RingCentral

RingCentral Office and RingCentral Video
Systems and Organization Controls (SOC 3)
For Controls Relevant to Security, Availability, and Confidentiality,

For the Period January 1, 2020 to December 31, 2020

THE cadence GROUP

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 Service Auditors

To: RingCentral, Inc.

Scope

We have examined RingCentral's accompanying assertion, titled "RingCentral's Assertion" (assertion), that the controls within RingCentral's Office and Video Products were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

RingCentral 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 RingCentral's service commitments and system requirements were achieved. RingCentral has provided 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 criteria, and for having a reasonable basis for its assertion by performing an assessment of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria

THE cadence GROUP

O 801.349.1360
F 866.326.6612

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

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

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 are achieved based on the applicable trust services 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 policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within RingCentral's system were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

Cadence Assurance LLC

June 30, 2021
Salt Lake City, Utah

Section II – RingCentral's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within RingCentral's Office and Video Products throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). RingCentral's objectives for the system, in applying the applicable trust services criteria, are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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

We assert that the controls within the system were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria.

RingCentral, Inc.
June 30, 2021

Attachment A – RingCentral's Description of the Boundaries of RingCentral Office and RingCentral Video Products

Company Overview

RingCentral is a leading provider of global enterprise cloud communications, collaboration, and contact center solutions. RingCentral products empower employees to work better together, from any location, on any device, and via any, improving business efficiency and customer satisfaction. The company provides unified voice, video meetings, team messaging, digital customer engagement, and integrated contact center solutions for enterprises globally.

System Description

RingCentral Office

RingCentral Office (RC Office) is a cloud-based business communications system with enterprise-grade voice, fax, text, online meetings, conferencing, and collaboration. RC Office integrates phone, fax, video, meetings, and messaging in one reliable, easy-to-use solution. With RC Office, customers can easily connect their office, remote, and mobile employees under one phone system, regardless of their location. Key features of RC Office include:

- Multi-tenant unified communications as a service (UCaaS) solution combining enterprise-grade telephony, team messaging and collaboration, audio conferencing, high-definition video meetings, webinars, business SMS / MMS, and fax.
- Smartphone, tablet, PC, and desk phones compatibility.
- Global coverage in 120+ countries.
- 200+ public integrations available with several leading productivity (Google, Office 365), automation (Okta, Box), customer relationship management (Salesforce, Microsoft Dynamics), and customer support (Zendesk, ServiceNow) apps.
- Open application program interfaces (API) and software development kits (SDK) for custom integrations.
- In-depth analytics designed for IT admin and line of business.
- Full range of network connectivity options to customers, including software-defined networking (SD-WAN).

RingCentral Video

RingCentral Video (RCV) is a virtualized meetings experience powered by RingCentral unified communications platform. It combines high-quality video, audio, screen sharing, and team messaging into a collaborative online meeting hub— anytime, anywhere, on any device. Key RCV features include:

- HD audio and video
- Powerful browser-based video meetings — no downloads needed
- Mobile and desktop meeting client with presence and instant messaging
- Interactive multimedia content and screen sharing cloud meetings recording

- In-meeting public and private chat
- Up to 200 interactive video participants
- Voice over Internet Protocol ("VoIP") with call-in and call-out audio options
- Quality-of-service analytics and usage insights
- Background noise reduction
- Personal meeting ID
- Open APIs
- Integration with Office 365 and Google Calendar
- Integration with Microsoft Teams, Salesforce, Slack, and other business apps
- Integration with RC Office

System Boundaries

Systems within the scope of this report include production, infrastructure, software, people, procedures, and data supporting RC Office and RCV.

Subservice Organizations

RC Office uses the following subservice organizations:

Amazon Web Services –Amazon Web Services (AWS) supports the RC Office messaging cloud computing environment.

Equinix – Colocation facilities supporting RC Office production systems and network devices are protected from physical intrusion, theft, fire, flood, excessive ambient temperature, humidity, electromagnetic disturbance, and other hazards.

