Proprietary & Confidential

RingCentral

System Description of the Engage Product

SOC 3

Relevant to Security, Availability, and Confidentiality

JANUARY 1, 2022 TO DECEMBER 31, 2022

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

RingCentral, Inc.
20 Davis Dr.
Belmont, CA 94002

To the Management of RingCentral:

Scope

We have examined RingCentral's accompanying assertion in Section II titled "RingCentral's Assertion" (assertion) that the controls within RingCentral's Engage Product (system) were effective throughout the period January 1, 2022 to December 31, 2022, 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 uses Claranet and Amazon Web Services (AWS) for cloud computing (subservice organizations). The description indicates that complementary subservice organization 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. The description presents the types of complementary subservice organization controls assumed in the design of RingCentral's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that 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. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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 also 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 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 (AICPA). 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 the applicable trust services criteria

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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, management's assertion that the controls within RingCentral's Engage Product were effective throughout the period January 1, 2022 to December 31, 2022, 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.

Moss Adams LLP

San Francisco, California
March 9, 2023

II. RingCentral's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within RingCentral's Engage Product (system) throughout the period January 1, 2022 to December 31, 2022 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 Section III titled "RingCentral's Description of the Boundaries of Its Engage Product" 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, 2022 to December 31, 2022, 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 Section III titled "RingCentral's Description of the Boundaries of Its Engage Product."

RingCentral uses Claranet and Amazon Web Services (AWS) for cloud computing (subservice organizations). The description indicates that complementary subservice organization 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. The description presents the types of complementary subservice organization controls assumed in the design of RingCentral's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that 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. The description presents RingCentral's complementary user entity controls assumed in the design of RingCentral's controls.

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, 2022 to December 31, 2022, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. RingCentral's Description of the Boundaries of Its Engage Product

A. System Overview

1. Services Provided

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 mode, 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's Engage Product (Engage) consists of Engage Digital (ED) and Engage Voice (EV).

ENGAGE DIGITAL

The ED product enables companies to manage their digital customer care channels such as questions, reactions, and complaints within a single platform. ED can facilitate a reduction of response time, a better allocation of resources, and better management of peaks. Companies using ED can be available where their customers expect them to be while reducing their expenses.

The sources managed within ED include different digital social media channels. Each of these sources appears to the agent in a uniform fashion for ease to interact with customers. Once configured, agents can address customer issues on behalf of the overall company identity, rather than individually, if they were signed into their own social media account. Example sources include, but not limited to:

- Facebook
- Google Play
- Instagram
- Lithium
- Messenger (Facebook)
- Twitter
- WhatsApp
- YouTube
- SMS
- Chat

ENGAGE VOICE

EV offers a cloud based CCaaS (Contact Center as a Service) model that users can customize to fit their unique needs. EV comes packaged within an agent and supervisor interface (Agent), an admin interface (Admin), and an analytics interface (Analytics) used for tracking, monitoring, and analyzing contact center activities.

Key services of EV include:

- *Agent* – An agent interface with inbound, outbound, blended voice, and live chat capabilities. A built-in softphone with Voice over Internet Protocol (VoIP), internal chat services, scripting, callback tools, agent stats, and supervisor monitoring and coaching tools.
- *Admin* – An administrator interface with configuration tools for inbound call routing, agent scripting, outbound dialing, IVR services, and live inbound and outbound customer chats.
- *Analytics* – An analytics interface with reporting tools that offer insight into contact center activities via historical reporting, scheduled reports, and customizable real-time reporting dashboards.

SYSTEM BOUNDARIES

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

SUBSERVICE ORGANIZATIONS

Engage uses the following subservice organizations:

- *Claranet* – For managed hosting of non-U.S. customers on ED.
- *Amazon Web Services (AWS)* – For managed hosting of U.S. customers on ED and EV and non-U.S. customers on EV. For managed hosting of non-U.S. customers on ED onboarded as of December 2021.

These subservice organizations are excluded from the scope of this report. The controls for which they are responsible are included in a subsequent section entitled Complementary Subservice Organization Controls.

