |
| HRS-06.01 | Policies and standards for the secure disposal of equipment are documented and maintained. | Inspected the data classification and media disposal policies to determine that policies and standards for the secure disposal of equipment were documented and maintained. | No exceptions noted. |
| HRS-06.02 | Documented policies and procedures are in place to enforce the process that organizationally owned assets be returned within an established period upon termination of workforce personnel and / or expiration of external business relationships. | Inspected the personnel security policy to determine that policies and procedures were in place to enforce the process that organizationally owned assets be returned within an established period upon termination of workforce personnel and / or expiration of external business relationships. | No exceptions noted. |
| HRS-06.03 | Upon termination of workforce personnel and/or expiration of external business relationships, organizationally owned assets shall be returned and sanitized within an established period. | Inspected the termination support ticket for a sample of employees terminated during the period to determine that organizationally owned assets were returned and sanitized upon termination of workforce personnel and/or expiration of external business relationships for each terminated employee sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: HRS-07:** *Employment Agreement Process* - Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets. | | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| **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. | | | |
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| **SCC5.3** COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | | |
| HRS-07.01 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period to determine that each employee sampled completed information security awareness training upon hire to understand their responsibilities under applicable policies. | No exceptions noted. |
| HRS-07.02 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of employees hired during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: HRS-08:** *Employment Agreement Consent* – The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies. | | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| **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. | | | |
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| **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. | | | |
| HRS-08.01 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period to determine that each employee sampled completed information security awareness training upon hire to understand their responsibilities under applicable policies. | No exceptions noted. |
| HRS-08.02 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of employees hired during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| **CCM: HRS-09:** *Personnel Roles and Responsibilities* - Document and communicate roles and responsibilities of employees, as they relate to information assets and security. | | | |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| **CC1.5** COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | | |
| **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. | | | |
| HRS-09.01 | Policies and standards for the secure disposal of equipment are documented and maintained. | Inspected the data classification and media disposal policies to determine that policies and standards for the secure disposal of equipment were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-09.02 | Documented roles and responsibilities are in place as they relate to information assets and security. | Inspected system and information integrity policy to determine that documented roles and responsibilities were in place as they relate to information assets and security. | No exceptions noted. |
| HRS-09.03 | Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities. | Inspected the job descriptions for a sample of employment positions to determine that position descriptions were documented and included the required behaviors and skills required to perform the job functions and responsibilities. | No exceptions noted. |
| HRS-09.04 | The responsibility for planning, implementing, operating, assessing, and improving the Information Security governance program is assigned to the CISO. | Inspected the information security management and governance standard to determine that the responsibility for planning, implementing, operating, assessing, and improving the Information Security governance program was assigned to the CISO. | No exceptions noted. |
| **CCM: HRS-10:** *Non-Disclosure Agreements* - Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details. | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| **P6.4** The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy.  The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary. | | | |
| HRS-10.01 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period and a sample of current employees to determine that employees were required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies for each newly hired and current employee sampled. | No exceptions noted. |
| HRS-10.02 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-10.03 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| HRS-10.04 | Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each vendor sampled was evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. | No exceptions noted. |
| HRS-10.05 | MSAs are in place to define security and confidentiality requirements for third parties with which confidential information is shared. | Inspected the MSAs for a sample of vendors to determine that MSAs were in place and defined security and confidentiality requirements for third parties with which confidential information was shared for each vendor sampled. | No exceptions noted. |
| HRS-10.06 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| **CCM: HRS-11:** *Security Awareness Training* - Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates. | | | |
| **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. | | | |
| HRS-11.01 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period and a sample of current employees to determine that employees were required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies for each newly hired and current employee sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-11.02 | Management monitors the completion of information security awareness training. | Inspected evidence of the monitoring of completion for security awareness training to determine that management monitored the completion of security awareness training for employees. | No exceptions noted. |
| HRS-11.03 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| HRS-11.04 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| **CCM: HRS-12:** *Personal and Sensitive Data Awareness and Training* - Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization. | | | |
| **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. | | | |
| HRS-12.01 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period and a sample of current employees to determine that employees were required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies for each newly hired and current employee sampled. | No exceptions noted. |
| HRS-12.02 | Management monitors the completion of information security awareness training. | Inspected evidence of the monitoring of completion for security awareness training to determine that management monitored the completion of security awareness training for employees. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| HRS-12.03 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| **CCM: HRS-13:** *Compliance User Responsibility* - Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. | | | |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| **CC1.5** COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | | |
| **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. | | | |
| HRS-13.01 | Documented roles and responsibilities are in place as they relate to information assets and security. | Inspected system and information integrity policy to determine that documented roles and responsibilities were in place as they relate to information assets and security. | No exceptions noted. |
| HRS-13.02 | Position descriptions are documented and include the required behaviors and skills required to perform the job functions and responsibilities. | Inspected the job descriptions for a sample of employment positions to determine that position descriptions were documented and included the required behaviors and skills required to perform the job functions and responsibilities. | No exceptions noted. |
| HRS-13.03 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| HRS-13.04 | Policies and procedures are in place to require that unattended workspaces do not have openly visible sensitive documents and that user computing sessions are disabled after an established period of inactivity. | Inspected the information security policy to determine that policies and procedures were in place that required unattended workspaces did not have openly visible sensitive documents and that user computing sessions were disabled after an established period of inactivity. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the session timeout configurations for an example workstation to determine that user computing sessions were disabled after an established period of inactivity. | No exceptions noted. |
| HRS-13.05 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period and a sample of current employees to determine that employees were required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies for each newly hired and current employee sampled. | No exceptions noted. |
| HRS-13.06 | Policies are documented and maintained that address disciplinary actions for lack of compliance with policies, standards, and procedures. | Inspected the employee handbook to determine that policies were documented and maintained that addressed disciplinary actions for lack of compliance with policies, standards, and procedures. | No exceptions noted. |