Google Cloud Platform –Google Cloud Platform (GCP) supports the product's live reports feature, which allows customers to manage queues, quality of service, service level agreements (SLAs), and peak hours.

NICE –NICE CXone, a cloud native contact center software, supports RingCentral's customers by providing the RC Contact Center feature, which allows customers to connect via an omni-channel solution through voice, text, chat, and email.

Zoom – RingCentral has partnered with Zoom to deliver RC Meetings, providing core technology used by RingCentral with the meetings hosted on both RingCentral's and Zoom's infrastructure. RC Meetings is used as an alternative to RCV, also available within RC Office. Effective mid-year 2020, new RC Office customers will default to RCV for video meeting functionality.

RCV uses the following subservice organizations:

Amazon Web Services –AWS provides a secure IT infrastructure for compute power, storage, and other application services over the internet, as well as storage of RCV recordings.

Equinix – Please see Equinix service description above.

NICE – Please see NICE service description above.

With respect to AWS, Equinix, GCP, NICE, and Zoom, these subservice organizations are excluded from the scope of this report. The controls they are responsible are included in Attachment D, entitled *Complementary Subservice Organization Controls*.

Infrastructure

System descriptions delineate the boundaries of the system, describe relevant system components, and outline the purpose and design of the system. RC Office and RCV operating system and storage infrastructure is powered by modern component types. RC Office, production databases contain customer data, metadata, and video meeting metadata/history. RCV, production databases contain video, history, and metadata.

Data Centers

North America customer environments are hosted in five third-party US-based data center facilities in Santa Clara, California, San Jose, California, Ashburn, Virginia, Vienna, Virginia and Chicago, Illinois. Europe customer environments are hosted in two third-party data center facilities in Amsterdam, Netherlands, and Zurich, Switzerland. Outside of North America and Europe, customer environments are hosted in one of seven major data centers listed above depending on proximity.

Data centers host mission-critical computer and communications systems with redundant, fault-tolerant subsystems and compartmentalized security zones. Management maintains a security program designed to help ensure the security and integrity of customer data, protect against security threats, and prevent unauthorized access to customer data. Access is restricted to on-demand servers and networks at production and remote backup facilities. See Figures 1 & 2 for diagrams of data center interconnectivity and data center network design.

Network and Database Architecture and Management

RingCentral's network and application perimeter are secured via firewalls and session border controllers (SBCs). In addition, RingCentral has network load balancing that distributes web application traffic across web server farms.

For RC Office, RingCentral deploys SBCs for a resilient VoIP border. SBCs inspect and throttle both high volumes of VoIP and anomalous registration traffic. For RCV, user dialing in via the RC Office application, call traffic routes through SBCs.

