SOC 3 Report

Cisco Webex Meetings + Cisco Webex Teams

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability, Privacy and the Suitability of the Design and Operating Effectiveness of Controls

For the period, October 13, 2018 to October 12, 2019

Manoj Jain, CPA in association with DNVGL

Table of Contents

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Section 1
Independent Service Auditor's Report

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Independent Service Auditor's Report

To: Management of Cisco Systems, Inc. – Collaboration

Scope

We have examined Cisco's ("Service Organization") accompanying assertion titled "Management of Cisco's Assertion" ("assertion") that the controls over "Cisco Webex Meetings and Cisco Webex Teams ("system") were effective throughout the period October 13, 2018 to October 12, 2019, to provide reasonable assurance that Cisco's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

Cisco 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 Cisco's service commitments and system requirements were achieved. Cisco has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cisco 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. 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 Cisco'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 Cisco's service commitments and system requirements based the applicable trust services criteria
- Cisco Webex ISO 27001:2013, 27017:2015, and 27018:2019 audit conducted by DNV GL and the related evidence

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

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

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 Cisco's system were effective throughout the period October 13, 2018 to October 12, 2019, to provide reasonable assurance that Cisco's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Manoj Jain, CPA
(Colorado Membership Number - 0023943)

October 19, 2019
Mumbai, India

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Annexure to Cisco Webex Meeting and Webex Teams SOC 3 Report

October 19, 2019

DNV-GL and Independent Service Auditor participated in the SOC 2 Type II attestation of Cisco Webex Meetings and Cisco Webex Teams.

The ISO 27001:2013, ISO 27017:2015 and ISO 27018:2019 audit evidences for these audits carried out by DNVGL were shared and used by the Independent Auditor for the attestation which formed the basis for the SOC 2 type II attestation to support criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria).

Signed,

Shamanna Nandakumar

Lead Auditor, ISMS

DNV-GL Business Assurance India Private Limited

DNV-GL Business Assurance , Unit No. S2003, 20th Floor, World Trade Center, Brigade Gateway Campus,

No.26/1, Dr. Rajkumar Road, Malleshwaram West, Bengaluru – 560 055 , +91 80 23081100 (B).
www.dnvgl.com

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Section 2
Management of Cisco's Assertion

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Management of Cisco's Assertion

Cisco's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over "Cisco Webex Meetings and Cisco Webex Teams" (system) throughout the period October 13, 2018 to October 12, 2019, to provide reasonable assurance that Cisco's service commitments and system requirements relevant to security, availability, confidentiality and privacy were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period October 13, 2018 to October 12, 2019, to provide reasonable assurance that Cisco's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy ("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).* Cisco Webex Meetings and Cisco Webex Teams 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 3.

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 October 13, 2018 to October 12, 2019, to provide reasonable assurance that Cisco's service commitments and system requirements were achieved based on the applicable trust services criteria.

Cisco Systems, Inc.

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Section 3

Description of Cisco Webex Meetings and Cisco Webex Teams

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Description of Cisco Webex Meetings and Cisco Webex Teams throughout the period October 13, 2018 to October 12, 2019

Company Background

Cisco Systems, Inc. (“Cisco” or the “Company”) (NASDAQ: CSCO) was incorporated in California in December 1984, and is headquartered in San Jose, California. Cisco is a global leader in information technology (IT). Cisco designs, manufactures, and sells Internet Protocol (IP)-based networking and other products related to the communications and IT industry and provides services associated with these products and their use. Cisco provides a broad line of products, services and solutions for transporting data, voice, and video within buildings, around campuses, and around the world. Cisco products are designed to transform how people connect, communicate, and collaborate. Cisco products are installed at enterprise businesses, public institutions, telecommunications companies and other service providers, commercial businesses, and personal residences.

Report Scope and Purpose

The scope of this report is limited to Cisco Webex Meetings and Cisco Webex Teams operations including equipment owned by Cisco and operated by permanent, temporary and contract Cisco personnel used for Cisco Webex Meetings and Cisco Webex Teams operations.

- Cisco Webex Meetings product is used in this report to refer to: Cisco Webex Messenger, Cisco Webex Meetings, Cisco Webex Training, Cisco Webex Events, Cisco Webex Support.
- Cisco Webex Teams product is used in this report to refer to: Cisco Webex Teams service, Cisco Webex Control Hub and Cisco Webex for Developers.

This Service Organization Controls (SOC) report is an examination of controls relevant to the security, availability, confidentiality, privacy and the C5 Cloud Controls of the services performed by Cisco Webex Meetings and Cisco Webex Teams under SSAE 18, Attest Engagements (AICPA, Professional Standards) prepared pursuant to the AICPA guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

This section of the report is intended to provide user organizations and independent auditors with information about Cisco Webex Meetings and Cisco Webex Teams system design and implementation to meet the criteria for the security, availability, confidentiality, and privacy principles set forth, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria) (“applicable trust services criteria”).

