RingCentral®

REPORT ON RINGCENTRAL'S OFFICE PRODUCT RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE PERIOD JANUARY 1, 2019 TO DECEMBER 31, 2019

ISSUED ON MAY 11, 2020

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 Product were effective throughout the period January 1, 2019 to December 31, 2019, 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.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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, 2019 to December 31, 2019, 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

May 11, 2020
Salt Lake City, Utah

Section II – RingCentral's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within RingCentral's Office Product throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that RingCentral's service commitments and system requirements relevant to security, availability, and confidentiality were achieved.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to December 31, 2019, 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.

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, 2019 to December 31, 2019, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria.

RingCentral, Inc.
May 11, 2020

Section III – Description of the RingCentral Office Product

Company 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 employees 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.

RingCentral was founded in 1999 and is headquartered in Northern California. RingCentral provides flexible, cost-effective cloud communications and collaboration solutions. RingCentral has created the ideal workplace, where business can be done efficiently and effectively. From an all-in-one cloud phone system with team messaging and video conferencing to a complete contact center and more, RingCentral builds solutions for every business, no matter how big or small. As a unified-communications-as-a-service provider, RingCentral understands the security implications of the cloud model. RingCentral makes security a priority to not only protect their own operations, but also to secure customer data.

System Description

The RingCentral Office Product (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 RingCentral 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).

System Boundaries

This report describes the controls RingCentral employs to ensure the security, availability, and confidentiality of its corporate infrastructure, customer-facing infrastructure, and customer data in RC Office. The system boundaries within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting RC Office.

Subservice Organizations

The scope of this report is limited to the controls executed by RingCentral, and excludes controls that are the responsibility of RingCentral's subservice organizations. RingCentral monitors compliance with the service organizations as it relates to security, availability, and confidentiality. These subservice organizations include:

Amazon Web Services - RingCentral utilizes Amazon Web Services (AWS) to support the Messaging (formerly Glip) cloud computing environment. AWS provides a secure IT infrastructure for compute power, storage, and other application services over the internet.

Equinix - Colocation facilities chosen to locate RC Office production systems and network devices are suitably protected from physical intrusion, theft, fire, flood, excessive ambient temperature, humidity, electromagnetic disturbance, and other hazards. Voice, fax, meetings, and video features that are part of RC Office are hosted, managed, and operate out of Equinix's data centers.

Zoom - RingCentral has partnered with Zoom to deliver its RC 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 applicable controls to gain comfort over its security controls.

Google Cloud Platform - RingCentral utilizes Google Cloud Platform (GCP) to support the live reports feature in RC Office, which allows customers to manage overload queues, quality of service, service level agreements, peak hours, etc.

With respect to AWS, Equinix, Zoom, and GCP these subservice organizations are excluded from the scope of this report. The expected controls for which they are responsible are included in a subsequent section entitled *Complementary Subservice Organization Controls*.

Principle Service Commitments and System Requirements

RingCentral designs its policies, procedures, and processes to ensure security, availability, and confidentiality commitments to customer data. RingCentral commitments are documented and communicated to customers in the Terms of Service, contractual agreements, addendums, or other related agreements. Details around the security, availability, and confidentiality commitments are located on the RingCentral website; https://www.ringcentral.com/legal/eulatos.html.

System Components

RC Office 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 components of RC Office include the following infrastructure, software, people, procedures, and data.

RC Office 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.

Infrastructure

Infrastructure consists of the data centers, networks, servers, databases, and other hardware powering RC Office.

Data Centers

North America customer environments are hosted in two third-party US based data center facilities in San Jose, California and Vienna, Virginia. Europe customer environments are hosted in two third-party data center facilities in Amsterdam, Netherlands and Zurich, Switzerland. Customer environments outside of North America and Europe are hosted in one of the four major data centers (San Jose, California, Vienna, Virginia, Amsterdam, Netherlands or Zurich, Switzerland) depending on proximity.

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 help 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. See Figure 1 & 2 for diagrams of data center interconnectivity and data center network design.

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.

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.

Service Resilience, Backup and Recovery

RingCentral's data centers are commercially available centers with private space for RingCentral equipment. The data centers have full redundancy on production environments. In addition, the RingCentral services in the data centers are fault tolerant to each other, which enables RingCentral to continue providing its services. 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.

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. The RingCentral production infrastructure is primarily powered by CentOS servers. Production databases are primarily managed with Oracle. Production storage devices are NetAPP storage devices.

Messaging Infrastructure

The Messaging feature provided as part of RC Office is hosted by AWS. It operates primarily from AWS' US-EAST-1 region in Northern Virginia. Backups of critical data are maintained in AWS' geographically separate and independent US-WEST-1 region. Within US-EAST-1, the production environment spans three AWS Availability Zones (separate distinct locations) to isolate Messaging from the failure of a single AWS location. Messaging benefits from AWS' low-latency network connectivity between Availability Zones within the same region.

Software

RC Office is supported by the following software and types of software:

1. Threat Management
2. Logging
3. Monitoring
4. Network Protection
5. Intrusion Detection
6. Vulnerability Testing and Vulnerability Management
7. System User Authentication
8. Patch Management
9. Document Portal
10. Change Management

People

The RingCentral Operations department is responsible for system security, confidentiality, and availability. RingCentral's Security team maintains, develops, operates, monitors, and reviews security and fraud-related controls. The team also defines and maintains the company Security Policy and supporting standards.