## Identity and Access Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-01:** *Identity and Access Management Policy and Procedures* - Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **CC6.2** 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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-01.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| IAM-01.02 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-01.03 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-01.04 | Documented policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. | Inspected the media protection policy and access control policy to determine that documented policies and procedures were established for permissible storage and access of identities used for authentication to ensure identities were only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. | No exceptions noted. |
| IAM-01.05 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-02:** *Strong Password Policy and Procedures* - Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures.  Review and update the policies and procedures at least annually. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| IAM-02.01 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained that defined the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| IAM-02.02 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-03:** *Identity Inventory* - Manage, store, and review the information of system identities, and level of access. | | | |
| **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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-03.01 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| IAM-03.02 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-03.03 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-03.04 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-04:** *Separation of Duties* - Employ the separation of duties principle when implementing information system access. | | | |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| **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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-04.01 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-04.02 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| IAM-04.03 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| IAM-04.04 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-04.05 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-04.06 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |
| IAM-04.07 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-04.08 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-05:** *Least Privilege* - Employ the least privilege principle when implementing information system access. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-05.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| IAM-05.02 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-05.03 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |
| IAM-05.04 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-06:** *User Access Provisioning* - Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| **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. | | | |
| IAM-06.01 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-06.02 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IAM-07:** *User Access Changes and Revocation* - De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies. | | | |
| **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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-07.01 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |
| IAM-07.02 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-07.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-07.04 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-08:** *User Access Review* - Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance. | | | |
| **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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives. | | | |
| IAM-08.01 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-09:** *Segregation of Privileged Access Roles* - Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated. | | | |
| **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. | | | |
| **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 | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives. | | | |
| IAM-09.01 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-09.02 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-09.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-10:** *Management of Privileged Access Roles* - Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access. | | | |
| **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 | | | |
| **CC6.2** 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. | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| IAM-10.01 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-10.02 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-10.03 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-11:** *CSCs Approval for Agreed Privileged Access Roles* - Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles. | | | |
| **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. | | | |
| **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 | | | |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives. | | | |
| IAM-11.01 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-11.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| IAM-11.03 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-11.04 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-11.05 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-11.06 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-12:** *Safeguard Logs Integrity* - Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| IAM-12.01 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-12.02 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |
| IAM-12.03 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-12.04 | The ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | Inspected firewall users listing with the assistance of the senior compliance analyst to determine that the ability to configure firewall rulesets and VPC security groups was restricted to authorized engineering personnel. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-12.05 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| **CCM: IAM-13:** *Uniquely Identifiable Users* - Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs. | | | |
| **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 | | | |
| IAM-13.01 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-13.02 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-14:** *Strong Authentication* - Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities. | | | |
| **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 | | | |
| **CC6.2** 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. | | | |
| IAM-14.01 | Policies and standards for identity and access management are documented, maintained, and reviewed at least annually. | Inspected the access control policy to determine that policies and standards for identity and access management were documented, maintained, and reviewed during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-14.02 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-15:** *Passwords Management* - Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords. | | | |
| **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 | | | |
| **CC6.2** 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. | | | |
| IAM-15.01 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IAM-16:** *Authorization Mechanisms* - Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized. | | | |
| **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 | | | |
| **CC6.2** 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. | | | |
| IAM-16.01 | The ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | Inspected firewall users listing with the assistance of the senior compliance analyst to determine that the ability to configure firewall rulesets and VPC security groups was restricted to authorized engineering personnel. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IAM-16.02 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| IAM-16.03 | An IDS / IPS is utilized to analyze network events and report possible or actual network security breaches and is configured to alert security operations personnel when certain network security events are detected. | Inspected the IDS / IPS monitoring configurations and example alert notification generated during the period to determine that an IDS / IPS was utilized to analyze network events and reported possible or actual network security breaches and was configured to alert security operations personnel when certain network security events were detected. | No exceptions noted. |
| IAM-16.04 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| IAM-16.05 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-16.06 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege and that user access was documented in a ticket and approved by the appropriate manager for each in scope system. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that users were provisioned role-based access on organization standards, using the principle of least privilege, user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-16.07 | User access is modified or revoked for employees and contractors changing job roles or separating from company employment. | Inspected the termination checklist and user access privileges for a sample of employees and contractors terminated during the period to determine that user access was modified or revoked for employees and contractors changing job roles or separating from company employment for each terminated employee and contractor sampled. | No exceptions noted. |
| IAM-16.08 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine that user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| IAM-16.09 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| IAM-16.10 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

## INTEROPERABILITY AND PORTABILITY

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IPY-01:** *Interoperability and Portability Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for:<br>a. Communications between application interfaces<br>b. Information processing interoperability<br>c. Application development portability<br>d. Information/Data exchange, usage, portability, integrity, and persistence<br>Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| IPY-01.01 | Zoom has implemented a standard description of its system and boundaries and communicated such description to authorized users on an as needed basis through independent third-party examination reports. | Inspected the independent third-party examination report to determine that Zoom has implemented a standard description of its system and boundaries. | No exceptions noted. |
| IPY-01.02 | Information regarding the design, configuration, and usage of the Zoom API is available to users through the Zoom public website. | Inspected Zoom's public website to determine that information regarding the design, configuration, and usage of the Zoom API was available to users through the Zoom public website. | No exceptions noted. |
| IPY-01.03 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer agreements and terms for a sample of customers onboarded during the period to determine that the security and availability commitments and the associated system requirements were documented in customer contracts for each customer sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IPY-01.04 | Documented policies and procedures are established to ensure integrity of information and information system security through configurations and system management. | Inspected the system and communications protection policy to determine that documented policies and procedures were established to ensure integrity of information and information system security through configurations and system management. | No exceptions noted. |
| **CCM: IPY-02:** *Application Interface Availability* - Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability. | | | |
| **PI1.1** The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | | |
| **PI1.2** The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. | | | |
| **PI1.3** The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. | | | |
| IPY-02.01 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| IPY-02.02 | Information regarding the design, configuration, and usage of the Zoom API is available to users through the Zoom public website. | Inspected Zoom's public website to determine that information regarding the design, configuration, and usage of the Zoom API was available to users through the Zoom public website. | No exceptions noted. |
| IPY-02.03 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |
| IPY-02.04 | Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website. | Inspected the company website overview page to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IPY-03:** *Secure Interoperability and Portability Management* - Implement cryptographically secure and standardized network protocols for the management, import and export of data. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| IPY-03.01 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| IPY-03.02 | Information regarding the design, configuration, and usage of the Zoom API is available to users through the Zoom public website. | Inspected Zoom's public website to determine that information regarding the design, configuration, and usage of the Zoom API was available to users through the Zoom public website. | No exceptions noted. |
| IPY-03.03 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |
| IPY-03.04 | Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website. | Inspected the company website overview page to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website. | No exceptions noted. |
| IPY-03.05 | System alerts, including planned changes to system components, planned outages, and known issues are issued and displayed on the external-facing website. | Inspected the Zoom service status page to determine that system alerts, including planned changes to system components, planned outages, and known issues were issued and displayed on the external-facing website. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IPY-04:** *Data Portability Contractual Obligations* - Agreements must include provisions specifying CSCs access to data upon contract termination and will include:<br>a. Data format<br>b. Length of time the data will be stored<br>c. Scope of the data retained and made available to the CSCs<br>d. Data deletion policy | | | |
| **PI1.1** The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | | |
| **PI1.2** The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. | | | |
| **PI1.3** The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. | | | |
| IPY-04.01 | Zoom has implemented a standard description of its system and boundaries and communicated such description to authorized users on an as needed basis through independent third-party examination reports. | Inspected the independent third-party examination report to determine that Zoom has implemented a standard description of its system and boundaries. | No exceptions noted. |
| IPY-04.02 | Information regarding the design, configuration, and usage of the Zoom API is available to users through the Zoom public website. | Inspected Zoom's public website to determine that information regarding the design, configuration, and usage of the Zoom API was available to users through the Zoom public website. | No exceptions noted. |
| IPY-04.03 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer agreements and terms for a sample of customers onboarded during the period to determine that the security and availability commitments and the associated system requirements were documented in customer contracts for each customer sampled. | No exceptions noted. |
| IPY-04.04 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| IPY-04.05 | A retention policy is in place to guide service personnel in the retention period applicable to personal information. | Inspected the data deletion and exceptions policies to determine that the entity had implemented a policy to guide service personnel in the retention period applicable to personal information. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IPY-04.06 | Documented data disposal policies are in place to guide personnel in the disposal of personal information. | Inspected the data deletion and exceptions policies to determine that the entity had implemented a policy to guide service personnel in the retention period applicable to personal information. | No exceptions noted. |