Because this description is intended to focus on the controls relevant to achieve the principles Security, Availability, Confidentiality, and Privacy only, it does not encompass all aspects of the services or procedures performed by Cisco Systems Inc.

Subservice Organizations

Cisco utilizes several subservice providers for hosting services, colocation services and other cloud services as part of offering Cisco Webex products to its customers. These subservices are not included within the scope of this description.

Principal Service Commitments and System Requirements

Cisco designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments that Cisco makes to user entities, the laws and regulations that govern the provision of products and services to its clients, and the financial, operational, and compliance requirements that Cisco has established for the services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

Cisco establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cisco's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, information technology (IT) and other hardware,
- Software including application programs and IT system software that support application programs,
- People including executives, sales and marketing, client services, product support, information processing, software development, IT,
- Procedures (automated and manual), and
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Cisco's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Cisco's customers are not included within the boundaries of its system.

All policies, process, procedures, monitoring, response, and communication described herein are implemented for the purpose of securing the Cisco Webex Meetings and Cisco Webex Teams infrastructure, and for ensuring the security, availability, confidentiality, and privacy of the customer information that Cisco Webex Meetings and Cisco Webex Teams requires to provide the service.

Cisco Webex Meetings Product Overview

Cisco Webex Meetings is a cloud-based service that provides virtual meeting rooms in which participants from diverse locations can collaborate in real time. The core of the Cisco Webex Meetings service offering is to host audio and video conferencing.

Cisco Webex Meetings offers its customers several types of conference services through ISPs and partners. These services provide a variety of conference formats adapted to meet differing customer requirements. Services include the following:

- Cisco Webex Meetings – Web and Video Conferencing service that enables people to meet and collaborate.
- Cisco Webex Events – Feature that enhances user's reach and effectiveness with online events and meetings. Users can communicate with internal and external audiences on a larger scale. Speakers can also interact with participants in real time using polling, chat, and threaded questions and answers (Q&A).
- Cisco Webex Training – Hosted online training solution that delivers live instruction.
- Cisco Webex Support – Provides real-time IT support and customer service to employees and customers anywhere in the world.
- Cisco Webex Messenger –Delivers Enterprise Instant Messaging (EIM) services securely over the Internet.

Cisco Webex Meetings is hosted on computer clusters located in data centers distributed around the world. Each service cluster in the data center connects to the larger Cisco Webex Meetings network which provides configuration, conference management, and security. The Cisco Webex Meetings network for each cluster connects to the Cisco network which provides additional security and separation for the Cisco Webex Meetings production environment.

System and Boundary Definition

Customer traffic originating on a Cisco Webex Meetings client is encrypted on the device and is carried across the internet to the Cisco data center. At the data center, customer traffic enters the Cisco shared network and is routed to the Cisco Webex Meetings network environment. Cisco Webex Meetings network border implements security through firewalls, intrusion detection systems (IDS), SSL load balancers, and SSL accelerators before it is handed off to the next architecture layer for processing.

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

The SSL accelerator terminates the session preventing direct connection between the user and the Cisco Webex Meetings environment. Firewalls are installed between all Cisco Webex Meetings production network segments.

Cisco Webex Meetings network infrastructure components add protection between Cisco Webex Meetings production components and external and internal users. The network perimeter is protected by firewalls. Any network traffic entering or leaving a Cisco Webex Meetings data center is continuously monitored using an intrusion detection system (IDS). The Cisco Webex Meetings network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and access control lists (ACLs).

Key infrastructure components include the following:

- DDOS Protection – Protects against Distributed Denial of Service attacks
- Firewalls – Filters traffic through Cisco Access Control Lists (ACL).
- IDS – Intrusion detection systems are used to analyze unencrypted traffic and identify known attacks and abnormal behavior. The appropriate security personnel are alerted when incidents are detected.
- SSL Load Balancers – Distributes SSL-based traffic among Cisco Webex Meetings application processors.
- SSL Accelerator – Negotiates SSL connection with Cisco Webex Meetings application processors and terminates traffic.

Core Cisco Webex Meetings production components include the following:

- Application and Web Servers – Provides authentication of customer users and site administration; Meeting portals for scheduling, editing, and attending meetings, and static content for pages. Customers are displayed different Cisco Webex Meetings landing pages based on privileges assigned to the user.
- Meeting Server – Provides desktop sharing capability for customer users. Desktop sharing includes remote desktop meetings, sharing of applications, and sharing of the desktop.
- Multimedia Server – Enables VOIP and video conference capability for customer users. When meeting attendees choose this option, voice conferencing is performed within the application and leverages a user's laptop speakers and microphone or a connected headset.
- Telephony Server –Provides audio conferencing service and serves as an audio bridge for PSTN and IP telephony devices. This option provides a phone number, meeting number and security PIN that users may dial into a meeting integrated with the Cisco Webex application hosted on a users' browser.

