Proprietary & Confidential

RingCentral

System Description of the Message Video Phone System

SOC 3

Relevant to Security, Availability, and Confidentiality

JANUARY 1, 2021 TO DECEMBER 31, 2021

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 Message Video Phone System (system) were effective throughout the period January 1, 2021 to December 31, 2021, 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 subservice organizations for cloud computing, infrastructure, storage, colocation services, and cloud contact center software. 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 organizations, 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.

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 Message Video Phone System were effective throughout the period January 1, 2021 to December 31, 2021, 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
April 22, 2022

II. RingCentral's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within RingCentral's Message Video Phone System (system) throughout the period January 1, 2021 to December 31, 2021 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 entitled "RingCentral's Description of the Boundaries of Its Message Video Phone System" 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, 2021 to December 31, 2021, 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 entitled "RingCentral's Description of the Boundaries of Its Message Video Phone System".

RingCentral uses subservice organizations for cloud computing, infrastructure, storage, colocation services, and cloud contact center software. 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, 2021 to December 31, 2021, 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 Message Video Phone System

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 MESSAGE VIDEO PHONE

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

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

RINGCENTRAL VIDEO

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

- HD audio and video
- Powerful browser-based video meetings — no downloads needed
- Mobile and desktop meeting client with presence and instant messaging
- Interactive multimedia content and screen sharing cloud meetings recording
- In-meeting public and private chat
- Up to 200 interactive video participants
- Voice over Internet Protocol (VoIP) with call-in and call-out audio options
- Quality-of-service analytics and usage insights
- Background noise reduction
- Personal meeting ID
- Open APIs
- Integration with Office 365 and Google Calendar
- Integration with Microsoft Teams, Salesforce, Slack, and other business apps
- Integration with RingCentral MVP

2. System Boundaries

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

3. Subservice Organizations

RingCentral MVP uses the following subservice organizations:

AMAZON WEB SERVICES

Amazon Web Services (AWS) supports the RingCentral MVP messaging cloud computing environment and provides a secure IT infrastructure for compute power, storage, and other application services over the internet, as well as storage of RingCentral Video recordings.

EQUINIX

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

GOOGLE CLOUD PLATFORM

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

NICE

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

ZOOM

RingCentral is partnered with Zoom to deliver RingCentral Meetings, providing core technology used by RingCentral with meetings hosted on both RingCentral and Zoom's infrastructure. With the release of RingCentral Video, the proprietary video conferencing solution, RingCentral Meetings is no longer offered to new customers.

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.

4. Infrastructure

System descriptions delineate the boundaries of the system, describe relevant system components, and outline the purpose and design of the system. RingCentral MVP operating system and storage infrastructure is powered by modern component types.

DATA CENTERS

North America customer environments are hosted in five third-party US-based data center facilities in Santa Clara, California, San Jose, California, Ashburn, Virginia, Vienna, Virginia and Chicago, Illinois. Europe customer environments are hosted in three third-party data center facilities in Amsterdam, Netherlands, Frankfurt, Germany, and Zurich, Switzerland. APAC customer environments are hosted in three third-party data center facilities in Singapore, Singapore and Tokyo, Japan. Outside of North America and Europe, customer environments are hosted in one of seven major data centers listed above depending on proximity. RingCentral customer environments and services may also be provided from third-party cloud Infrastructure-as-a-Service (IaaS) data centers in the US and Europe, including us-east, us-central, us-west locations, Amsterdam, Netherlands, Frankfurt, Germany. RingCentral has no access to cloud IaaS data centers; all operations and support is provided in a remote manner.

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

NETWORK AND DATABASE ARCHITECTURE AND MANAGEMENT

RingCentral's network and application perimeter are secured via firewalls with intrusion detection and web-application firewall features and session border controllers (SBCs). In addition, RingCentral has network load balancing that distributes web application traffic across web server farms. RingCentral uses firewalls to help prevent unauthorized network access and to help protect the network based on the Network Access Policy.

RingCentral MVP databases are based on MongoDB and OracleDB. Databases are run in an active-active or high-availability configuration.