2. Infrastructure

System descriptions delineate the boundaries of the system, describe relevant system components, and outline the purpose and design of the system. The ED production infrastructure is powered by Claranet and AWS. Production databases are based on MongoDB and PostgreSQL. The EV production infrastructure is powered by Docker containers. Production databases are based on PostgreSQL and MySQL. Production storage devices are AWS S3 buckets and Elastic File System (EFS).

For non-U.S. customers, the primary components of ED are built on top of Claranet using the following services:

Claranet Services	Function
Claranet Monitoring	Claranet Monitoring provides metrics and alerts based on the health of servers, services, and specific business metrics.
Claranet NetApp Service	Claranet NetApp Service is virtual storage used in conjunction with server hosting to store file attachments and share across servers.
Claranet Load Balancing Service	Claranet Load Balancing distributes incoming application traffic across multiple servers increasing the availability of the application.

For U.S. customers, and non-U.S. customers onboarded as of December 2021, the primary components of ED and EV are built on top of AWS, using the services in the Amazon Web Services table below. Note that the services indicated as EV or ED only are applicable only to that product.

Amazon Web Services	Function
Amazon Simple Storage Service (S3)	Amazon S3 is virtual storage used in conjunction with Amazon EC2 and Amazon EBS to store object data. Amazon S3 is also used to automatically replicate data across AWS regions.
ElastiCache	Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. ElastiCache improves the performance of web applications by allowing retrieval of information form a fast, managed, in-memory system instead of relying entirely on slower disk-based databases. (ED only)
Amazon Elastic Block Store (EBS)	Amazon EBS is a high-performance block storage service designed to use with Amazon EC2 for both throughput and transaction intensive workloads at any scale. (ED only)
Amazon Elastic Compute Cloud (EC2)	Amazon EC2 provides a virtual computing environment that uses web service interfaces to perform the following functions: • Launch instances of operating systems. • Create Amazon Machine Images (AMI) containing applications, libraries, data, and associated configuration settings. • Configure security and network access on the AWS EC2 instances.
Amazon Elastic Kubernetes Service (Amazon EKS)	Amazon EKS is a fully managed Kubernetes service.

Amazon Web Services	Function
Amazon Elastic File System (EFS)	Amazon EFS is a cloud storage service designed to provide scalable, elastic, and encrypted file storage.
Amazon Application Load Balancers (ALBs)	Amazon ALBs distribute incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones, increasing the availability of the application.
Amazon Network Load Balancers (NLBs)	Amazon NLBs distribute end-user traffic across multiple cloud resources to help ensure low latency and high throughput for applications.
Amazon Elastic Container Registry (ECR)	Amazon Elastic Container Registry (ECR) is a fully managed Docker container registry that makes it easy to store, share, and deploy container images.
Amazon Virtual Private Cloud (VPC)	Amazon VPC is used to provision logically isolated virtual networks in the AWS Cloud. AWS VPC is used to manage the virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways.
Amazon Lambda	Amazon Lambda lets code run without provisioning or managing servers. (EV only)
Amazon Route 53	Amazon Route 53 is a scalable cloud Domain Name System (DNS) web service.
Amazon CloudWatch	Amazon CloudWatch provides monitoring for AWS cloud resources and applications. AWS CloudWatch provides visibility into resource utilization, operational performance, and overall demand patterns —including metrics such as CPU utilization, disk reads and writes, and network traffic. AWS CloudWatch provides the ability to review statistics, view graphs, and set alarms for specified metric data.
Amazon GuardDuty	Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon S3.
Amazon Relational Database Service (RDS)	Amazon RDS is designed to simplify the setup, operation, and scaling of relational databases.
Amazon DynamoDB	Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It is a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. (EV only)

DATA CENTERS

Non-U.S. customers on ED are hosted on Claranet data centers. U.S. customers on ED and EV are hosted on us-east and us-west locations. Non-U.S. customers for ED are hosted on eu-west locations. RingCentral has no access to cloud IaaS data centers; all operations and support is provided in a remote manner.

