REPORT ON RINGCENTRAL'S ON DEMAND UNIFIED COMMUNICATIONS SYSTEM AND GLIP COLLABORATION SYSTEM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE *PERIOD JANUARY 1, 2017 TO DECEMBER 31, 2017*

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Auditors

To RingCentral, Inc.:

Scope

We have examined RingCentral management's accompanying assertion that RingCentral maintained effective controls to provide reasonable assurance that:

- the RingCentral On Demand Unified Communications System and Glip Collaboration System were protected against unauthorized access, use, or modification to achieve RingCentral's commitments and system requirements
- the RingCentral On Demand Unified Communications System and Glip Collaboration System were available for operation and use to achieve RingCentral's commitments and system requirements
- the RingCentral On Demand Unified Communications System and Glip Collaboration System information was collected, used, disclosed, and retained to achieve RingCentral's commitments and system requirements

during the period January 1, 2017 to December 31, 2017 based on the criteria for security, availability, and confidentiality set forth in the 2016 edition of TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*). This assertion is the responsibility of RingCentral's management. Our responsibility is to express an opinion based on our examination.

During the period under review, RingCentral used multiple sub-service providers; Amazon Web Services for management and hosting of production servers and databases related to the Glip Collaboration System, Equinix for management and hosting of production servers and databases for the On Demand Unified Communications System, and Zoom to deliver its RingCentral Office online meeting platform. Consequently, certain controls are the responsibility of AWS, Equinix, and Zoom, and were not included within the scope of this examination.

RingCentral's assertion also indicates certain trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of RingCentral's controls are suitably designed and operating effectively, along with related controls at RingCentral. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

RingCentral is responsible for its commitments and system requirements and for designing, implementing, operating, and maintaining effective controls within the On Demand Unified Communications System and Glip Collaboration System to provide reasonable assurance that RingCentral's commitments and system requirements were achieved. RingCentral has also provided

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, RingCentral is responsible for selecting, and identifying in its assertion, the applicable trust services principles and criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services principles and criteria.

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, management's assertion is fairly stated. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of RingCentral's relevant security, availability, and confidentiality controls, (2) assessing the risks that controls were not effective to achieve RingCentral's service commitments and system requirements based on the applicable trust services principles and criteria, and (3) performing procedures to obtain evidence about whether controls within the system were effective to achieve RingCentral's commitments and system requirements based on the applicable trust services principles and criteria, and (4) performing such other procedures as we considered necessary. We believe that our examination provides a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services principles and criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, RingCentral management's assertion, referred to above, is fairly stated in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Cadence Assurance LLC

May 7, 2018
Salt Lake City, Utah

Section II – RingCentral's Assertion Regarding the Effectiveness of its Controls over the On Demand Unified Communications System and Glip Collaboration System

We, as management of RingCentral, are responsible for designing, implementing, operating, and maintaining effective controls over the RingCentral On Demand Unified Communications System and Glip Collaboration System to provide reasonable assurance that the commitments and system requirements related to security, availability, and confidentiality were achieved.

We have performed an evaluation of the effectiveness of the controls over the On Demand Unified Communications System and Glip Collaboration System throughout the period January 1, 2017 to December 31, 2017, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable criteria for security, availability, and confidentiality principles set forth in the 2016 edition of TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*). Based on this evaluation and the applicable trust services principles and criteria, we assert that the controls were effective throughout the period January 1, 2017 to December 31, 2017 to provide reasonable assurance that:

- the RingCentral On Demand Unified Communications System and Glip Collaboration System were protected against unauthorized access, use, or modification to achieve RingCentral's commitments and system requirements
- the RingCentral On Demand Unified Communications System and Glip Collaboration System were available for operation and use to achieve RingCentral's commitments and system requirements
- the RingCentral On Demand Unified Communications System and Glip Collaboration System information was collected, used, disclosed, and retained to achieve RingCentral's commitments and system requirements