Figure 1: Overview of RingCentral's Data Center Network Design

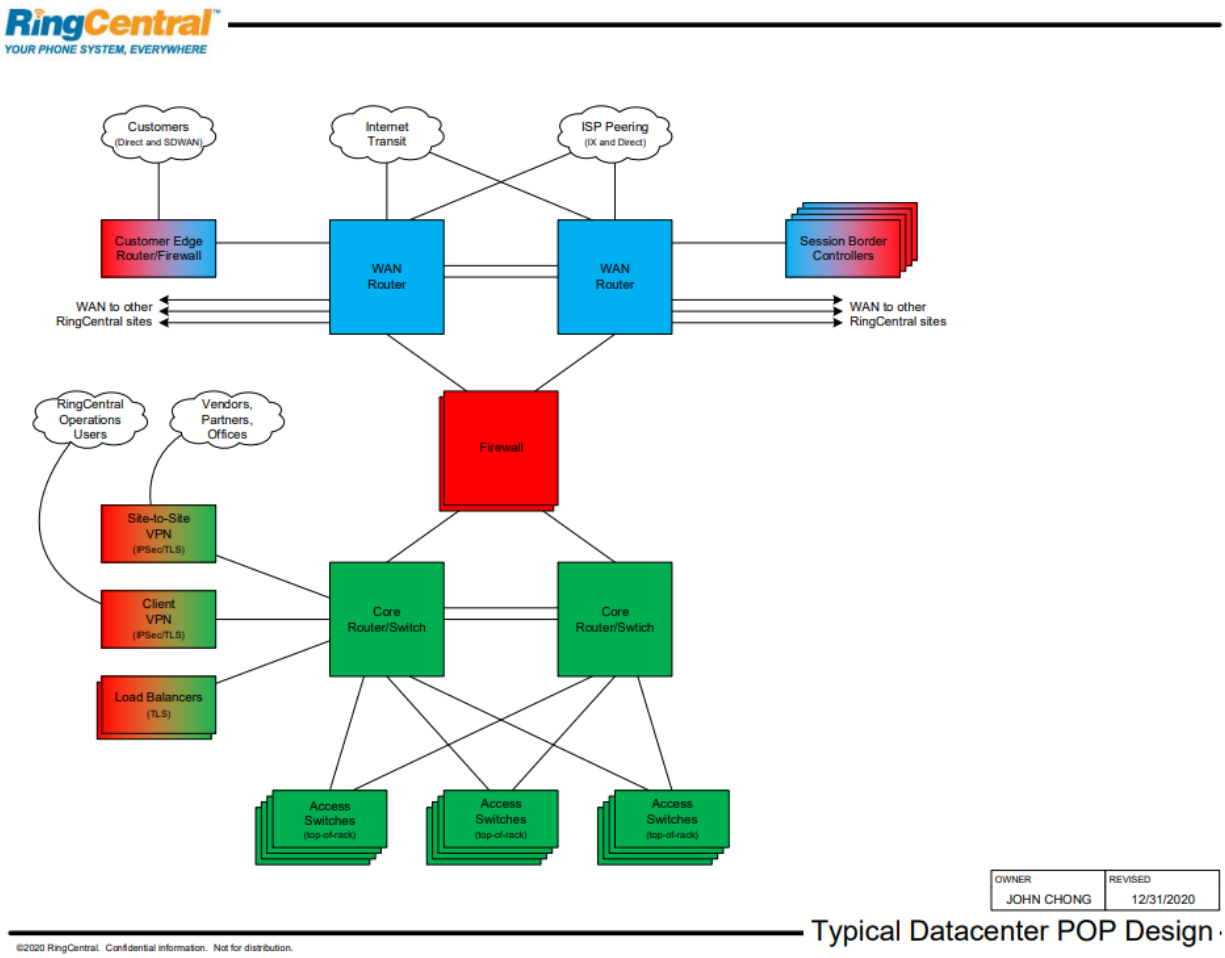
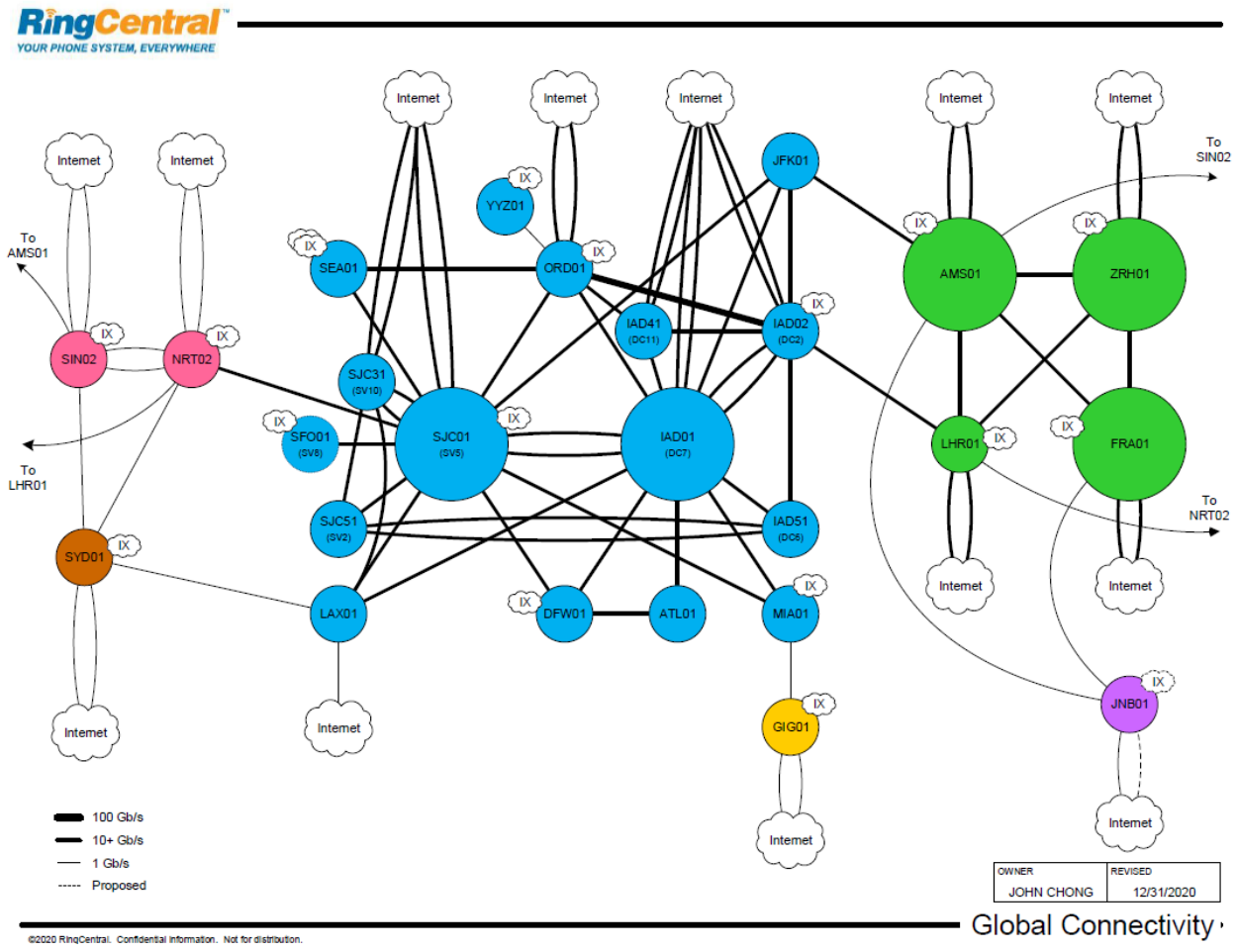