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

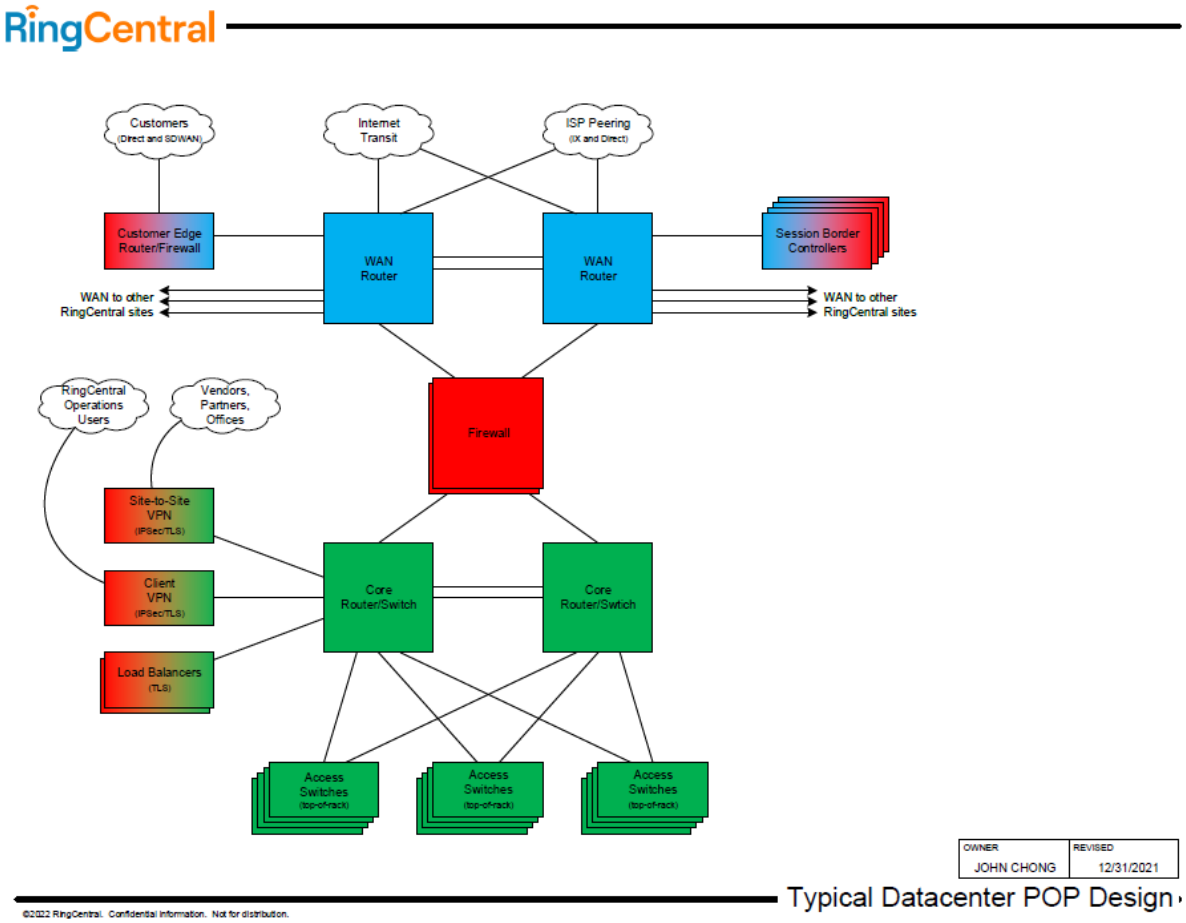

FIGURE 1: OVERVIEW OF RINGCENTRAL'S DATA CENTER NETWORK DESIGN

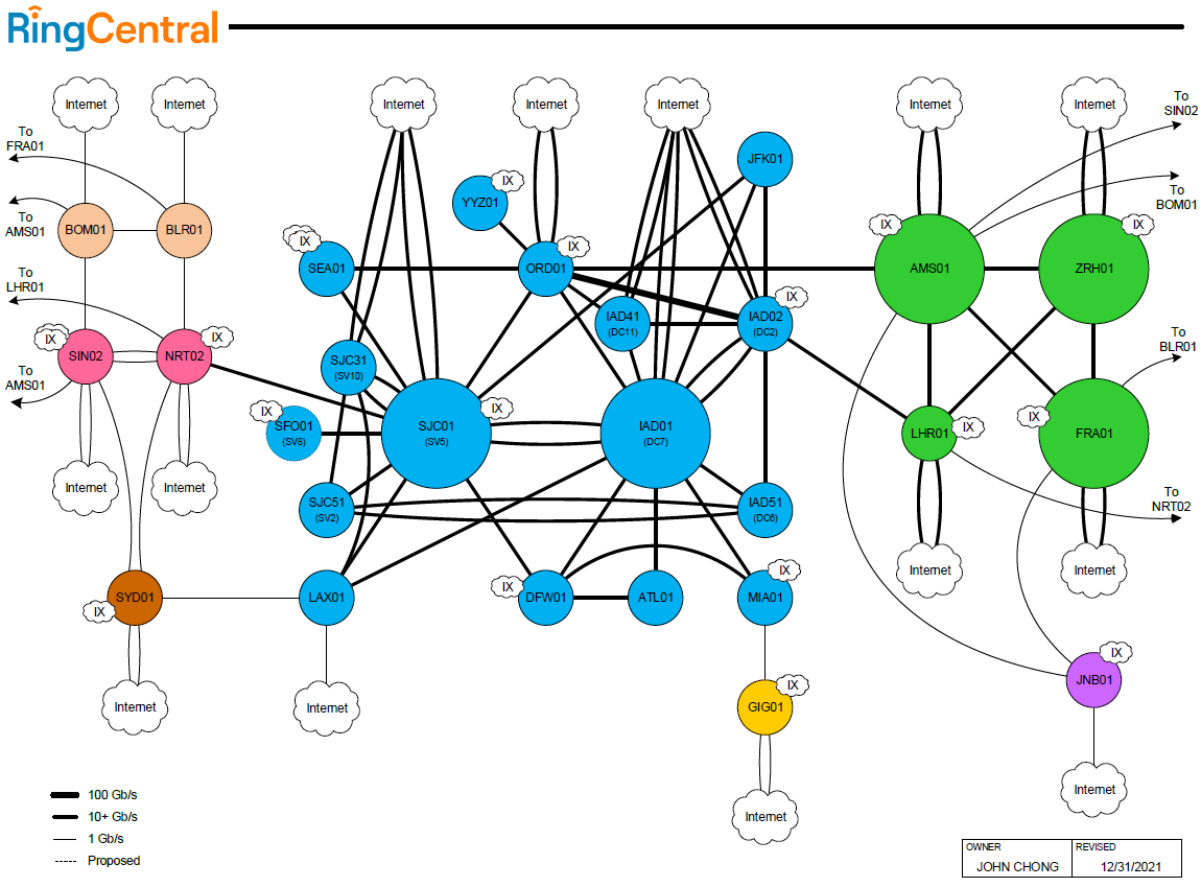

FIGURE 2: OVERVIEW OF RINGCENTRAL'S DATA CENTER INTERCONNECTIVITY

5. Software

IT & SECURITY SYSTEM SOFTWARE

RingCentral MVP are supported by the following software and types of software:

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

6. People

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 including:

- Security Operations
- Security Operations Center (SOC)
- Application Security
- Trust and Enablement
- Compliance
- Service Abuse and Fraud Management (SAFM)

The Operations team consists of various teams including Architectural Operations (ArchOps), Database Administrators (DBAs), Data Center Operations (DCOps), Media ArchOps, and Network Operations (NetOps).

The IT team consists of Corporate IT Infrastructure and IT End User Services (EUS). The Site Reliability Engineering (SRE) division includes Development Operations (DevOps), Network Operations Center (NOC), and System Operations (SysOps) teams.

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. 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.