Key operations teams include:

- Architectural Operations (ArchOps)
- Network Operations (NetOps)
- Database Administrators (DBAs)
- Security
- Media Architecture and Operations (Media ArchOps)
- Telco Operations
- RingCentral Local Exchange Carrier (RCLEC)

The roles and responsibilities of the Information Technology (IT) division includes the Corporate IT Infrastructure and the IT Global Service Desk (GSD) teams. The Engineering 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 resources for the following services:

- *Nordigy* – engineering, operations, product development, quality assurance (QA), website development and maintenance, and support services
- *ABSoft* – software development, QA, and IT support
- *Acquire* – customer support

Procedures

RingCentral maintains the following key policies and procedures to operate RC Office:

- Information Security Policy
- Active Directory-SSL VPN Access Policy
- User Accounts Management on Databases
- SBC Access Policy
- Access Control Policy
- Change Management Policy
- Secure SDLC Policy
- Backup Retention Policy
- Security Incident Response Guide
- Incident Management Policy
- Security Incident Response Plan
- Risk Assessment Policy

Data

Key types of customer content collected by RC Office include:

- Account data (customer name, email address, etc.)
- Usage data
- Call detail records (CDRs)
- Metadata (including time, recipient, sender, and location) associated with faxes, voicemails, and call recordings

Key types of service data collected by RC Office include:

- Text messages
- Faxes
- Attachments
- Voicemails
- Call recordings

RingCentral provides an API tool for customers to export their data to meet their internal data retention compliance requirements. Service data is retained based on the agreements signed with individual customers. Further, if service data is needed for troubleshooting, any exported data is removed immediately after troubleshooting or assistance has been completed. Troubleshooting with service data requires a service ticket.

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.

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 the directors meets quarterly to review company financial and operational results and discuss organizational risks. The board of directors is comprised of senior management and external advisors, who are independent from the company's operations. Annually, the security team communicates significant findings to the executive leadership team.

RingCentral's Security and Governance Council meets quarterly and reports to the board annually. This council, under the direction of the board of directors, oversees the security activities of RingCentral. The committee members are from a cross section of business lines. The council is charged with establishing overall security policies and procedures for RingCentral. 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.

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 TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)* .Changes in security threats and risks are reviewed by RingCentral, and updates to existing control activities and information security policies are performed as necessary.

RingCentral administers and maintains the Red Flags Rule Program which allows RingCentral to develop, implement, and administer an identity theft prevention program. This program includes the basic elements that create a framework to deal with the threat of identity theft.

Control Activities

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

- Asset management
- Logical access security
- Network security

- Encryption
- Endpoint security
- Physical security
- System monitoring
- Backup and availability
- Incident management
- Vulnerability management
- Customer data retention and disposal
- Change management
- Configuration management

Information and Communication

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.

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 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 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 website 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

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, the Security team provides further security monitoring by reviewing metrics weekly at departmental staff meetings.

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

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 on 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 are rather a summary of controls necessary to meet the stated trust services criteria presented in this report.

- User entities are responsible for managing their PBX policies, user permissions, and login information (CC6.3).
- User entities are responsible for designating an administrator extension (phones numbers) (CC6.3).
- User entities are responsible for the settings on their extensions (CC 6.3).
- User entities are responsible for securing communications with their email system (CC2.3, C1.1).

Complementary Subservice Organization Controls

RingCentral uses subservice organizations in conjunction with providing RC Office. RingCentral utilizes AWS for management and hosting of production servers and databases related to the Messaging feature. RingCentral also utilizes Equinix for management and hosting of production servers and databases for RC Office. In addition, RingCentral utilizes Zoom to deliver the RingCentral Office platform, and GCP to support the live reports feature. 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 criteria are included below.

Criteria	Expected Controls for AWS, Zoom, and GCP	Expected Controls for Equinix
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.	Access to hosted systems requires users to use a secure method to authenticate. User content is segregated and made viewable only to authorized individuals. Network security mechanisms restrict external access to the production environment.	Not Applicable
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.	New user accounts are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.	Not Applicable

Criteria	Expected Controls for AWS, Zoom, and GCP	Expected Controls for Equinix
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.	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.	Not Applicable
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.	Access to physical facilities is restricted to authorized users.	Access to physical facilities is restricted to authorized users.
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.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms restrict external access to the production environment. Encrypted communication is required for connections to the production system.	Not Applicable

Criteria	Expected Controls for AWS, Zoom, and GCP	Expected Controls for Equinix
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.	Access to hosted data is restricted to appropriate users. Hosted data is protected during transmission through encryption and secure protocols.	Not Applicable
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.	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.	Not Applicable
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.	System configuration changes are logged and monitored. Vulnerabilities are identified and tracked to resolution.	Not Applicable
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.	Security events are monitored and evaluated to determine potential impact per policy.	Not Applicable
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.	Operations personnel log, monitor, and evaluate incident events identified by monitoring systems	Not Applicable

Criteria	Expected Controls for AWS, Zoom, and GCP	Expected Controls for Equinix
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.	Operations personnel respond to, contain, and remediate incident events, and update stakeholders, as needed.	Not Applicable
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.	System changes are documented, tested, and approved prior to migration to production. Access to make system changes is restricted to appropriate personnel.	Not Applicable
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.	Operations personnel monitor processing and system capacity.	Not Applicable
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.	Environmental controls protect the physical devices supporting the production environment.	Environmental controls protect the physical devices supporting the production environment.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	System failover and backup procedures are tested.	Not Applicable