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

RingCentral uses multiple subservice organizations in conjunction with providing the On Demand Unified Communications System and Glip Collaboration System. RingCentral utilizes Amazon Web Services for management and hosting of production servers and databases related to the Glip Collaboration System. In addition, RingCentral utilizes Equinix for management and hosting of production servers and databases for the On Demand Unified Communications System. Finally, RingCentral utilizes Zoom to deliver its RingCentral Office online meeting platform. The Description also indicates that certain trust services criteria specified therein can be met only if these subservice organizations' controls contemplated in the design of RingCentral's controls are suitably designed and

operating effectively along with related controls at RingCentral. Our testing procedures do not extend to controls of these subservice organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of RingCentral's controls are suitably designed and operating effectively, along with related controls at RingCentral. Our testing procedures do not extend to controls of user entities.

We assert that the controls within the On Demand Unified Communications System and Glip Collaboration System were effective throughout the period January 1, 2017 to December 31, 2017, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services principles and criteria.

RingCentral, Inc.
May 7, 2018

Section III – Description of RingCentral's On Demand Unified Communications System and Glip Collaboration System

SYSTEM OVERVIEW

RingCentral provides an on-demand cloud-based unified communications platform for businesses utilizing a Software as a Service (SaaS) business model (system). RingCentral's unified communications platform supports distributed workforces, mobile employees, and "bring-your-own" communications devices. RingCentral unifies the way customers communicate through mobile and desktop devices, text messaging, audio, video, and web conferencing as well as collaborating on projects with document sharing and team messaging. Through application programming interfaces (APIs) RingCentral systems are integrated with other cloud solutions for web and videoconferencing, contact center services, content sharing and collaboration and sales support and service.

Products and Services

Unified On Demand Communications System

The RingCentral Unified On Demand Communications System includes four products: RingCentral Office, RingCentral Professional, RingCentral Fax, and RingCentral Contact Center.

RingCentral Office: The RingCentral Office solution is a multi-location, multi-user, enterprise-grade communications solution that enables customers to communicate via different channels and on multiple devices. Businesses are able to seamlessly connect users working in multiple office locations on smartphones, tablets, PCs, and desk phones. RingCentral Office is sold in three editions: Standard, Premium, and Enterprise. The Standard Edition of RingCentral Office includes call management, mobile applications, voice, business SMS, team messaging and collaboration, business analytics and reporting, audio, video, and web conferencing capabilities, and integration with other cloud-based business applications such as Box, Dropbox, Google for Work, Microsoft Office365 and Outlook. Premium and Enterprise Editions include the Standard Edition functionality together with additional software integrations with other cloud-based business applications such as Salesforce CRM, Zendesk, Desk.com, high-definition voice, more advanced call routing for larger customers with multiple business units, and automatic call recording. Editions also vary in the number of included toll-free minutes and number of concurrent video and web conference meeting attendees. RingCentral Office customers also have RingCentral Global Office available.

Within the RingCentral application, every customer designates an 'administrator extension' that registers and authorizes other extensions and digital lines within that account. The administrator extension has the ability to make changes to user settings within that account. Customer endpoints provide SIP registration credentials to place VoIP calls. Customers enter their phone number and password when logging into the service through the web site, mobile application, and RingCentral's soft phones. Customers enter their PIN when accessing their extension via IVR. In addition, the application provides account access confirmation feature. This feature has a setting, which requires a secondary authentication in cases where the user workstation is not recognized as having been previously used to access the user extension.

RingCentral Professional: The RingCentral Professional solution provides a subset of the RingCentral Office solution capabilities designed primarily for smaller businesses. RingCentral Professional is principally used as an inbound, call-routing solution with text and fax capabilities.

RingCentral Fax: The RingCentral Fax solution provides Internet fax capabilities that allow businesses to send and receive fax documents without the need for a fax machine.

RingCentral Contact Center: The RingCentral Contact Center solution provides a cloud-based contact center solution that delivers multichannel capabilities so businesses can allow customers to engage in the manner they prefer. The solution leverages technology from InContact and has a comprehensive feature set that integrates with RingCentral Office. The scope of this report does not include the Contact Center. RingCentral performs a separate review of InContact's security reports.

