RingCentral®

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, 2018 TO DECEMBER 31, 2018

ISSUED ON MAY 15, 2019

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 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 service 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 service 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 service commitments and system requirements

during the period January 1, 2018 to December 31, 2018 based on the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). This assertion is the responsibility of RingCentral's management. Our responsibility is to express opinion based on our examination.

During the period under review, RingCentral used multiple subservice organizations; 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 service 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 service commitments and system requirements were achieved. RingCentral has also

THE cadence GROUP

O 801.349.1360
F 866.326.6612

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

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 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 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, 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 criteria, and (3) performing procedures to obtain evidence about whether controls within the system were effective to achieve RingCentral's service commitments and system requirements based the applicable trust services 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 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'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 14, 2019
Salt Lake City, Utah

Section II – RingCentral's Assertion

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, 2018 to December 31, 2018, 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*). Based on this evaluation and the applicable trust services criteria, we assert that the controls were effective throughout the period January 1, 2018 to December 31, 2018 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 service 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 service 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 service 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. 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. 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, 2018 to December 31, 2018, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria.

RingCentral, Inc.
May 14, 2019

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

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.

System Description

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 employees 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. The 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 the number of concurrent video and web conference meeting attendees. RingCentral Office customers also have RingCentral Global Office available.

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 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 the On Demand Unified Communications System and Glip Collaboration System. The system boundaries within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting RingCentral's On Demand Unified Communications System and Glip Collaboration System.

RingCentral offers the On Demand Unified Communications System and Glip Collaboration System in both hosted and customer on-premise versions. The following are excluded from the scope of this report:

- Real-time live reports feature
- On-premise versions, or customer installations of the RingCentral On Demand Unified Communications System and Glip Collaboration System

Subservice Organizations

RingCentral monitors compliance with the service organizations as it relates to security, availability, and confidentiality.

Amazon Web Services

RingCentral utilizes Amazon Web Services (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' SOC 2 reports to gain comfort over its security controls.

Equinix

Colocation facilities chosen to locate the On Demand Unified Communications 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 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 applicable controls to gain comfort over its security 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

The components of the RingCentral On Demand Unified Communications System and Glip Collaboration System include the following infrastructure, software, people, procedures, and data.

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

Infrastructure consists of the data centers, networks, servers, databases, and other hardware powering the On Demand Unified Communications System and Glip Collaboration System.

Unified On Demand Communications System

Data Centers: North America customer environments are hosted in two third-party U.S. based data center facilities in San Jose, California and Vienna, Virginia, and United Kingdom customer environments are hosted in two third-party data center facilities in Amsterdam, Netherlands and Zurich, Switzerland.

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 Service Organization Controls audits or ISO controls audits 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 Architectural Operations function (ArchOps) 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 (in California) and carry a minimum of three days on-site fuel. In addition, the RingCentral services in the data centers are fault tolerant to each other, which enables RingCentral 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 maintains a staffed NOC to continuously monitor the status of its operating networks for both systems and voice components.

Glip Collaboration System

The Glip system is hosted by AWS. Glip 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 Glip from the failure of a single AWS location. Glip benefits from AWS' low-latency network connectivity between Availability Zones within the same region.

Glip resides within a virtual private cloud hosted by AWS (Glip VPC) that spans multiple AWS Availability Zones as described above. The Glip VPC is logically isolated from other virtual networks in the AWS cloud. This 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 fault tolerance in the system, seamlessly providing the required amount of load balancing capacity needed to route application traffic.

Fault tolerance is accomplished within the Glip application. Should a server or connection no longer be functioning as intended, the system load will automatically be redirected without impacting Glip users. Together with automatic scaling this configuration is designed to ensure the system remains highly available.

System servers responsible for communicating data and events to and from Glip users have been optimized for input/output speeds.

To further ensure the availability of the applications running behind the ELB, AWS Route 53 health checking (monitoring) and DNS failover features are used. Route 53 is configured to fail away from a load balancer if there are no healthy instances registered with the load balancer or if the load balancer itself is unhealthy.