Internal Cisco Webex Meetings administrators perform a variety of functions for Cisco Webex Meetings operations. Internal administrative users are subject to, manage, or apply in the Cisco Webex Meetings environment. An overview of the functions is as follows:

- Authentication – Cisco Webex Meetings uses several types of authentication methods to manage access to all parts of the production environment. Privilege levels have been created to manage internal user access to different aspects of the network and customer access to the service.
- Database – Database servers are used to store configuration, meeting metadata, and meeting recordings when they are requested.
- Application – The application server supports activity that includes authentication of customer users, site administration, and the meeting portal for scheduling, editing, and attending meetings.
- Security – Security tools are used to monitor the network, identify risk, collect data, store data, and analyze data.

Cisco Webex Teams Product Overview

Cisco Webex Teams service offering is a cloud Collaboration platform that provides messaging, calling and meeting features. The Cisco Webex Teams application is a client app that connects to the Cisco Webex Teams Platform and provides a comprehensive tool for teamwork and collaboration across multiple types of endpoint devices. Users can send messages, share files, and meet with different teams, all in one place. Calling and meeting features are provided by Cisco Webex Meeting.

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

System and Boundary Definition

Cisco Webex Teams is a portfolio of capabilities that provides a collaboration suite for teams to create, meet, message, place and receive calls, whiteboard, and share. The following capabilities are in scope for this report:

- The Cisco Webex Teams service (henceforth referred to as “Platform”).
- Cisco Webex Control Hub (henceforth referred to as “Control Hub”).
- Cisco Webex for Developers (Application Programming Interface, henceforth referred to as “API”).

The Cisco Webex Teams Platform provides a Platform as a Service (PaaS) for applications, integrations and bots. Customers interact with the Control Hub application. Customers may use the API to develop applications, integrations or bots.

The Platform provides a highly-scalable, public cloud system that offers data, operations, logging, monitoring, and alerting services. The Platform is a cloud service that itself uses global cloud Infrastructure as a Service (IaaS) from Cloud Service Providers.

The Control Hub provides a user interface and functionality for administration of customer companies, partners, and users. It is primarily used by external customer administrators to administer customer users, manage customer configurations, and other capabilities delegated to customers.

The Control Hub is comprised of a user interface and backend services which utilizes the Platform. These provide status and reports of services, Cisco Webex Teams spaces, users, devices, etc. Settings can be configured at an organizational level including domains, SIP addresses, directory synchronization, and authentication. Information for troubleshooting is made available to users.

The API provides access to the Platform for development of applications, integrations, and bots. The API is available through standard secure internet protocols. Cisco internal and external customers can develop applications, integrations, and bots that utilize the messaging and file repository capabilities of the Platform.

Shared Responsibility

The compliance and controls environment for the Platform, Control Hub, and API is based upon the shared responsibility and governance of:

- Cisco Management
- Cisco Webex Teams
- Cloud Service Providers
- Application and integration owners
- The customer

Cisco Management and Cisco Webex Teams have established and maintain an internal control environment that regularly validates and monitors compliance with established policies and procedures. The objective of the internal control environment is to provide reasonable assurance as to the security, availability, integrity, confidentiality, and privacy of customer information. The internal control environment, policies and procedures, and assurance practices includes validation and monitoring of controls provided by third parties, including IaaS Cloud Service Providers.

The owners of the applications, integrations and bots that utilize the Platform are responsible for security compliance and controls for their applications, integrations, and bots, including updates, security patches, and security of data that does not reside within the Cisco Webex Teams service.

Customers are responsible for the security compliance and governance of their user accounts, account settings and other information within their control.

People

Cisco’s organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing the Cisco’s tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Cisco has also established authority and appropriate lines of reporting for key personnel.

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Cisco is organized into business entities, units and corporate functions. Cisco Webex is in the business entity called Collaboration. Collaboration produces a suite of products that make work more intuitive with easy-to-use collaborative technologies. The suite of Collaboration products enables businesses through Unified Communications, Contact Center, Conferencing, and Collaboration Endpoints solutions.

The Cisco Collaboration security organization is embedded in the Cisco Webex product operation, and directly aligned with the Cisco enterprise Security and Trust Organization. The organizational independence and intrinsic presence institutionalizes a security-first governance model for Cisco Webex.