Glip Collaboration System

Glip is a provider of cloud-based team messaging services, integrated with project management, group calendars, notes, annotations, and file sharing. Through an integration with RingCentral, Glip extends the RingCentral platform, which provides communication capabilities across multiple channels, including voice, text, team messaging collaboration, HD video for web conferencing and fax. Glip also includes integrations with a number of third-party business solutions such as Asana, Dropbox, Evernote, JIRA, Github, Zendesk, Google, and others.

Glip is both a feature of RingCentral Office and a standalone collaboration offering. RingCentral Office customers receive Glip integrated with RingCentral Telephony and Video Conferencing features as part of the RingCentral Unified Communications as a service offering. The Glip service is available on the web, as a Mac and Windows desktop application, and as a mobile app available on both the iOS App Store and Google Play Store.

SYSTEM COMPONENTS

The RingCentral system supports hundreds of thousands of users and is currently managing over ten billion minutes of voice traffic per year. The system is built on a highly scalable and flexible infrastructure comprised of commercially available hardware and software components. Both hardware and software components of the platform can be replaced, upgraded, or added with minimal or no interruption in service. The system is designed to have no single point-of-failure.

The RingCentral system leverages a modular point of data (pod) design, which enables the seamless integration of additional pods as the subscriber base grows. This design permits new user groups to be added without the need to take the system offline to rebuild databases or add new servers. This pod design also incorporates a virtual chassis, which optimizes traffic with a direct-path algorithm.

Network application triggers alert the Network Operations team when a reallocation of resources is required, and the entire system is constantly monitored for bottlenecks or other blockages.

Infrastructure

Unified On Demand Communications System

Data Centers: RingCentral leverages Equinix as a third-party data center provider with sites around the world. These data centers are designed to host mission-critical computer and communications systems with redundant, fault-tolerant subsystems and compartmentalized security zones. Management maintains a security program designed to ensure the security and integrity of customer data, protect against security threats or data breaches, and prevent unauthorized access to customer data. Access is restricted to on-demand servers and networks at production and remote backup facilities.

Each data center undergoes separate System and Organizational Control (SOC) or ISO 27001 attestations by independent auditors annually to evaluate the design and operating effectiveness of the data centers' physical and environmental safeguards. RingCentral obtains and reviews the data centers' SOC or ISO reports, and evaluates the data centers' controls and any relevant exceptions noted in these audit reports to assess the impact on RingCentral's control environment.

RingCentral's Operations team provides a list of authorized personnel for physical access to colocation data centers where production infrastructure is located. Physical access controls for production infrastructure include 24x7x365 on-site security guards, sign-in logs, biometric scans, key card scans, and CCTV cameras.

Service Resilience and Recovery and Backup: RingCentral's data centers are commercially available centers with private space for RingCentral equipment. The data centers have full redundancy on production environments, are zone-4 conditioned for earthquakes and carry a minimum of three days of on-site fuel. In addition, the RingCentral services in the data centers are fault tolerant to each other, which enables us to continue providing back-office systems such as e-commerce sign-ups, support portal, billing and revenue collection, and complete service operability in the event required. With real-time database replication between locations and failover built into the service, RingCentral can continue business operations and service functionality completely within one site with minimal reconfiguration. RingCentral has a private production backbone to protect data replication between data centers.

Network Architecture and Management: RingCentral's network and application perimeter are implemented via firewalls and session border controllers. RingCentral implements network load balancing that distributes web application traffic across web server farms. RingCentral deploys session border controllers for a resilient VoIP border. The session controllers inspect and throttle both high volumes of VoIP registration traffic and anomalous registration traffic.

RingCentral has implemented system hardening practices and has additionally automated the ongoing assessment of production server and network device configurations.

RingCentral maintains a staffed NOC to continuously monitor the status of its operating networks for both systems and voice components.

A secure VPN border segments production access from other corporate networks. Access to RingCentral's production network is restricted to authorized personnel. RingCentral Operations staff enter their production VPN credentials to access the production network and production systems.