Software

Unified On Demand Communications System

The RingCentral production infrastructure is primarily powered by a Microsoft technology stack (Microsoft Server, Microsoft Windows) with CentOS as required to meet specific business requirements, with endpoint security from Symantec. Production databases are managed with Oracle.

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 customers with the option of enabling the account access confirmation feature. When enabled, this feature activates 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.

Glip Collaboration System

The system is currently running a hardened version of AWS' Linux. RingCentral has designed the system so that the majority of its business logic resides within API instances that communicate directly with its databases. To reduce the load from HTTPS calls, authorized RingCentral personnel connect to the system through a secure internal connection.

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 companies that are RingCentral customers, a Glip account is automatically provisioned for every user with a RingCentral 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 co-worker is on Glip, only one of the company'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 companies, users who are administrators in the company's RingCentral Office account are automatically designated the Glip administrators.

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.

The roles and responsibilities of the Operations team are as follows:

- *Architectural Operations (ArchOps)* – Architectural Operations is responsible for the design, build, deployment, and maintenance of the physical and operating system level components supporting the RingCentral and Glip system infrastructure.
- *Network Operations (NetOps)* – Network Operations is responsible for the design, build, configuration, and maintenance of the network components supporting the RingCentral and Glip network infrastructure.
- *Database Administrators (DBAs)* – Database Administrators are responsible for the design, build, and configuration of the production databases.
- *Network Operations Center (NOC)* – The NOC maintains monitoring and troubleshooting services for the RingCentral and Glip networks. The NOC maintains a 24x7x365 schedule to ensure compliance with service level agreements.
- *Security* – Security is responsible for designing, implementing, and maintaining information security measures for the RingCentral and Glip production environments and RingCentral office networks. In addition, the Security team is also responsible for fraud monitoring and prevention, and security audit and compliance.
- *Media Architecture and Operations* – Media Architecture Operations is responsible for design, deployment, and maintenance of the Voice over Internet Protocol section of the RingCentral production service.
- *Integrations* – Integrations provides management and technical support for integrating larger enterprise customers and business partners.
- *RingCentral Local Exchange Carrier (RCLEC)* – RCLEC is responsible for providing local exchange carrier services to RingCentral. RCLEC provides connectivity and exchange services between RingCentral and traditional carrier services. RCLEC also provides RingCentral with its customer available phone numbers.

The Engineering & Innovation division also include two key teams, System Operations (SysOps) and Development Operations (DevOps). Roles and responsibilities of these teams are as follows:

- *SysOps* – SysOps is responsible for the 24x7x365 maintenance of software systems and related APIs. SysOps maintains the customer-facing web components of the RingCentral and Glip services. In addition, SysOps also responds to issue escalation and resolution from the NOC teams, systems analysis, and development review of new systems.
- *DevOps* – DevOps is responsible for deployment of software systems, i.e., application layer, products in laboratory and stage environments, in addition to the RingCentral and Glip production environment. DevOps is also responsible for code deployments.

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 Monitoring: The Security team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include firewall notifications, IDS or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. The Security team review these alerts and notifications daily by the 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 Control Board review. RingCentral's software development activities include internal and external application security testing.

System Account Management: RingCentral has implemented role-based security to limit and control access within the production network environment. RingCentral production access is tightly controlled using the least privilege principle. Through the use of privileged access management systems, access to production is logged and granted using two factors of authentication. Users requesting access submit a request, which is reviewed by the Sr. Director of Operations or delegate. If the access is approved, the Security team grants the new user access to VPN and Active Directory for the production environment. Employees' managers follow a documented process to request modified production access for their team members. Management reviews the requests, and if approved, assigns the request to the Operations team to grant or modify user access. The ability to create or

modify user access accounts and user access privileges is limited to authorized system administrators. The SysOps team updates the ticket to include a notification for the Security team. In addition, any non-standard access request is forwarded to the Security team for review. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

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. RingCentral provides an API tool for customers to export their data to meet their internal data retention compliance requirements.