See Figure 1 and Figure 2 for diagrams of the Engage Digital and Engage Voice architecture.

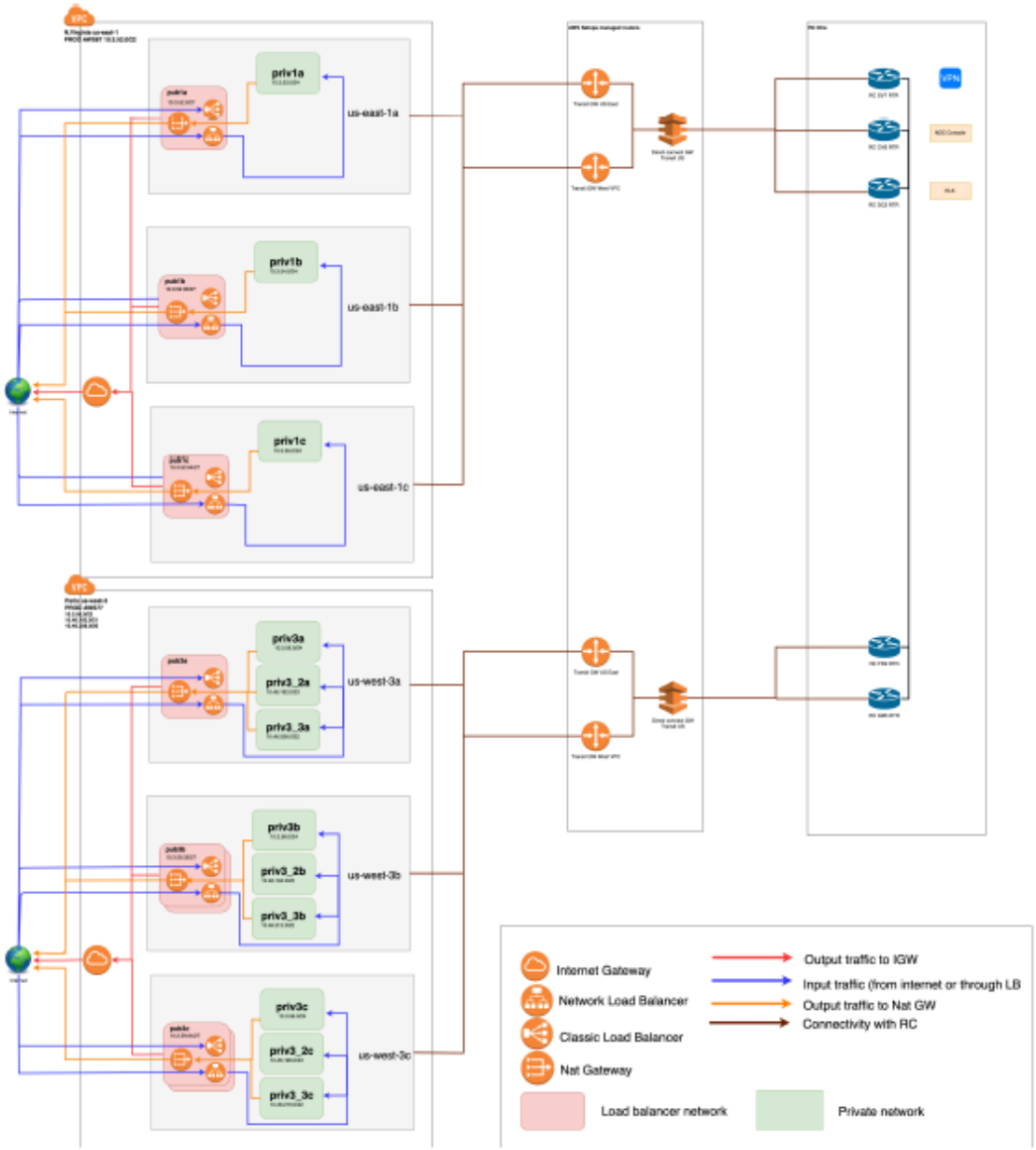

FIGURE 1: OVERVIEW OF ENGAGE DIGITAL