Glip Collaboration System

The Glip system is hosted by Amazon Web Services (AWS). Glip resides within a virtual private cloud hosted by AWS (Glip VPC) that spans multiple AWS Availability Zones. The Glip VPC is logically isolated from other virtual networks in the AWS cloud. The virtual network closely resembles a traditional network with the benefits of using the scalable infrastructure of AWS.

Network load balancing is implemented to distribute web application traffic across the system's web server farms. This Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple AWS instances. ELB enables Glip to achieve fault tolerance in the system, seamlessly providing the required amount of load balancing capacity needed to route application traffic.

System servers responsible for communicating data and events to and from Glip users have been optimized for input/output speeds. The Glip system is currently running a hardened version of Amazon's Linux. The system is designed so that the majority of its business logic resides within API instances that communicate directly with its databases.

To provision a new user account on Glip, any co-worker in a company that already has an account on Glip can simply join without an invitation, so long as that company account was set up with a private email domain (e.g., Acme.com). In the case where users with differing email domains wish to collaborate through Glip, the company or team with an existing Glip account must simply send the new user an invitation to join. For RingCentral Office customers, a Glip account is automatically provisioned for every user with a RingCentral Office phone extension (assuming that they did not already have an account) when the first person from that company signs into Glip using their RingCentral credentials.

Once a user is on Glip, only one of the customer's Glip administrators can remove a Glip user. By default, the first person to sign up for Glip from a given company or team becomes the administrator of that Glip account, and that person can then make other users administrators. For RingCentral Office customers, users who are administrators in the company's RingCentral Office account are automatically designated as the Glip administrators.

People

RingCentral hires highly skilled personnel to meet business goals and offer a reliant and secure service. Formal organizational structures exist and are maintained by Human Resources team. RingCentral has developed cross functional, efficient and quality teams across the company to deliver their products to customers. RingCentral has formal policies and documentation in place for operational areas including security monitoring and administration. All employees have access to the security documentation upon hire and throughout their employment period via the internal employee site.

The RingCentral Operations Department is primarily responsible for system security, confidentiality, and availability. The Security team is part of RingCentral's Operations team. The Security team primarily leads all security and compliance initiatives and works collaboratively with other teams in the company to meet security objectives. RingCentral's Security team maintains, develops, operates,

monitors, and reviews security and fraud-related controls. The security team maintains the company Security Policy and supporting standards.

Procedures

Security Management: RingCentral has a dedicated Security team responsible for management of security throughout the organization, which includes developing, maintaining, and enforcing RingCentral's security policies.

System Account Management: RingCentral has implemented role-based security to limit and control access within the production environment. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user accounts and user privileges is limited to authorized administrators. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts. Access to applications requires two-factor authentication.

System Monitoring: The Security team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, SIEM alerts, DNS analytics, telco fraud analytics, vulnerability assessment reports, EDR (Endpoint detection and response) and anti-malware events, and operating system event logs. The Security team reviews these alerts and notifications daily by using a security incident and event monitoring (SIEM) product.

Change Management: RingCentral has implemented a change control policy and conducts weekly Change Management Board meetings to review and manage changes to its production environment. Cases are opened to track development of system changes. Stakeholders participate in the design and planning of system-related changes. Prior to deployment into production, the change control process is followed, including documented change requests and approval by multiple stakeholder teams during the Change Management Board review. RingCentral's software development activities include internal and external application security testing.

Data

RingCentral has established an information classification policy within its Information Security Policy document that categorizes data based on its criticality and sensitivity. That classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements. Management reviews and approves the RingCentral information classification policy at least annually. Reviews are documented in the Revision History table contained within the policy.

Data is retained based on the agreements signed with individual customers & per the required laws and regulations. RingCentral provides an API tool for customers to export their data to meet their internal data retention compliance requirements.

Sub-Service Organizations

AWS: RingCentral utilizes AWS to support the Glip Collaboration System cloud computing environment. AWS provides a secure IT infrastructure for compute power, storage, and other application services over the internet. Authentication controls to the AWS admin console are controlled by the AWS Identity and Access Management (IAM) tools. RingCentral reviews AWS's SOC 2 audit reports to gain comfort over its security controls.