Internal Control Framework

RingCentral's control environment reflects the philosophy of senior management concerning the importance of protecting data and information. RingCentral's Security and Governance Council meets quarterly and reports to the board annually. This council, under the direction of the RingCentral 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.

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 Information Security Policy.

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

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 and key members of the board of directors.

The SVP of Operations retains qualified professional staff responsible for the design, development, implementation, operation, maintenance, and monitoring of the systems that affect security, availability, and confidentiality of the RingCentral Service.

RingCentral maintains and provides for professional training related to the job functions of its personnel. This includes relevant vendor training, internal training, and funding in departmental budgets.

RingCentral maintains a published Employee Handbook, which contains workforce conduct standards. Employees are required to execute confidentiality agreements and accept RingCentral's employee Code of Conduct. Where laws and regulations permit, and upon obtaining signed consent from job candidates, the HR department conducts candidate background checks.

Security Policies

The RingCentral Security team maintains the company's Information Security Policy outlining the security-related roles and responsibilities of company employees.

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 established to ensure key processes operate as intended. These activities are designed to address both the relevant business risks and the underlying infrastructure relevant to the On Demand Communications System and Glip Collaboration System.

RingCentral utilizes Nordigy provide engineering, mobile applications development, network, operations, product, QA, website development and maintenance, support services and other services. Nordigy acts as a subcontractor and executes controls on behalf of RingCentral under the oversight of RingCentral's 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 Fraud Management team. Carrier partners report incidents directly to the Fraud team via emails. The Security team utilizes tools and documented procedures for detecting and resolving toll fraud and 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 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.

RingCentral utilizes Acquire to provide inbound support, outbound sales, marketing call center services and customer support services. Acquire acts as a subcontractor and executes controls on behalf of RingCentral under the oversight of RingCentral's management.

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's Security team 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 monitors the network and customer input for security and service impacting issues at all times. RingCentral's NOC also utilizes 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 generates an email.

Internal Control Reviews

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 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 criteria presented in this report.

- User entities are responsible for managing their PBX 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 defining data retention periods within the Glip environment.
- User entities are responsible for storing meeting recordings and applicable data retention.

Complementary Subservice Organization Controls

RingCentral uses subservice organizations in conjunction with providing its On Demand Unified Communications System and Glip Collaboration System. RingCentral utilizes AWS 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. Expected subservice provider controls that have an effect on specific criteria are included below.

Criteria	Expected Controls
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to the in-scope systems requires users to authenticate using a valid, unique user ID and password before being granted access. User content is segregated and made viewable only to authorized individuals. Encrypted communication is required for connections to the production system. *Not Applicable for Equinix*
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 for Equinix*

Criteria	Expected Controls
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 requests 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 for Equinix*
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.	Only authorized users have access to the physical facilities housing the system.
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.	Customer data is deleted or anonymized upon request. 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.
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 customer information is restricted to appropriate users. Customer data is protected during transmission through encryption and secure protocols. *Not Applicable for Equinix*

Criteria	Expected Controls
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 for Equinix*
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.	Vulnerabilities are logged and tracked to resolution. Operations personnel monitor and respond to incident events identified by monitoring systems. *Not Applicable for Equinix*
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.	Security events are assessed for impact and addressed failures. *Not Applicable 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.	Incidents are logged and tracked to resolution. *Not Applicable for Equinix*
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. *Not Applicable for Equinix*
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.	Monitoring processes alert appropriate personnel when capacity thresholds are exceeded. *Not Applicable for Equinix*

Criteria	Expected Controls
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 protections are implemented in the production environment. Backup and recovery processes are in place to perform and monitor backup activities.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Backups are tested. *Not Applicable for Equinix*
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Customer data is retained in a security environment in accordance with data retention policies. *Not Applicable for Equinix*
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Customer data is deleted or anonymized upon request. *Not Applicable for Equinix*