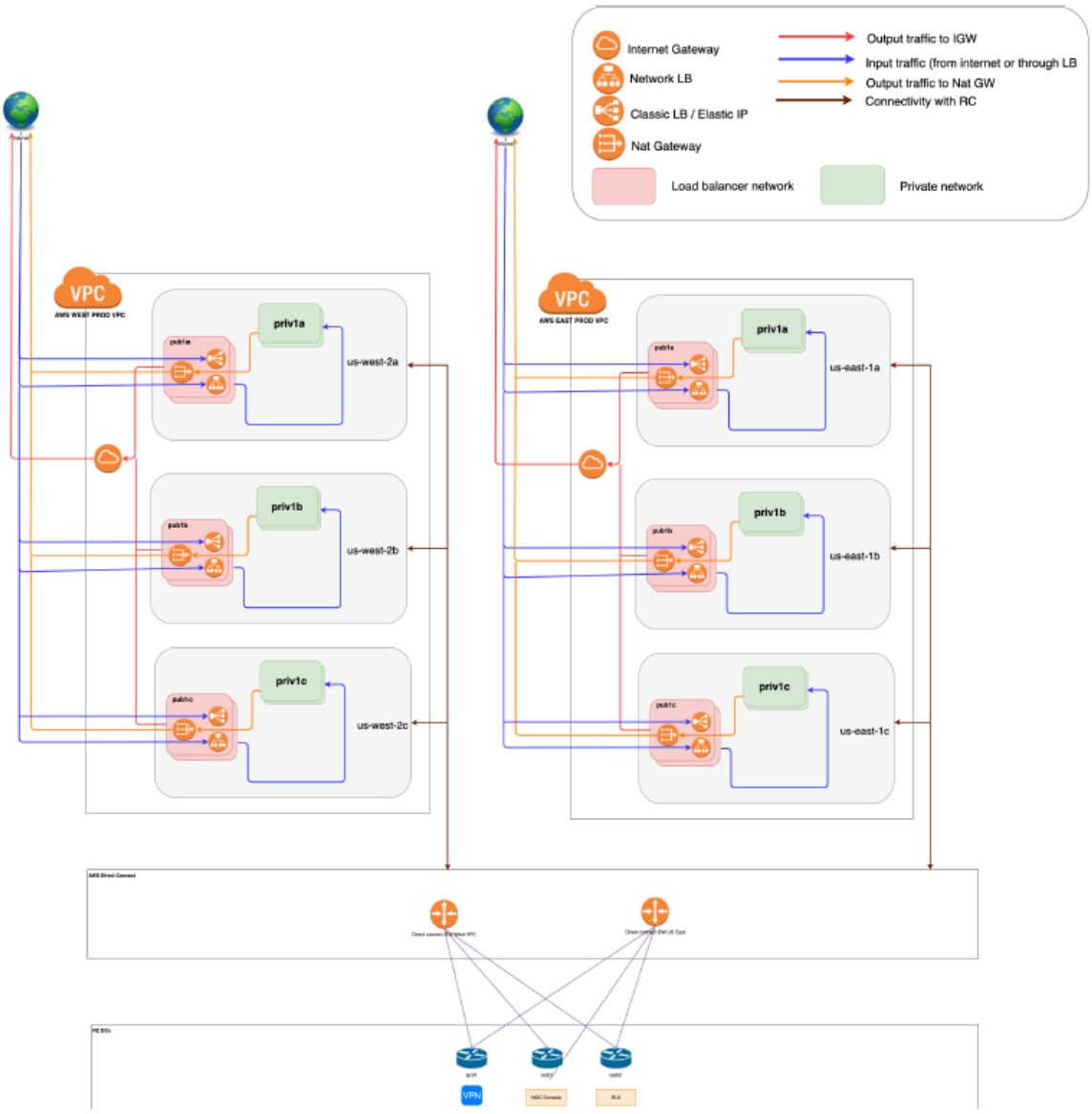

FIGURE 2: OVERVIEW OF ENGAGE VOICE

3. Software

Engage is supported by the following software and types of software:

- Threat Management
  - Endpoint protection antivirus
  - Continuous monitoring
  - Incident Response
  - Intrusion detection/prevention

- Logging
  - Component-based logging of system events
  - Centralized log management
- Monitoring
  - Health and Quality of Service (QoS) metrics
  - Security-related events
  - Alerting
- Application Security
  - Input validation
  - Application security testing
  - Penetration testing
- Network Protection
  - Networking devices (routers, SBCs, load balancers, WAF/firewalls) with access control lists (ACLs)
  - Network Intrusion detection/prevention
  - Traffic (security/QoS) monitoring
  - Firewalls with ACLs
  - Distributed Denial of Service (DDoS) protection
  - Domain Name System (DNS) and DNS monitoring
- Vulnerability Testing and Vulnerability Management
  - Vulnerability scans of major system components
- System User Authentication and Access Management
  - Centralized access management
  - Two-factor authentication technology
  - VPN (virtual private network)
- Change and Configuration Management
  - Online internal CMP portal
  - Ticketing system
  - Testing tools
  - Environmental isolation (development, testing, production)

4. People

The executive management team of RingCentral consists of 10 individuals. Their biographies are available at https://www.ringcentral.com/whyringcentral/leadership.html.

CHIEF INFORMATION SECURITY OFFICER (CISO) TEAM

The primary responsibility of the CISO team is to design, implement, and maintain information security measures for RingCentral. In addition to maintaining RingCentral's Information Security Policy, the CISO team includes several core functions, as depicted in Figure 3, including:

- Security Operations, responsible for:
  - Overall secure hardening, configuration, vulnerability and patch management
  - Management and oversight of critical vulnerability remediation
- Security Operations Center (SOC), responsible for:
  - Monitoring and response to alerts from third-party security tools
  - Creation, monitoring and management of aggregate alarms and response
- Application Security, responsible for:
  - Application security reviews and oversight
  - Automated security testing
  - Internal and independent, third-party penetration testing
- Trust and Enablement, responsible for:
  - Implement, maintain, and operate overall third-party risk management discipline for RingCentral's (outbound) vendors including sub-processors
  - Support responses to customer-driven third part risk assessment responses
- Compliance, responsible for:
  - Scheduling, managing RingCentral's third-party audit and certification discipline
  - Manage ongoing risk assessment including enterprise level and business continuity risk assessments
  - Working with teams to ensure ongoing compliance with RingCentral's security policies and standards

The following diagram (Figure 3) depicts the functional reporting within RingCentral's CISO team.