Equinix: Colocation facilities chosen to locate the On Demand Unified Communication System computer systems and network devices are suitably protected from physical intrusion, theft, fire, flood, excessive ambient temperature, humidity, electromagnetic disturbance, and other hazards, and are safe for RingCentral personnel and visitors. RingCentral reviews Equinix's SOC 2 audit reports to gain comfort over its security controls.

Zoom: RingCentral has partnered with Zoom to deliver its RingCentral Office platform. Zoom provides the core technology used by RingCentral with the meetings hosted on both RingCentral's and Zoom's infrastructure. RingCentral reviews Zoom's SOC 2 audit report to gain comfort over its security controls.

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

Control Environment

RingCentral's control environment reflects the philosophy of senior management concerning the importance of protecting data and information. RingCentral's Security Council meets quarterly and the security department reports to the board annually. This council oversees the security activities of RingCentral. The committee members are business leadership from a cross section of business lines. The importance of security is emphasized within RingCentral through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out these policies.

Management Controls: RingCentral has defined responsibilities for development, implementation, and maintenance of its security program and has also defined responsibilities for governance and oversight. These responsibilities are documented in RingCentral's Security Policy.

In designing its controls, RingCentral has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Policies: The RingCentral Security team maintains the company Security Policy outlining the security-related roles and responsibilities of company employees. This policy is reviewed and approved annually.

Risk Assessment

RingCentral regularly reviews the risks that may threaten the achievement of its business objectives. Changes in security threats and risks are reviewed by RingCentral, and updates to existing control activities and information security policies are performed as necessary.

Information and Communication Systems

RingCentral has an Information Security policy to help ensure employees understand their individual roles and responsibilities. Formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes ensure key personnel are notified in the event of problems. Additional methods of communication further ensure employees understand their roles and responsibilities and ensure that important information and events are communicated to management.

RingCentral has also established methods of communicating information about RingCentral, its products and services, and its policies to customers. The primary conduit of communicating to customers is RingCentral's web site, including RingCentral's online End-User License Agreement Terms of Service (EULA TOS), RingCentral's Privacy Notice, RingCentral's Security website, RingCentral support sites, customer communications from RingCentral's Customer Marketing Department, RingCentral's blog, and the company's social media channels.

Monitoring Controls

RingCentral's Security team monitors for anomalous and unauthorized use of customer accounts. In addition to the daily oversight, ongoing vulnerability assessments, and use of SIEM (security information and event management) technology, the Security team provides further security monitoring by reviewing metrics weekly at departmental staff meetings.

RingCentral's Security team also maintains tools and procedures for detecting and resolving toll fraud and security incidents, including anomalous and unauthorized use of customer accounts. Operations personnel maintain tools and procedures for identifying and responding to operational availability risks and service interruptions.

The RingCentral NOC continuously monitors the network and customer input for security and service-impacting issues. RingCentral's NOC also utilizes various tools to monitor, maintain, and resolve issues related to system availability.

Upon detecting a potential security or service-impacting issue, including outages, NOC personnel verify the symptoms are not an anomaly or false alert. This verification process may require the use of multiple monitoring and troubleshooting tools. The incident is logged via a tracker that describes the security or service-impacting issue. NOC personnel quickly define the nature, scope, and priority of the detected incident. They log the issue information in the Incident Management Portal, which notifies the appropriate personnel and tracks the issue through to resolution.

Complementary User Entity Controls

RingCentral's control environment was designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities RingCentral believes should be present at each customer and has considered in developing its controls reported on herein. RingCentral customers should evaluate their own control environment to assess if the following controls are in place. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by RingCentral customers, but are rather a summary of controls necessary to meet the stated trust services principles and criteria presented in this report.

- User entities are responsible for managing their application settings, user permissions, and login information.
- User entities are responsible for designating an administrator extension and Glip administrator accounts.
- User entities are responsible for securing communications with their email system.
- User entities are responsible for recordings on their end points and data retention.