7. Data

RingCentral MVP production databases contain customer data, metadata, and history data for the message, video, and phone services. RingCentral Video production databases contain video, history, and metadata. Key types of customer content collected by RingCentral MVP include, but not limited to text messages, faxes, attachments, voicemails, transcripts, messages, message attachments, video recordings, and video meeting transcripts. Key types of service data collected by RingCentral MVP include, but not limited to account data (including customer name and email address), usage data, call detail records (CDRs), and metadata (including time, recipient, sender, and location) associated with faxes, voicemails, and call recordings.

Key types of data collected by RingCentral Video include, but not limited to access tokens for calendar integration, chat messages, participants' names, account IDs, extension IDs, phone numbers, list of rooms and room statuses, and meeting recordings.

8. Processes and Procedures

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

- Information Security Policy
- Data Classification Standard
- Active Directory-SSL VPN Access Policy
- User Accounts Management on Databases
- Access Control Policy
- Change Management Policy
- Secure SDLC Policy
- Backup Retention Policy
- Global Service Desk Procedural Document
- Hardening Procedures
- Incident Management Process
- Security Incident Response Plan
- Security Policy
- Risk Assessment Policy
- Data Retention Policy and Procedure
- Datacenter Switchover/Isolation and Restoration and Datacenter Outages Prevention Playbooks
- Vulnerability Management and Patch Management Policy
- External Vulnerability Scan and Remediation Policy
- Network Access Policy

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, 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 Message Video Phone System cover only a portion of overall internal control for each user entity of RingCentral. It is not feasible for the criteria related to the Message Video Phone System 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 related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	Complementary Subservice Organization Controls	Related Criteria
1	Access to hosted systems requires users to use a secure method to authenticate.	**CC 6.1**
2	User content is segregated and made viewable only to authorized individuals.	**CC 6.1**
3	Network security mechanisms restrict external access to the production environment.	**CC 6.1 and CC 6.6**
4	New user accounts are approved by appropriate individuals prior to being provisioned.	**CC 6.2**
5	User accounts are removed when access is no longer needed.	**CC 6.2 and CC 6.3**
6	User accounts are reviewed on a regular basis by appropriate personnel.	**CC 6.2 and CC 6.3**
7	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.	**CC 6.3**
8	Access to physical facilities is restricted to authorized users.	**CC 6.4**

	Complementary Subservice Organization Controls	Related Criteria
9	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	CC 6.5
10	Encrypted communication is required for connections to the production system.	CC 6.6
11	Access to hosted data is restricted to appropriate users.	CC 6.7
12	Hosted data is protected during transmission through encryption and secure protocols.	CC 6.7
13	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.	CC 6.8
14	System configuration changes are logged and monitored.	CC 7.1
15	Vulnerabilities are identified and tracked to resolution.	CC 7.1
16	Security events are monitored and evaluated to determine potential impact per policy.	CC 7.2
17	Operations personnel log, monitor, and evaluate incident events identified by monitoring systems	CC 7.3
18	Operations personnel respond to, contain, and remediate incident events, and update stakeholders, as needed.	CC 7.4
19	System changes are documented, tested, and approved prior to migration to production.	CC 8.1
20	Access to make system changes is restricted to appropriate personnel.	CC 8.1
22	Operations personnel monitor processing and system capacity.	A 1.1
23	Environmental controls protect the physical devices supporting the production environment.	A 1.2
24	System failover and backup procedures are tested.	A 1.3

D. Complementary User Entity Controls

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

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

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

	Complementary User Entity Controls	Related Criteria
1	User entities are responsible for managing their account policies, user permissions, and login information.	**CC 6.3**
2	User entities are responsible for designating an administrator extension (phones numbers).	**CC 6.3**
3	User entities are responsible for the settings on their extensions.	**CC 6.3**
4	User entities are responsible for securing communications with their email system.	**CC 2.3, C 1.1**
5	User entities are responsible for implementing single sign-on.	**CC 6.1**
6	User entities are responsible for their account and meeting configurations.	**CC 6.1**

MOSSADAMS