## Infrastructure and Virtualization Security

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IVS-01:** *Infrastructure and Virtualization Security Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually. | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| **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. | | | |
| IVS-01.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that a documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| IVS-01.02 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| IVS-01.03 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-01.04 | Policies and standards are in place for identifying and remediating vulnerabilities in production operation systems. | Inspected the automated patching tool configuration and an example patch applied during the period to determine that policies and standards were in place for identifying and remediating vulnerabilities in production operation systems. | No exceptions noted. |
| IVS-01.05 | Zoom Video has a documented network architecture diagram in place to identify high-risk environments and data flows that may have legal compliance impacts. | Inspected the network architecture diagram to determine that a documented network architecture diagram was in place to identify high-risk environments and data flows that may have legal compliance impacts. | No exceptions noted. |
| **CCM: IVS-02:** *Capacity and Resource Planning* - Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business. | | | |
| **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. | | | |
| IVS-02.01 | Monitoring tools are configured to alert security operations personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert IT personnel for possible or actual security breaches. | No exceptions noted. |
| IVS-02.02 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| IVS-02.03 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| IVS-02.04 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-02.05 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| | AWS and OCI are responsible for ensuring capacity demand controls are in place to meet Zoom's availability commitments and requirements. | | |
| **CCM: IVS-03:** *Network Security* - Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business.  Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating 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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| IVS-03.01 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| IVS-03.02 | An IDS / IPS is utilized to analyze network events and report possible or actual network security breaches and is configured to alert security operations personnel when certain network security events are detected. | Inspected the IDS / IPS monitoring configurations and example alert notification generated during the period to determine that an IDS / IPS was utilized to analyze network events and reported possible or actual network security breaches and was configured to alert security operations personnel when certain network security events were detected. | No exceptions noted. |
| IVS-03.03 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| IVS-03.04 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-03.05 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| IVS-03.06 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents during the period to determine that no security incidents requiring a change to the system occurred during the period; therefore, no testing of operating effectiveness was performed. | No exceptions noted. |
| IVS-03.07 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| IVS-03.08 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| IVS-03.09 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| IVS-03.10 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| IVS-03.11 | A firewall system is in place for the in-scope applications and configured to deny any network connections that are not explicitly authorized. | Inspected firewall configuration and rules to determine that a firewall system was in place for the in-scope applications and configured to deny any network connections that were not explicitly authorized. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-03.12 | VPC security groups are configured to restrict access to the in-scope applications. | Inspected the security group listing to determine that security groups were configured to restrict access to the in-scope applications. | No exceptions noted. |
| IVS-03.13 | The ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | Inspected firewall users listing to determine that the ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | No exceptions noted. |
| IVS-03.14 | Management performs a review of the firewall rulesets on at least an annual basis. | Inspected the most recently completed firewall ruleset review to determine that management performed a review of the firewall rulesets during the period. | No exceptions noted. |
| IVS-03.15 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IVS-04:** *OS Hardening and Base Controls* - Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline. | | | |
| **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. | | | |
| **CC6.8** The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives. | | | |
| **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. | | | |
| IVS-04.01 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |
| IVS-04.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-04.03 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| IVS-04.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| IVS-04.05 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |
| IVS-04.06 | Policies and standards are in place for identifying and remediating vulnerabilities in production operation systems. | Inspected the automated patching tool configuration and an example patch applied during the period to determine that policies and standards were in place for identifying and remediating vulnerabilities in production operation systems. | No exceptions noted. |
| IVS-04.07 | An IDS / IPS is utilized to analyze network events and report possible or actual network security breaches and is configured to alert security operations personnel when certain network security events are detected. | Inspected the IDS / IPS monitoring configurations and example alert notification generated during the period to determine that an IDS / IPS was utilized to analyze network events and reported possible or actual network security breaches and was configured to alert security operations personnel when certain network security events were detected. | No exceptions noted. |
| IVS-04.08 | Monitoring tools are configured to alert security operations personnel for possible or actual security breaches. | Inspected monitoring tool alerting configuration and an example alert to determine that security monitoring tools were configured to alert IT personnel for possible or actual security breaches. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-04.09 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| IVS-04.10 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IVS-05:** *Production and Non-Production Environments* - Separate production and non-production environments. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| IVS-05.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| IVS-05.02 | The production and non-production environments are logically segmented. | Inspected the production and development environment configurations to determine that the production and non-production environments were logically segmented. | No exceptions noted. |
| IVS-05.03 | Privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | Inquired of the senior compliance analyst regarding access to promote changes to production to determine that access privileges to implement system, application, and maintenance changes into production are limited to authorized individuals. | No exceptions noted. |
| | | Inspected the listing of users with the ability to promote production changes, with the assistance of the senior compliance analyst, to determine that privileges to implement system, application, and maintenance changes into production were limited to authorized individuals. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-05.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |
| **CCM: IVS-06:** *Segmentation and Segregation* - Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| IVS-06.01 | A firewall system is in place for the in-scope applications and configured to deny any network connections that are not explicitly authorized. | Inspected firewall configuration and rules to determine that a firewall system was in place for the in-scope applications and configured to deny any network connections that were not explicitly authorized. | No exceptions noted. |
| IVS-06.02 | VPC security groups are configured to serve as a virtual firewall to restrict access to the in-scope applications. | Inspected the security group listing to determine that security groups are configured to serve as a virtual firewall to restrict access to the in-scope applications. | No exceptions noted. |
| IVS-06.03 | The ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | Inspected firewall users listing to determine that the ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | No exceptions noted. |
| IVS-06.04 | Management performs a review of the firewall rulesets on at least an annual basis. | Inspected the most recently completed firewall ruleset review to determine that management performed a review of the firewall rulesets during the period. | No exceptions noted. |
| IVS-06.05 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| IVS-06.06 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: IVS-07:** *Migration to Cloud Environments* - Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments.  Such channels must include only up-to-date and approved protocols. | | | |
| **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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| IVS-07.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| IVS-07.02 | Clock synchronization is in place to help ensure that a reliable and mutually agreed upon external time source is used to synchronize the system clocks of relevant information processing systems. | Inspected the clock synchronization configuration to determine that clock synchronization was in place to help ensure that a reliable and mutually agreed upon external time source was used to synchronize the system clocks of relevant information processing systems. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: IVS-08:** *Network Architecture Documentation* - Identify and document high-risk environments. | | | |
| **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. | | | |
| **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. | | | |
| **CC7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| **CC7.3** 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. | | | |
| IVS-08.01 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-08.02 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: IVS-09:** *Network Defense* - Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks. | | | |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| **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. | | | |
| **CC7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| IVS-09.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| IVS-09.02 | Clock synchronization is in place to help ensure that a reliable and mutually agreed upon external time source is used to synchronize the system clocks of relevant information processing systems. | Inspected the clock synchronization configuration to determine that clock synchronization was in place to help ensure that a reliable and mutually agreed upon external time source was used to synchronize the system clocks of relevant information processing systems. | No exceptions noted. |
| IVS-09.03 | Management meetings are held on a monthly basis to discuss system availability issues and planning. | Inspected the management meeting calendar recurring event and description to determine that management meetings were held on a monthly basis to discuss system availability issues and planning. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-09.04 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |
| IVS-09.05 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| IVS-09.06 | A firewall system is in place for the in-scope applications and configured to deny any network connections that are not explicitly authorized. | Inspected firewall configuration and rules to determine that a firewall system was in place for the in-scope applications and configured to deny any network connections that were not explicitly authorized. | No exceptions noted. |
| IVS-09.07 | VPC security groups are configured to serve as a virtual firewall to restrict access to the in-scope applications. | Inspected the security group listing to determine that security groups are configured to serve as a virtual firewall to restrict access to the in-scope applications. | No exceptions noted. |
| IVS-09.08 | The ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | Inspected firewall users listing to determine that the ability to configure firewall rulesets and VPC security groups is restricted to authorized engineering personnel. | No exceptions noted. |
| IVS-09.09 | Management performs a review of the firewall rulesets on at least an annual basis. | Inspected the most recently completed firewall ruleset review to determine that management performed a review of the firewall rulesets during the period. | No exceptions noted. |
| IVS-09.10 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| IVS-09.11 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| IVS-09.12 | Vulnerability scans are performed on a monthly basis.<br>Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| IVS-09.13 | Backups of in-scope systems are encrypted. | Inspected the automated backup system encryption configurations for a sample of database clusters to determine that backups of in-scope systems were encrypted for each database cluster sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |

## Logging and Monitoring

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: LOG-01:** *Logging and Monitoring Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-01.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| LOG-01.02 | Policies and standards are in place for identifying and remediating vulnerabilities in production operation systems. | Inspected the automated patching tool configuration and an example patch applied during the period to determine that policies and standards were in place for identifying and remediating vulnerabilities in production operation systems. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-01.03 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the data protection and loss prevention standard and the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | The test of the control activity disclosed that the data protection and loss standard was not updated annually. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: LOG-02:** *Audit Logs Protection* - Define, implement, and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| LOG-02.01 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |
| LOG-02.02 | Employees are required to complete information security awareness training upon hire and annually thereafter to understand their responsibilities under applicable policies. | Inspected the security awareness training documentation and evidence of completion for a sample of employees hired during the period to determine that each employee sampled completed information security awareness training upon hire to understand their responsibilities under applicable policies. | No exceptions noted. |
| | | Inspected the security awareness training documentation and evidence of completion for a sample of current employees to determine that each employee sampled completed information security awareness training during the period to understand their responsibilities under applicable policies. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-02.03 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| LOG-02.04 | Backups of in-scope systems are encrypted. | Inspected the automated backup system encryption configurations for a sample of database clusters to determine that backups of in-scope systems were encrypted for each database cluster sampled. | No exceptions noted. |
| **CCM: LOG-03:** *Security Monitoring and Alerting* - Identify and monitor security-related events within applications and the underlying infrastructure.  Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics. | | | |
| **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. | | | |
| **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. | | | |
| LOG-03.01 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| LOG-03.02 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| LOG-03.03 | A firewall system is in place for the in-scope applications and configured to deny any network connections that are not explicitly authorized. | Inspected firewall configuration and rules to determine that a firewall system was in place for the in-scope applications and configured to deny any network connections that were not explicitly authorized. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-03.04 | An IDS / IPS is utilized to analyze network events and report possible or actual network security breaches and is configured to alert security operations personnel when certain network security events are detected. | Inspected the IDS / IPS monitoring configurations and example alert notification generated during the period to determine that an IDS / IPS was utilized to analyze network events and reported possible or actual network security breaches and was configured to alert security operations personnel when certain network security events were detected. | No exceptions noted. |
| LOG-03.05 | Penetration testing is conducted by an independent third party on an annual basis.  Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| LOG-03.06 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| **CCM: LOG-04:** *Audit Logs Access and Accountability* - Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| LOG-04.01 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-04.02 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| LOG-04.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| **CCM: LOG-05:** *Audit Logs Monitoring and Response* - Monitor security audit logs to detect activity outside of typical or expected patterns.  Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-04.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| LOG-04.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-04.03 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: LOG-06:** *Clock Synchronization* - Use a reliable time source across all relevant information processing systems. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| LOG-06.01 | Clock synchronization is in place to help ensure that a reliable and mutually agreed upon external time source is used to synchronize the system clocks of relevant information processing systems. | Inspected the clock synchronization configuration to determine that clock synchronization was in place to help ensure that a reliable and mutually agreed upon external time source was used to synchronize the system clocks of relevant information processing systems. | No exceptions noted. |
| **CCM: LOG-07:** *Logging Scope* - Establish, document, and implement which information meta/data system events should be logged.  Review and update the scope at least annually or whenever there is a change in the threat environment. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-07.01 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| LOG-07.02 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| LOG-07.03 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: LOG-08:** *Log Records* - Generate audit records containing relevant security information. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-08.01 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| LOG-08.02 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: LOG-09:** *Log Protection* - The information system protects audit records from unauthorized access, modification, and deletion. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| LOG-09.01 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| LOG-09.02 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| LOG-09.03 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-09.04 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| LOG-09.05 | Users are assigned unique user IDs. | Inspected the user listings for a sample of in scope systems to determine that users were assigned unique user IDs. | No exceptions noted. |
| LOG-09.06 | Users are provisioned role-based access on organizational standards, using the principle of least privilege. User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| **CCM: LOG-10:** *Encryption Monitoring and Reporting* - Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and 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. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-10.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| LOG-10.02 | Secure and encrypted communications are used to secure web communication sessions. | Inspected the TLS encryption certificate to determine that secure and encrypted communications were used to secure web communication sessions. | No exceptions noted. |
| LOG-10.03 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and multi-factor authentication configurations to determine that encrypted VPNs were required for remote access to production which required authentication through multi-factor authentication protocols. | No exceptions noted. |
| LOG-10.04 | Data is replicated across geographically separate availability zones. | Inspected the data replication configurations to determine that data was replicated across geographically separate availability zones. | No exceptions noted. |
| LOG-10.05 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| LOG-10.06 | VPC security groups are configured to restrict access to the in-scope applications. | Inspected the security group listing to determine that security groups were configured to restrict access to the in-scope applications. | No exceptions noted. |
| LOG-10.07 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |
|  | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. |  |  |
|  | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. |  |  |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: LOG-11:** *Transaction/Activity Logging* - Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys. | | | |
| **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. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-11.01 | Policies and standards for cryptography, encryption, and key management practices are documented and maintained. | Inquired of senior compliance analyst regarding key management procedures to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| | | Inspected the key management standard to determine that policies and standards for cryptography, encryption, and key management practices were documented and maintained. | No exceptions noted. |
| LOG-11.02 | Data input and output test cases are performed on a routine basis to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | Inspected integrity check software configurations and scan log to determine that data input and output test cases were performed during the period to help ensure that input and output integrity routines were implemented for application interfaces and databases to help prevent manual or systematic processing errors, corruption of data, or misuse. | No exceptions noted. |
| LOG-11.03 | A key management system is maintained to track and report cryptographic materials and changes in status. | Inspected the key management policy to determine that a key management system was maintained to track and report cryptographic materials and changes in status. | No exceptions noted. |
| LOG-11.04 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: LOG-12:** *Access Control Logs* - Monitor and log physical access using an auditable access control system. | | | |
| **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. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| LOG-12.01 | Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the administrator listings for a sample of in-scope systems with the assistance of the senior compliance analyst to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| LOG-12.02 | Standards for system authentication, including use of unique user accounts and minimum password requirements are documented and maintained. | Inspected the authentication configurations and system authentication policies for a sample of in-scope systems to determine that standards for system authentication, including use of unique use accounts and minimum password requirements were documented and maintained for the following in scope systems:<br>• Production Servers<br>• Databases<br>• AWS<br>• OCI | No exceptions noted. |
| LOG-12.03 | Users are provisioned role-based access on organizational standards, using the principle of least privilege.  User access must be documented in a ticket and approved by the appropriate manager. | Inspected the user account listing for a sample of in-scope systems to determine that users were provisioned role-based access on organization standards, using the principle of least privilege. | No exceptions noted. |
| | | Inspected the access request ticket for a sample of employees hired during the period to determine user access was documented in a ticket and approved by the appropriate manager for each new employee sampled. | No exceptions noted. |
| LOG-12.04 | User access reviews are performed by management on a quarterly basis to ensure that access to data is restricted and authorized. | Inspected the user access review for a sample of quarters during the period to determine that user access reviews were performed by management to ensure that access to data was restricted and authorized for each quarter sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | Digital Realty, Databank, eStruxture, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Deutsche Telekom, Zayo, AWS, and OCI are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: LOG-13:** *Failures and Anomalies Reporting* - Define, implement, and evaluate processes, procedures, and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party. | | | |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| **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. | | | |
| LOG-13.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| LOG-13.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| LOG-13.03 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting invitations for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| LOG-13.04 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |

# Security Incident Management, e-Discovery, & Cloud Forensics

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: SEF-01:** *Security Incident Management Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| SEF-01.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-01.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| SEF-01.03 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| SEF-01.04 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting minutes for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| SEF-01.05 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: SEF-02:** *Service Management Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| SEF-02.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-02.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| SEF-02.03 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| SEF-02.04 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting minutes for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| SEF-02.05 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: SEF-03:** *Incident Response Plans* - Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| **CC7.3** 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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| SEF-03.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-03.02 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| SEF-03.03 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting minutes for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| SEF-03.04 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: SEF-04:** *Incident Response Testing* - Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| SEF-04.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| SEF-04.02 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting minutes for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |
| SEF-04.03 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| SEF-04.04 | The incident response plan is tested on an annual basis. | Inspected evidence of the most recent incident response exercise to determine that the incident response plan was tested during the period. | No exceptions noted. |
| **CCM: SEF-05:** *Incident Response Metrics* - Establish and monitor information security incident metrics. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| SEF-05.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-05.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| SEF-05.03 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |
| SEF-05.04 | Security management meetings are held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | Inspected meeting minutes for a sample of months to determine that security management meetings were held on a monthly basis to document and review the operational, reporting, and compliance objectives to align them with the company's mission and risk review process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: SEF-06:** *Event Triage Processes* - Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events. | | | |
| **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. | | | |
| SEF-06.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-06.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |
| **CCM: SEF-07:** *Security Breach Notification* - Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations. | | | |
| **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. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| SEF-07.01 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |
| SEF-07.02 | Security incidents, responses, and resolutions are documented and tracked. | Inspected the security incident tracking listing and security incident tickets for a sample of security incidents during the period to determine that security incidents, responses, and resolutions were documented and tracked for each incident sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: SEF-08:** *Points of Contact Maintenance* - Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. | | | |
| **CC2.3** The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| SEF-08.01 | Contact information for compliance liaisons for local and federal law enforcement agency escalation are documented within Zoom policies and procedures to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement. | Inspected the incident response plan and the data guidance tool to determine that contact information for compliance liaisons for local and federal law enforcement agency escalation were documented within Zoom policies and procedures to ensure direct compliance liaisons was established and prepared for a forensic investigation requiring rapid engagement with law enforcement. | No exceptions noted. |
| SEF-08.02 | A documented security incident response plan includes requirements for threat identification, triaging, communication, remediation, and lessons learned. | Inspected the incident response plan to determine that the documented security incident response plan included requirements for threat identification, triaging, communication, remediation, and lessons learned. | No exceptions noted. |