Complementary Subservice Organization Controls

RingCentral uses subservice organizations in conjunction with providing the On Demand Unified Communications System and Glip Collaboration System. RingCentral utilizes Amazon Web Services for management and hosting of production servers and databases related to the Glip Collaboration System. In addition, RingCentral utilizes Equinix for management and hosting of production servers and databases for the On Demand Unified Communications System. RingCentral utilizes Zoom to deliver the RingCentral Office platform. Controls managed by these third-party subservice providers are not included in the scope of this report. The affected criteria are included below along with the controls expected to be in place at the subservice providers.

Criteria	Controls expected to be in place at the relevant subservice provider		
	AWS	Zoom	Equinix
CC5.1 – Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Access to the in-scope systems requires users to authenticate using a valid unique user ID and password before being granted access.	Access to the in-scope systems requires users to authenticate using a valid unique user ID and password before being granted access.	Not Applicable

Criteria	Controls expected to be in place at the relevant subservice provider		
	AWS	Zoom	Equinix
CC5.2 – New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials, and granted the ability to access the system, to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	User accounts are approved by appropriate individuals prior to being provisioned.	User accounts are approved by appropriate individuals prior to being provisioned.	Not Applicable
CC5.3 – Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Users are authenticated prior to accessing system components.	Users are authenticated prior to accessing system components.	Not Applicable
CC5.4 – Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	User accounts are removed when access is no longer needed or users are terminated. User accounts are reviewed on a regular basis by appropriate personnel.	User accounts are removed when access is no longer needed or users are terminated. User accounts are reviewed on a regular basis by appropriate personnel.	Not Applicable

Criteria	Controls expected to be in place at the relevant subservice provider		
	AWS	Zoom	Equinix
CC5.5 – Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Only authorized users have access to the physical facilities housing the system.	Only authorized users have access to the physical facilities housing the system.	Only authorized users have access to the physical facilities housing the system.
CC5.6 – Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Network security mechanisms are in place to restrict external access to the production environment.	Network security mechanisms are in place to restrict external access to the production environment.	Not Applicable
CC5.7 – The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	Customer data is protected during transmission, movement, and removal.	Customer data is protected during transmission, movement, and removal.	Not Applicable
CC5.8 – Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and requirements as they relate to security, availability, and confidentiality.	Anti-virus or anti-malware applications are installed to detect or prevent unauthorized or malicious software.	Anti-virus or anti-malware applications are installed to detect or prevent unauthorized or malicious software.	Not Applicable

Criteria	Controls expected to be in place at the relevant subservice provider		
	AWS	Zoom	Equinix
CC6.1 – Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Vulnerabilities are logged, assigned severity rating and tracked to resolution.	Vulnerabilities are logged, assigned severity rating and tracked to resolution.	Not Applicable
CC6.2 – Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Incidents are logged, assigned severity rating and tracked to resolution.	Incidents are logged, assigned severity rating and tracked to resolution.	Not Applicable
CC7.4 – Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.	System changes are documented, tested, and approved prior to migration to production.	System changes are documented, tested, and approved prior to migration to production.	Not Applicable

Criteria	Controls expected to be in place at the relevant subservice provider		
	AWS	Zoom	Equinix
A1.1 – Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Monitoring processes alert appropriate personnel when capacity thresholds are exceeded.	Monitoring processes alert appropriate personnel when capacity thresholds are exceeded.	Not Applicable
A1.2 – Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Environmental protections, including backup controls are implemented in the production environment.	Environmental protections, including backup controls are implemented in the production environment.	Environmental protections, including backup controls are implemented in the production environment.
A1.3 – Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Backups are tested.	Backups are tested.	Not Applicable
C1.3 – Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Encrypted communication is required for connections to the production system.	Encrypted communication is required for connections to the production system.	Not Applicable
C1.7 – The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Customer data is retained as requested.	Customer data is retained as requested.	Not Applicable
C1.8 – The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Customer data is deleted or anonymized upon request.	Customer data is deleted or anonymized upon request.	Not Applicable