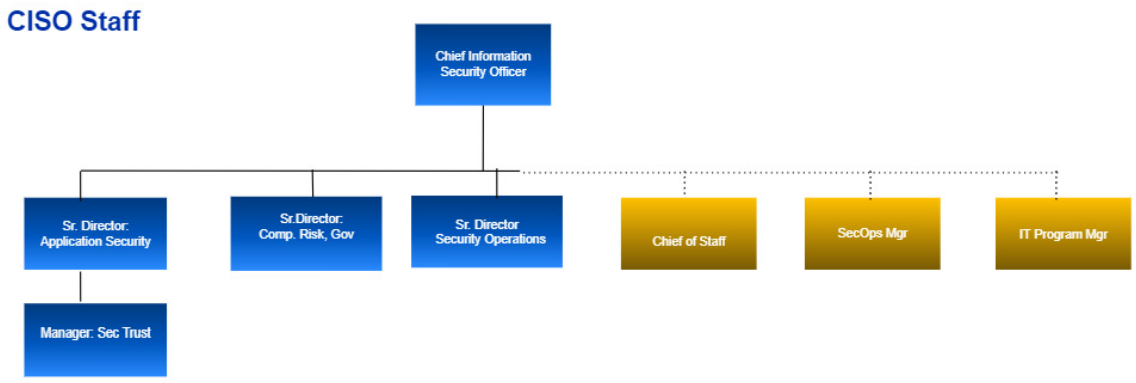

FIGURE 3: RINGCENTRAL SECURITY PERSONNEL

OPERATIONS

Responsible for the design, build, deployment, and maintenance of physical and virtual operating system infrastructure components, production databases, network components, and VoIP services; providing connectivity and exchange services between RingCentral and traditional carrier services, and monitoring and maintaining gateway connectivity between RingCentral and common carrier PSTNs; providing authentication services; and providing interconnection services. The Operations team consists of various teams including Architectural Operations (ArchOps), Database Administrators (DBAs), Data Center Operations (DCOPs), Cloud Operations (CloudOps), Media Architectural Operations (Media ArchOps), Telco Operations, Network Operations (NetOps), Innovation, Innovation Development, and additional assistance from the System Operations (SysOps) team. Operations also includes the Service Abuse and Fraud Management (SAFM) team, who is responsible for monitoring, and responding to alerts for service abuse or fraud.

INFORMATION TECHNOLOGY (IT)

Responsible for provisioning and managing corporate users' identity, corporate office networks, users' endpoints, internal corporate applications, and other corporate assets; responsible for managing the user account lifecycle for RingCentral users' corporate network credentials. The IT team consists of Corporate IT, which includes Merger and Acquisition (M&A) Integration and IT End User Services (EUS).

SITE RELIABILITY ENGINEERING (SRE)

The SRE team is responsible for processes related to security, availability, and confidentiality of data, information, and services. Made up of three core functions (DevOps, NOC, and SysOps), the SRE team responsibilities include software system deployments including design build and configuration of production databases, network monitoring and troubleshooting, SLA compliance, incident response, system analysis and maintenance.

- *DevOps* – DevOps is responsible for deployment of software systems, i.e., application layer, products in laboratory and stage environments, in addition to the production environment. DevOps is also responsible for code deployments and for the design, build, and configuration of the production databases.
- *Network Operations Center (NOC)* – The NOC team maintains monitoring and troubleshooting services for the RingCentral networks. The NOC maintains a 24x7x365 schedule to help ensure compliance with service level agreements. The NOC is responsible for resolving or escalating any production incidents identified through its continuous monitoring of services and hosts. The NOC is further responsible for communicating incidents with external partners, customers and internal teams as required.
- *SysOps* – SysOps is responsible for the 24x7x365 maintenance of software systems and related APIs. SysOps maintains the customer-facing web components of RingCentral Engage. In addition, SysOps also responds to issue escalation and resolution from the NOC teams, systems analysis, and development review of new systems.

CUSTOMER SUPPORT

The Global Support Services (GSS) team assists customers troubleshoot account and service-usage issues. Tier 1, 2 and 3 support teams are part of the broader GSS team. Within this team are Customer Success Managers (CSM) and Customer Ad.

HUMAN RESOURCES/PEOPLE OPERATIONS

The Human Resources (HR) team, internally rebranded to "People and Place" midway through 2021, is responsible for recruiting, onboarding, training, evaluations, compensation, and development of RingCentral employees.

RingCentral maintains relationships with sub-contractors who may act as sub-processors in the performance of duties. Sub-processors execute controls on behalf of RingCentral under the oversight of RingCentral's management. RingCentral communicates security, confidentiality, and availability requirements to its sub-contractors through its contracts. These subcontractors provide aspects of engineering, operations, development, quality assurance, and customer support.