Figure 2: Overview of RingCentral's Data Center Interconnectivity



Messaging Infrastructure

The Messaging feature provided as part of RC Office is hosted by AWS. Backups of critical data are maintained in a geographically separate region. The production environment spans three AWS Availability Zones (separate distinct locations) to ensure resiliency, leveraging AWS' low-latency network connectivity between Availability Zones within the same region.

Software

IT & Security System Software

RC Office and RCV are supported by the following software and types of software:

- Threat Management
- Logging
- Monitoring
- Application Security
- Network Protection
- Vulnerability Testing and Vulnerability Management
- System User Authentication and Access Management
- Change Configuration Management

People

The primary responsibility of the Security team is to design, implement, and maintain information security measures for RingCentral. This team is tasked with the designing, implementing, and maintaining information security measures for RingCentral.

The Operations teams consists of the following:

- Architectural Operations (ArchOps)
- Database Administrators (DBAs)
- Network Operations (NetOps)

The roles and responsibilities of the Information Technology (IT) division include the Corporate IT Infrastructure and the IT Global Service Desk (GSD) teams. The Site Reliability Engineering (SRE) division includes System Operations (SysOps), Development Operations (DevOps), and the Network Operations Center (NOC) teams.

Global Support Services (GSS) is responsible for assisting customers troubleshoot issues with their account and service usage related problems. GSS utilizes the Admin Web Utility to access customer accounts. Human Resources (HR) is responsible for onboarding, background checks, recruitment, training, evaluations, compensation, and development.

Nordigy, ABSoft, and Acquire act as subcontractors and execute controls on behalf of RingCentral under the oversight of RingCentral's management. RingCentral communicates its security, confidentiality, and availability requirements of Nordigy, ABSoft, and Acquire through its contracts. These subcontractors provide aspects of engineering, operations, development, quality assurance, and customer support.

Procedures

RingCentral maintains the following key policies and procedures related to RC Office and RCV's security, availability, and confidentiality operations:

- Information Security Policy
- Active Directory-SSL VPN Access Policy
- User Accounts Management on Databases
- Access Control Policy
- Change Management Policy
- Secure SDLC Policy
- Backup Retention Policy
- Security Incident Response Guide
- Hardening Procedures
- Incident Management Policy
- Security Incident Response Plan
- Security Policy
- Risk Assessment Policy
- Data Retention Policy and Procedure
- Vulnerability Management and Patch Management Policy
- Network Access Policy

Data

Key types of customer content collected by RC Office include text messages, faxes, attachments, voicemails, transcripts, messages, message attachments, video recordings, and video meeting transcripts. Key types of service data collected by RC Office include account data (including customer name and email address), usage data, call detail records (CDRs), and metadata (including time, recipient, sender, and location) associated with faxes, voicemails, and call recordings.

Key types of data collected by RCV include access tokens for calendar integration, chat messages, participants' names, account IDs, extension IDs, phone numbers, list of rooms and room statuses, and meeting recordings.

RingCentral provides an API for customer data-export to support data retention compliance requirements. Service data is retained based on the Data Retention Policy and Procedure. Troubleshooting with service data requires a service ticket.

RingCentral has established an Information Classification Policy within its Information Security Policy that categorizes data based on criticality and sensitivity. That classification is used to define protection requirements, access rights and restrictions, and retention and destruction requirements. For account terminations, customer content and service data are deleted within 45 days for RC Office and RCV.

Internal Control Framework

RingCentral has adopted the following control framework to meet its security, availability, and confidentiality commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Additionally, complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at RingCentral, to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria. See Attachment C for identified complementary user entity controls.

Control Environment

An organization's control environment represents the attitude, awareness, and actions of the board of directors, executive management, and other key stakeholders concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, operations, and organizational structure.

The board of directors includes executive management and external advisors, who are independent from the company's operations. The Audit Committee, which includes independent members of the board of directors, meets semi-annually to review company financial and operational results and discuss organizational risks. On a quarterly basis, the Security team communicates significant security findings related to risk assessments and control evaluations with the executive leadership team and key members of the board of directors.

Risk Assessment

RingCentral regularly reviews the risks that may threaten the achievement of the criteria for the security, availability, and confidentiality categories set forth in the AICPA's Trust Services Criteria. Changes in security threats and risks are reviewed by RingCentral, and updates to existing control activities and security policies are performed as necessary.

Control Activities

Controls have been implemented to address system and data risks. Controls have been designed and implemented in the following areas:

- Onboarding and Terminations
- Logical Access
- Encryption
- Network Security
- Vulnerability Management
- Configuration Management
- Physical Security / Environmental Controls
- System Monitoring
- Incident Management
- Change Management
- Business Continuity and Recovery
- Availability
- Data Management

Information and Communication

RingCentral's Information Security Policy ensures employees understand individual roles and responsibilities. Formal and informal training programs and 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 ensure important information and events are communicated to management.

The Security team implements a security and fraud prevention program based on industry best practices. Customers report security incidents via the Customer Support team, which escalates incidents related to fraud and service abuse to the Security Fraud team. Carrier partners report incidents directly to the Security Fraud team via emails. The Security Fraud team documents and tracks fraud incidents to resolution and performs an assessment of any potential unintended disclosure of sensitive information. The Security team utilizes tools and documented procedures for detecting and resolving security incidents. Procedures are maintained to act upon security breaches that threaten system security. The procedures are defined in the Security Incident Response Guide. In addition, RingCentral's Security team staffs dedicated personnel for handling fraud cases inbound from customers.