## Supply Chain Management, Transparency, and Accountability

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-01:** *SSRM Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-01.01 | Documented policies and procedures are in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | Inspected the incident management and response policy to determine that documented policies and procedures were in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | No exceptions noted. |
| STA-01.02 | Standards for assessing third-party vendors for compliance with security policies and standards are documented and maintained. Vendors are assessed using this standard at least annually. | Inspected the vendor management policy to determine that standards for assessing third-party vendors for compliance with security policies and standards were documented and maintained and that vendors were assessed using this standard during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-01.03 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| STA-01.04 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| STA-01.05 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| **CCM: STA-02:** *SSRM Supply Chain* - Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-02.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| STA-02.02 | Management meetings are held on a monthly basis to discuss availability issues that arise from the ongoing business operations and monitoring of the system. | Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss availability issues that arose from the ongoing business operations and monitoring of the system for each month sampled. | No exceptions noted. |
| STA-02.03 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-02.04 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-02.05 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-02.06 | The entity's security, availability, and privacy commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual non-disclosure agreement (NDA), and privacy statement to determine that the security, availability, and privacy commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| **CCM: STA-03:** *SSRM Guidance* - Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain. | | | |
| **CC2.3** The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| STA-03.01 | Information regarding the design, configuration, and usage of the Zoom API is available to users through the Zoom public website. | Inspected Zoom's public website to determine that information regarding the design, configuration, and usage of the Zoom API was available to users through the Zoom public website. | No exceptions noted. |
| STA-03.02 | Documented policies and procedures are in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | Inspected the incident management and response policy to determine that documented policies and procedures were in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-03.03 | The entity’s security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| STA-03.04 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-03.05 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| **CCM: STA-04:** *SSRM Control Ownership* - Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-04.01 | Documented policies and procedures are in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | Inspected the incident management and response policy to determine that documented policies and procedures were in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | No exceptions noted. |
| STA-04.02 | The entity’s security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-04.03 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-04.04 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-04.05 | Management performs a risk assessment on an annual basis to identify and analyze the business and security risks, changes to the system, vulnerabilities, laws, and regulations.  The risk assessment also includes the analysis of assessed changes that could significantly impact the system of internal control.  Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that management performed a risk assessment during the period that identified and analyzed the business and security risks, changes to the system, vulnerabilities, laws, and regulations, and that the risk assessment included the analysis of assessed changes that could significantly impact the system of internal control, and others with access to the entity's information system, and that risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | No exceptions noted. |
| **CCM: STA-05:** *SSRM Documentation Review* - Review and validate SSRM documentation for all cloud services offerings the organization uses. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-05.01 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-05.02 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-05.03 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-05.04 | A systems inventory is developed and maintained to track physical devices and systems, virtual devices, and external information systems that are used to store and access company data. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that a systems inventory was developed and maintained to track physical devices and systems, virtual devices, and external information systems that were used to store and access company data. | No exceptions noted. |
| STA-05.05 | Management performs a risk assessment on an annual basis to identify and analyze the business and security risks, changes to the system, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of assessed changes that could significantly impact the system of internal control. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that management performed a risk assessment during the period that identified and analyzed the business and security risks, changes to the system, vulnerabilities, laws, and regulations, and that the risk assessment included the analysis of assessed changes that could significantly impact the system of internal control, and others with access to the entity’s information system, and that risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-06:** *SSRM Control Implementation* - Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-06.01 | Documented policies and procedures are in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | Inspected the incident management and response policy to determine that documented policies and procedures were in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | No exceptions noted. |
| STA-06.02 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| STA-06.03 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| STA-06.04 | Management meetings are held on a monthly basis to discuss availability issues that arise from the ongoing business operations and monitoring of the system. | Inspected the management meeting minutes for a sample of months during the period to determine that management meetings were held to discuss availability issues that arose from the ongoing business operations and monitoring of the system for each month sampled. | No exceptions noted. |
| STA-06.05 | Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each vendor sampled was evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-07:** *Supply Chain Inventory -* Develop and maintain an inventory of all supply chain relationships. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-07.01 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-07.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-07.03 | A systems inventory is developed and maintained to track physical devices and systems, virtual devices, and external information systems that are used to store and access company data. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that a systems inventory was developed and maintained to track physical devices and systems, virtual devices, and external information systems that were used to store and access company data. | No exceptions noted. |
| **CCM: STA-08:** *Supply Chain Risk Management -* CSPs periodically review risk factors associated with all organizations within their supply chain. | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| STA-08.01 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-08.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-09:** *Primary Service and Contractual Agreement* - Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms:<br>• Scope, characteristics and location of business relationship and services offered<br>• Information security requirements (including SSRM)<br>• Change management process<br>• Logging and monitoring capability<br>• Incident management and communication procedures<br>• Right to audit and third party assessment<br>• Service termination<br>• Interoperability and portability requirements<br>• Data privacy | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| STA-09.01 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-09.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-09.03 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-09.04 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-09.05 | Information regarding the design and operation of the system and its boundaries is communicated to customers via the company website. | Inspected the company website overview page to determine that information regarding the design and operation of the system and its boundaries was communicated to customers via the company website. | No exceptions noted. |
| **CCM: STA-10:** *Supply Chain Agreement Review* - Review supply chain agreements between CSPs and CSCs at least annually. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-10.01 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-10.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| **CCM: STA-11:** *Internal Compliance Testing* - Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| STA-11.01 | Policies and standards are documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | Inspected the risk assessment policy to determine that policies and standards were documented and maintained for the risk management program, including identification, evaluation, ownership, treatment, and acceptance of risks. | No exceptions noted. |
| STA-11.02 | Risks identified during the annual risk assessment are managed and tracked in the risk register where they are given a rating and risk mitigation plan with service level agreements. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that risks identified during the annual risk assessment were managed and tracked in the risk register where they were given a rating and risk mitigation plan with service level agreements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| STA-11.03 | The entity's security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer master subscription agreement (MSA), terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| STA-11.04 | A systems inventory is developed and maintained to track physical devices and systems, virtual devices, and external information systems that are used to store and access company data. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that a systems inventory was developed and maintained to track physical devices and systems, virtual devices, and external information systems that were used to store and access company data. | No exceptions noted. |
| STA-11.05 | Management performs a risk assessment on an annual basis to identify and analyze the business and security risks, changes to the system, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of assessed changes that could significantly impact the system of internal control. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the most recently completed risk assessment, risk register, and evidence of review by management to determine that management performed a risk assessment during the period that identified and analyzed the business and security risks, changes to the system, vulnerabilities, laws, and regulations, and that the risk assessment included the analysis of assessed changes that could significantly impact the system of internal control, and others with access to the entity's information system, and that risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | No exceptions noted. |
| STA-11.06 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-12:** *Supply Chain Service Agreement Compliance* - Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards. | | | |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| STA-12.01 | Policies and contractual measures require third parties to comply with the organization's information security policies and standards, and service level requirements. | Inspected the service agreement for a sample of vendors to determine that policies and contractual measures required third parties to comply with the organization's information security policies and standards, and service level requirements. | No exceptions noted. |
| STA-12.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-12.03 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-12.04 | The entity’s security and availability commitments and the associated system requirements are documented in customer contracts. | Inspected the customer MSA, terms of service, mutual NDA, and privacy statement to determine that the security and availability commitments and the associated system requirements were documented in customer contracts. | No exceptions noted. |
| STA-12.05 | Policies and standards are documented and maintained defining the requirements for secure application design, development, deployment, and operation. | Inspected the information security and system development lifecycle policies to determine that policies and standards were documented and maintained defining the requirements for secure application design, development, deployment, and operation. | No exceptions noted. |
| STA-12.06 | Documented policies and procedures are in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | Inspected the incident management and response policy to determine that documented policies and procedures were in place to guide personnel in providing security incident information to affected customers and providers periodically through electronic methods. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: STA-13:** *Supply Chain Governance Review* - Periodically review the organization's supply chain partners' IT governance policies and procedures. | | | |
| **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. | | | |
| STA-13.01 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |
| STA-13.02 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| **CCM: STA-14:** *Supply Chain Data Security Assessment* - Define and implement a process for conducting security assessments periodically for all organizations within the supply chain. | | | |
| **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. | | | |
| STA-14.01 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |
| STA-14.02 | The compliance team reviews changes to high and critical tiered third-party vendors along with their completed audit reports on at least an annual basis to help ensure that third-party vendors maintain compliance with security and availability commitments. | Inspected evidence of review for a sample of high and critical tiered vendors to determine that the compliance team reviewed changes to high and critical tiered third-party vendors during the period for each third-party vendor sampled to ensure that third-party vendors maintained compliance with security and availability commitments. | No exceptions noted. |