The following are the roles within Cisco Collaboration organization is accountable to the security, availability, confidentiality, privacy, and the C5 Cloud Controls:

- Chief Security Officer
- SVP/GM, Webex Meetings, Teams, Calling & Devices
- VP/Director of Platform
- VP/Director of Operations
- VP/Director of Development Engineering

Cisco follows a structured on-boarding process to familiarize new employees with Cisco processes, systems, security practices, policies and procedures. Cisco requires that newly hired employees certify that they have reviewed, understand, and agree to confidentiality and data protection policies and guidelines by signing the Code of Business Conduct (COBC). Contractor companies are required to sign a contract including terms and conditions with confidentiality and non-disclosure restrictions.

Anyone receiving access to Cisco facilities, systems, or sensitive information must meet Cisco's background check standards. Any applicant who refuses to complete the background check process will not be eligible for Cisco employment or Cisco access. Cisco complies with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting background checks. All pre-employment and pre-access background checks are individually assessed.

Data

Several layers of security technologies and processes protect all data collected in Cisco Webex utilizing a defense-in-depth approach. Below are examples of controls placed in different layers of Cisco Webex operations to protect customer data.

- Physical access control – Controlled through biometrics, badges, and video surveillance. Access to the data center requires approvals and is managed through an electronic ticketing system.
- Network access control – Network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco data center is continuously monitored using an intrusion detection system (IDS). Network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and access control lists (ACLs).
- Infrastructure monitoring and management controls – Every component of infrastructure, including network devices, application servers, databases, and storage devices, is hardened to stringent guidelines. They are also subject to regular scans to identify and address any security concerns.
- Logical access control – All access to systems is allowed only in accordance with the "segregation of duties" principle. It is granted only on a need-to-know basis and with only the level of access required to do the job. Employee and contractor access to these systems is regularly reviewed for compliance. Cisco Webex employees and contractors do not access customer data unless access is requested by the customer for support reasons.

Reviewed and approved annually, the Cisco cryptographic policies help ensure the types and levels of encryption necessary for all products and services. All data in-transit to and from the Cisco Webex data center to Cisco Webex clients, with the exception of Collaboration Meeting Rooms (CMR) enabled devices, is encrypted. Additionally, in accordance with Cisco policies, passwords are encrypted.

For more information, refer to the Cisco Webex Meetings Security White Paper and Cisco Webex Teams Security White Paper

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public

Availability

The Cisco Webex Collaboration Cloud environment consists of server clusters to manage shared computing resources over the network. The Cisco data centers' global site backups and high-availability design enables the geographic failover of Cisco Webex services. There is no single point of failure. There are geographically diverse failover clusters that can immediately resume the duties of primary clusters to prevent any discontinuity of service. Capacity monitoring meetings are held to monitor trends of network and server usage and identify needs for cluster expansion.

Cisco Collaboration organization has a formal Disaster Recovery Plan (DRP) in place. The DRP establishes a process for responding to a catastrophic event. In some cases, the DRP can be relied upon in response to extended disruption of service as laid out in the Cisco Incident Response Plan. The DRP describes the objectives, assumptions, responsibilities, and actions to be performed in such an event. The plan identifies teams, contacts, responsibilities, and action plans.

Confidentiality

Cisco will retain personal information as needed to fulfill the purposes for which it was collected. Personal information will be used as necessary to comply with our business requirements, legal obligations, resolve disputes, protect our assets, and enforce our agreements.

Customer Active Site Data is stored as long as that customer site is active, until the customer requests deletion. Customer deactivated sites will hold the data for a limited time and after that it will be purged. After the retention period is reached, all the content is purged and becomes irretrievable. For more information on data deletion and retention, refer to Cisco Webex Meetings Privacy Data Sheet and Cisco Webex Teams Privacy Data Sheet.

Customers can request deletion of other personal data retained on the Cisco Webex platform by sending a request to privacy@cisco.com or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes, Cisco endeavors to delete the requested data from its systems within 30 days. Users seeking deletion of other personal data retained on the Cisco Webex platform must request deletion from their employer's site administrator.

Privacy

Cisco intends to protect the personally identifiable information (PII) entrusted to us and treat it securely in accordance with the Privacy Statement. Cisco Webex has a privacy program based on Privacy by Design in order to protect customer's PII. The privacy program is driven by policies and requirements that are determined by the corporate Chief Privacy Officer, Global Data Privacy Office, and Data Protection & Privacy group.

For personal data collected by Cisco Webex products, and listed in the Cisco Webex Meetings Privacy Data Sheet and Cisco Webex Teams Privacy Data Sheet, Cisco acts as the Processor of this data. Cisco processes this information in order to provide the service requested by the customer. Cisco Webex provides Privacy Data Sheets containing information on PII that is being processed. For more information regarding PII or to view the Privacy Data Sheets, refer to the Cisco Trust Center.

Cisco also acts as a Controller for a subset of the Registration and Host and Usage data listed in the Privacy Data Sheet. Cisco determines the purposes and means of processing some of this data for marketing and to conduct usage analytics of the product.

© 2019 Cisco and its affiliates. All rights reserved.

Classification: Cisco Public