RingCentral has established methods of communicating information about RingCentral, its products and services, and its policies to customers. Specifically, RingCentral provides onboarding guides to new customers to assist them in establishing and maintaining their accounts. The primary conduit of communicating to customers is RingCentral's website including RingCentral's online End-User License Agreement Terms of Service (EULA ToS), Data Protection Agreement, 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

RingCentral has implemented monitoring controls to periodically evaluate operating effectiveness of its internal controls. These controls include annual certification assessments, penetration tests, and vulnerability scans. High-risk findings are shared with executive leadership and corresponding remediation actions are tracked to resolution.

Attachment B – Principal Service Commitments and System Requirements

RingCentral policies, procedures, and processes ensure security, availability, and confidentiality of services and has established programs to help ensure compliance with various laws, regulations, and frameworks, including FINRA cybersecurity regulations, HIPAA Security Rule requirements, and National Institute of Standards and Framework's Cybersecurity Framework (NIST CSF) standards.

RingCentral commitments to security, availability, confidentiality and the aforementioned frameworks are documented and communicated to customers on the RingCentral website and as requested. In addition, third-party service providers with access to ePHI sign business associate agreements (BAAs) which require business associates to appropriately safeguard information and report any security incidents. Security, availability, and confidentiality commitments are further communicated to customers in Terms of Service, contractual agreements, and located on the RingCentral website.

RingCentral has adopted a control framework. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring outlined in Attachment A.

Attachment C – Complementary User Entity Controls

RingCentral's controls were 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 herein. RingCentral customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by RingCentral customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- User entities are responsible for managing their account policies, user permissions, and login information.
- User entities are responsible for designating an administrator extension (phones numbers).
- User entities are responsible for the settings on their extensions.
- User entities are responsible for securing communications with their email system.
- User entities are responsible for implementing single sign-on.
- User entities are responsible for their account and meeting configurations.

Attachment D – Complementary Subservice Organization Controls

RingCentral uses multiple subservice organizations in conjunction with providing RC Office and RCV. RC Office uses Amazon Web Services (AWS) for cloud computing and storage, Equinix for colocation services, Google Cloud Platform (GCP) to support the live reports feature in RC Office, NICE for contract center software, and Zoom to deliver its RC Office platform. RCV uses AWS for storage of RCV recordings, Equinix for colocation services, and NICE for contact center software. Controls managed by these third-party subservice providers are not included in the scope of this report. Expected subservice provider controls that have an effect on specific trust services criteria include the following:

AWS, GCP, NICE, Zoom:

- Access to hosted systems requires strong authentication mechanisms.
- New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to be granted.
- Terminated user access permissions to hosted systems are removed in a timely manner.
- User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.
- Privileged access to hosted systems and the underlying data is restricted to appropriate users.
- Access to the physical facilities housing hosted systems is restricted to authorized users.
- Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
- Network security mechanisms restrict external access to the production environment to authorized ports and protocols.
- Connections to the production environment require encrypted communications.
- Antivirus or antimalware solutions detect or prevent unauthorized or malicious software on hosted systems.
- System configuration changes are enforced, logged, and monitored.
- Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution.
- System activities on hosted systems are logged, monitored and evaluated for security events. Any identified incidents are contained, remediated and communicated according to defined protocols.
- Access to make changes to hosted systems is restricted to appropriate personnel.
- Changes to hosted systems are documented, tested, and approved prior to migration to production.
- Personnel monitor processing and system capacity on hosted systems.
- Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner.
- Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.
- Software and recovery infrastructure are implemented over hosted systems.

Equinix:

- Access to the physical facilities housing hosted systems is restricted to authorized users.
- Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
- Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.