# Threat and Vulnerability Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: TVM-01:** *Threat and Vulnerability Management Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| TVM-01.01 | Documented policies and procedures are established to support business processes and technical measures implemented and to prevent the execution of malware on organizationally-owned or managed user end-point devices, IT infrastructure network, and systems components. | Inspected the system and information integrity policy and system to determine that documented policies and procedures were established to support business processes and technical measures implemented and to prevent the execution of malware on organizationally-owned or managed user end-point devices, IT infrastructure network, and systems components. | No exceptions noted. |
| TVM-01.02 | Standard build procedures are used for the installation and maintenance of production servers and includes the use of an access control system to restrict access to authorized personnel. | Inspected the current standard server build procedures to determine that standard build procedures were used for the installation and maintenance of production servers and included the use of an access control system to restrict access to authorized personnel. | No exceptions noted. |
| TVM-01.03 | Documented policies and procedures are established to support processes and technical measures implemented, for detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network, and system components to ensure the efficiency of implemented security controls. | Inspected the risk assessment policy to determine that documented policies and procedures were established to support processes and technical measures implemented, for detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network, and system components to ensure the efficiency of implemented security controls. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| TVM-01.04 | Backout procedures are documented for system, application, and maintenance changes to allow for the rollback of changes that impair system operation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that backout procedures were documented for system, application, and maintenance changes to allow for the rollback of changes that impaired system operation for each change sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: TVM-02:** *Malware Protection Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually. | | | |
| **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. | | | |
| **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. | | | |
| TVM-02.01 | Documented policies and procedures are established to support business processes and technical measures implemented and to prevent the execution of malware on organizationally-owned or managed user end-point devices, IT infrastructure network, and systems components. | Inspected the system and information integrity policy and system to determine that documented policies and procedures were established to support business processes and technical measures implemented and to prevent the execution of malware on organizationally-owned or managed user end-point devices, IT infrastructure network, and systems components. | No exceptions noted. |
| TVM-02.02 | Documented policies and procedures are established to support processes and technical measures implemented, for detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network, and system components to ensure the efficiency of implemented security controls. | Inspected the risk assessment policy to determine that documented policies and procedures were established to support processes and technical measures implemented, for detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network, and system components to ensure the efficiency of implemented security controls. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: TVM-03:** *Vulnerability Remediation Schedule* - Define, implement, and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk. | | | |
| **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. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| TVM-03.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| TVM-03.02 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| TVM-03.03 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: TVM-04:** *Detection Updates* - Define, implement, and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis. | | | |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| TVM-04.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| TVM-04.02 | Incidents requiring a change to the system follow the standard change control process. | Inspected the listing of security incidents and a sample incident during the period to determine that incidents requiring a change to the system follow the standard change control process. | No exceptions noted. |
| TVM-04.03 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| | AWS and OCI are responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | | |
| **CCM: TVM-05:** *External Library Vulnerabilities* - Define, implement, and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy. | | | |
| **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. | | | |
| TVM-05.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored. Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| TVM-05.02 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: TVM-06:** *Penetration Testing* - Define, implement, and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties. | | | |
| **CC4.2** 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. | | | |
| **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. | | | |
| TVM-06.01 | Penetration testing is conducted by an independent third party on an annual basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| TVM-06.02 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| TVM-06.03 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: TVM-07:** *Vulnerability Identification* - Define, implement, and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly. | | | |
| **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. | | | |
| TVM-07.01 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| TVM-07.02 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| TVM-07.03 | Penetration testing is conducted by an independent third party on an annual basis.  Vulnerabilities identified are tracked and monitored for remediation. | Inspected the most recently completed penetration test performed to determine that penetration testing was conducted by an independent third party during the period and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| TVM-07.04 | Vulnerability scans are performed on a monthly basis. Vulnerabilities identified are tracked and monitored for remediation. | Inspected the vulnerability scan configurations to determine that vulnerability scans were performed on a monthly basis and that vulnerabilities identified were tracked and monitored for remediation. | No exceptions noted. |
| TVM-07.05 | Monitoring tools are configured to alert security personnel for possible or actual security breaches. | Inspected the monitoring tool alerting configurations and an example alert to determine that monitoring tools were configured to alert security personnel for possible or actual security breaches. | No exceptions noted. |
| TVM-07.06 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| TVM-07.07 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| TVM-07.08 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alerted on changes that deviate from the established baseline via FIM. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| TVM-07.09 | Backout procedures are documented for system, application, and maintenance changes to allow for the rollback of changes that impair system operation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that backout procedures were documented for system, application, and maintenance changes to allow for the rollback of changes that impaired system operation for each change sampled. | No exceptions noted. |
| TVM-07.10 | Encrypted VPNs are required for remote access to production which require authentication through MFA protocols. | Inspected the VPN encryption and MFA configurations to determine that encrypted VPNs were required for remote access to production which required authentication through MFA protocols. | No exceptions noted. |
| TVM-07.11 | The system is configured to automatically enforce peer review and approval for software changes prior to implementation into the production environment. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period and the branch protection configurations for a sample of production branches to determine that the system was configured to automatically enforce peer review and approval for application changes to be reviewed prior to implementation into the production environment for each change sampled. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: TVM-08:** *Vulnerability Prioritization* - Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| TVM-08.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| TVM-08.02 | A change management meeting is held weekly to discuss and communicate the ongoing and upcoming projects that affect the system. | Inspected the meeting minutes for a sample of change management meetings held during the period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affect the system for each week sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| TVM-08.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| **CCM: TVM-09:** *Vulnerability Management Reporting* - Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification. | | | |
| **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. | | | |
| **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. | | | |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| TVM-09.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |
| TVM-09.02 | A change management meeting is held weekly to discuss and communicate the ongoing and upcoming projects that affect the system. | Inspected the meeting minutes for a sample of change management meetings held during the period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affect the system for each week sampled. | No exceptions noted. |
| TVM-09.03 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: TVM-10:** *Vulnerability Management Metrics* - Establish, monitor, and report metrics for vulnerability identification and remediation at defined intervals. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| TVM-10.01 | The performance, availability, and capacity of system resources and infrastructure are continuously monitored.  Operations personnel are alerted when defined monitoring conditions are detected. | Inspected the enterprise monitoring applications' configurations to determine that the performance, availability, and capacity of system resources and infrastructure were continuously monitored and that operations personnel were alerted when defined monitoring conditions were detected. | No exceptions noted. |