5. Data

Key types of content data collected by ED includes, but not limited to:

- Content and data of interactions
- Attachments related to interactions
- End-user information
- Authentication credentials

Key types of service data collected by ED includes, but not limited to:

- Account data (customer name, email address, etc.)
- Usage data
- Metadata (including time, recipient, sender) associated with interactions

Key types of content data collected by EV includes, but not limited to:

- SMS and chat messages
- Call recordings
- End-user information (address book, contact information)
- Authentication credentials

Key types of service data collected by EV includes, but not limited to:

- 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

6. Processes and Procedures

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

- Active Directory-SSL VPN Access Policy
- User Accounts Management on Databases
- Backup Retention Policy
- Security Policy
- Network Access Policy
- Access Control Procedure
- Change Management Policy
- Cybersecurity Risk Assessment Policy
- Data Classification Standard
- Data Retention Policy and Procedure
- Datacenter Switchover/Isolation and Restoration and Datacenter Outages Prevention Playbooks
- External Vulnerability Scan and Remediation Policy
- Hardening Procedures
- Incident Management Process
- Information Security Policy
- Network Access Policy
- Phone Support Call Handling and Escalation Process
- Risk Assessment Policy
- Secure Development Lifecycle (SDLC) Policy
- Security Incident Response Plan
- Vulnerability Management and Patch Management Standard

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 HIPAA Security Rule requirements, FINRA cybersecurity regulations, and National Institute of Standards and Framework's Cybersecurity Framework (NIST CSF) standards.

RingCentral commitments to security, availability, and confidentiality are documented and communicated to customers in RingCentral's published Information Security Addendum available through the RingCentral generally available Trust Center via RingCentral's website and upon request. Agreements with third parties and vendors include clearly defined terms, conditions, and responsibilities. Formal information-sharing agreements, such as confidentiality agreements or data processing agreements are in place with third parties and vendors who have access to customer-generated content and provide customer-facing features. 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 in accordance with HIPAA. Security, availability, and confidentiality commitments, between RingCentral and third parties performing services for RingCentral for its customers, are further communicated to customers in Terms of Service located on the RingCentral website, or contractual agreements signed by customers and RingCentral, such as RingCentral Master Services Agreements (MSA), including similar terms than the online Terms of Service. Each RingCentral online Terms of Services and MSA includes RingCentral Data Processing Addendum and Security Addendum, describing RingCentral's commitment to its customers regarding security, availability, and confidentiality of their data.

C. Complementary Subservice Organization Controls

RingCentral's controls related to the Engage Product cover only a portion of overall internal control for each user entity of RingCentral. It is not feasible for the criteria related to the Engage Product to be achieved solely by RingCentral. Therefore, each user entity's internal controls must be evaluated in conjunction with RingCentral's controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
1	Access to hosted systems requires users to use a secure method to authenticate.
2	User content is segregated and made viewable only to authorized individuals.
3	Network security mechanisms restrict external access to the production environment.
4	New user accounts are approved by appropriate individuals prior to being provisioned.
5	User accounts are removed when access is no longer needed.
6	User accounts are reviewed on a regular basis by appropriate personnel.
7	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.
8	Access to physical facilities is restricted to authorized users.
9	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
10	Encrypted communication is required for connections to the production system.
11	Access to hosted data is restricted to appropriate users.

Complementary Subservice Organization Controls	
12	Hosted data is protected during transmission through encryption and secure protocols.
13	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
14	System configuration changes are logged and monitored.
15	Vulnerabilities are identified and tracked to resolution.
16	Security events are monitored and evaluated to determine potential impact per policy.
17	Operations personnel log, monitor, and evaluate incident events identified by monitoring systems
18	Operations personnel respond to, contain, and remediate incident events, and update stakeholders, as needed.
19	System changes are documented, tested, and approved prior to migration to production.
20	Access to make system changes is restricted to appropriate personnel.
21	Operations personnel monitor processing and system capacity.
22	Environmental controls protect the physical devices supporting the production environment.
23	System failover and backup procedures are tested.

D. Complementary User Entity Controls

RingCentral's Engage Product was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Engage Product. In these situations, the application of specific controls at these user entities is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the user entities to complement the controls at RingCentral. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	Managing their user permissions and login information.
2	Designating user accounts with administrator privileges.

MOSSADAMS