## Universal Endpoint Management

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: UEM-01:** *Endpoint Devices Policy and Procedures* - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints.  Review and update the policies and procedures at least annually. | | | |
| **CC2.1** COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| **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. | | | |
| UEM-01.01 | Endpoints are configured and managed using device management tools to enforce security requirements and protect against security threats. | Inspected the mobile device management (MDM) approved applications listing and restricted applications listing to determine that endpoints were configured and managed using device management tools to enforce security requirements and protect against security threats. | No exceptions noted. |
| UEM-01.02 | Policies are documented and maintained which require that only Zoom managed devices are allowed to access corporate data. | Inspected the mobile device policy and MDM settings to determine that policies were documented and maintained which required that only Zoom managed devices were allowed to access corporate data. | No exceptions noted. |
| UEM-01.03 | Policies are documented and maintained which prohibit the usage of unapproved application stores and require the use of anti-malware software (where supported). | Inspected the mobile device policy and MDM settings to determine that policies were documented and maintained which prohibited the usage of unapproved application stores and required the use of anti-malware software (where supported). | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| UEM-01.04 | Policies and procedures are documented that prohibit the circumvention of built-in security controls on mobile devices. | Inspected the mobile device policy and MDM settings to determine that policies and procedures were documented that prohibited the circumvention of built-in security controls on mobile devices. | No exceptions noted. |
| UEM-01.05 | Policies are documented and maintained which require the use of encryption either for the entire device or for data identified as sensitive on mobile devices and shall be enforced through technology controls. | Inspected the mobile device policy and MDM settings to determine that policies were documented and maintained which required the use of encryption either for the entire device or for data identified as sensitive on mobile devices and was enforced through technology controls. | No exceptions noted. |
| UEM-01.06 | Policies are documented and maintained which define the device and eligibility requirements to allow for BYOD usage. | Inspected the access control policy and MDM settings to determine that policies were documented and maintained which defined the device and eligibility requirements to allow for BYOD usage. | No exceptions noted. |
| UEM-01.07 | Policies are documented and maintained which prohibit the installation of non-approved applications or approved applications not obtained through a pre-identified application store. | Inspected the mobile device policy and endpoint management configuration to determine that policies were documented and maintained which prohibited the installation of non-approved applications or approved applications not obtained through a pre-identified application store. | No exceptions noted. |
| UEM-01.08 | Policies are documented and maintained that define the requirements for the classification, protection, and handling of data throughout its lifecycle. | Inspected the information security and information classification policies to determine that policies were documented and maintained that defined the requirements for the classification, protection, and handling of data throughout its lifecycle. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: UEM-02:** *Application and Service Approval* - Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-02.01 | Endpoints are configured and managed using device management tools to enforce security requirements and protect against security threats. | Inspected the MDM approved applications listing and restricted applications listing to determine that endpoints were configured and managed using device management tools to enforce security requirements and protect against security threats. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| UEM-02.02 | Policies are documented and maintained which prohibit the installation of non-approved applications or approved applications not obtained through a pre-identified application store. | Inspected the mobile device management policy to determine that policies were documented and maintained which prohibited the installation of non-approved applications or approved applications not obtained through a pre-identified application store. | No exceptions noted. |
| UEM-02.03 | Auditing applications are installed on Zoom managed mobile devices to prevent the installation of blacklisted software on those systems. | Inspected the auditing application configurations to determine that auditing applications were installed on Zoom managed mobile devices to prevent the installation of blacklisted software on those systems. | No exceptions noted. |
| **CCM: UEM-03:** *Compatibility* - Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-03.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| UEM-03.02 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| UEM-03.03 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| UEM-03.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: UEM-04:** *Endpoint Inventory* - Maintain an inventory of all endpoints used to store and access company data. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-04.01 | An inventory of managed mobile devices is maintained in Zoom's mobile device management systems. | Inspected the mobile device management system to determine that an inventory of managed mobile devices was maintained in Zoom's mobile device management systems. | No exceptions noted. |
| **CCM: UEM-05:** *Endpoint Management* - Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-05.01 | Zoom has the capability to apply patches to mobile devices that are managed by Zoom. | Inspected the mobile device listing and configurations for a sample device to determine that Zoom had the capability to remotely patch mobile devices that were managed by Zoom. | No exceptions noted. |
| UEM-05.02 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| **CCM: UEM-06:** *Automatic Lock Screen* - Configure all relevant interactive-use endpoints to require an automatic lock screen. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-06.01 | Policies are documented that require automatic timeout of unattended devices after an established period of inactivity. | Inspected the information security policy and mobile device policy to determine that policies were documented that required automatic timeout of unattended devices after an established period of inactivity. | No exceptions noted. |
| UEM-06.02 | BYOD and company-owned devices are configured to require an automatic lockout screen. | Inspected the session timeout configurations for an example mobile device to determine that BYOD and company-owned devices were configured to require an automatic lockout screen. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: UEM-07:** *Operating Systems* - Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes. | | | |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| **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. | | | |
| UEM-07.01 | Policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations are documented and maintained. | Inspected the release management and change management policies and procedures to determine that policies and standards for changes to company assets, including applications, systems, infrastructure, and configurations were documented and maintained. | No exceptions noted. |
| UEM-07.02 | A ticketing system is utilized to track and document changes throughout the change management process. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to track and document changes throughout the change management process for each change sampled. | No exceptions noted. |
| UEM-07.03 | Production system, application and maintenance changes made to in-scope systems are authorized, tested, and approved prior to implementation. | Inspected the change tickets for a sample of production application and infrastructure changes implemented during the period to determine that production system, application, and maintenance changes made to in-scope systems were authorized, tested, and approved prior to implementation for each change sampled. | No exceptions noted. |
| UEM-07.04 | Configuration artifacts are kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | Inspected the configurations and example alerts generated during the period from the FIM tool to determine that configuration artifacts were kept under version control, and systems alert on changes that deviate from the established baseline via FIM. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: UEM-08:** *Storage Encryption* - Protect information from unauthorized disclosure on managed endpoint devices with storage encryption. | | | |
| **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. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| UEM-08.01 | Policies are documented that require the enforcement of passwords on company devices and devices approved for BYOD usage. | Inspected the access control policy and mobile device policy to determine that policies were documented that required enforcement of passwords on company devices and devices approved for BYOD usage. | No exceptions noted. |
| UEM-08.02 | A PIN with a minimum length is enforced on the mobile devices managed by Zoom's MDM software. | Inquired of the senior compliance analyst regarding MDM configurations to determine that a PIN with a minimum length was enforced on the mobile devices managed by Zoom's MDM software. | No exceptions noted. |
| | | Inspected the MDM minimum length passcode policy to determine that a PIN with a minimum length was enforced on the mobile devices managed by Zoom's MDM software. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: UEM-09:** *Anti-Malware Detection and Prevention* - Configure managed endpoints with anti-malware detection and prevention technology and services. | | | |
| **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. | | | |
| UEM-09.01 | Production servers and registered endpoints are protected with a managed tool that scans for malicious code on a real-time basis and updates its detection definitions hourly. | Inspected the antivirus configurations to determine that production servers and registered endpoints were protected with a managed tool that scanned for malicious code on a real-time basis and updated its detection definitions hourly. | No exceptions noted. |
| **CCM: UEM-10:** *Software Firewall* - Configure managed endpoints with properly configured software firewalls. | | | |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| UEM-10.01 | Endpoints are configured and managed using device management tools to enforce security requirements and protect against security threats. | Inspected the MDM approved applications listing and restricted applications listing to determine that endpoints were configured and managed using device management tools to enforce security requirements and protect against security threats. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CCM: UEM-11:** *Data Loss Prevention* - Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment. | | | |
| **SOC 2 CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| UEM-11.01 | Policies and procedures are documented that prohibit the circumvention of built-in security controls on mobile devices. | Inspected the mobile device policy to determine that policies and procedures were documented that prohibited the circumvention of built-in security controls on mobile devices. | No exceptions noted. |
| | AWS and OCI are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zoom applications reside. | | |
| **CCM: UEM-12:** *Remote Locate* - Enable remote geo-location capabilities for all managed mobile endpoints. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-12.01 | Policies and procedures are documented that prohibit the circumvention of built-in security controls on mobile devices. | Inspected the mobile device policy to determine that policies and procedures were documented that prohibited the circumvention of built-in security controls on mobile devices. | No exceptions noted. |
| **CCM: UEM-13:** *Remote Wipe* - Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-13.01 | Zoom has the capability to remotely wipe mobile devices that are managed by Zoom. | Inspected the remote wipe configurations to determine that Zoom had the capability to remotely wipe mobile devices that were managed by Zoom. | No exceptions noted. |
| **CCM: UEM-14:** *Third-Party Endpoint Security Posture* - Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets. | | | |
| *No mapping to SOC 2 TSCs.* | | | |
| UEM-14.01 | Policies are documented and maintained which state the expectations regarding the loss of non-company data in the case a wipe of the device is required. | Inspected the mobile device policy and MDM settings to determine that policies were documented and maintained which stated the expectations regarding the loss of non-company data in the case a wipe of the device was required. | No exceptions noted. |
| UEM-14.02 | Employees are required to acknowledge that they have been given access to information governance and security policies and understand their responsibility for adhering to them before they may be granted access to organizational resources. | Inspected the code of conduct acknowledgements for a sample of newly hired employees during the period to determine that each employee sampled acknowledged that they were given access to the information governance and security policies and understood their responsibility for adhering to the associated policies before being granted access to organizational resources. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| UEM-14.03 | Zoom uses an MDM application for managing mobile devices to ensure that cloud-based services utilized by the company's mobile devices or BYOD are pre-approved for usage and the storage of company business data. | Inspected the MDM application configurations and the mobile device policy to determine that Zoom uses an MDM application for managing mobile devices to ensure that cloud-based services utilized by the company's mobile devices or BYOD were pre-approved for usage and the storage of company business data. | No exceptions noted. |
| UEM-14.04 | New third-party vendors are assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | Inspected evidence of vendor screening and management approval for a sample of vendors onboarded during the period to determine that each new third-party vendor sampled was assessed for risk prior to procurement to ensure they maintain compliance with security and availability commitments. | No exceptions noted. |

# SECTION 5

## OTHER INFORMATION PROVIDED BY ZOOM

# Management’s Response to Testing Exceptions

### Data Security and Privacy Lifecycle Management & Logging and Monitoring

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| DSP-01.06 | Information classifications and data ownership are defined in policies and procedures, which are reviewed annually for accuracy. | Inspected the data protection and loss standard, media protection policy, and data classification standard to determine that information classifications and data ownership was defined in the policies and procedures and were reviewed annually for accuracy. | The test of the control activity disclosed that the data protection and loss standard was not updated annually. |
| LOG-01.03 | A documented information security policy is in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | Inspected the data protection and loss prevention standard and the information security policy to determine that a documented information security policy was in place in support of data security across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. | |
| **Management’s Response:** | As of November 2022, Zoom Management reviewed and updated the Data Protection and Loss Standard to ensure it's updated with the latest minimum requirements.  This, along with the accompanying security standards will be formally reviewed and updated on at least an annual basis. | | |