SOC 3 Report

Program:

Cisco WebEx LLC's

WebEx messenger, WebEx meeting center, WebEx training center, WebEx event center, WebEx support center (WebEx Cloud Services)

For the period

November 16, 2016 to November 15, 2017

Accedere Inc. in association with DNV-GL

Accedere Inc.

Certified Public Accountants

info@accedere.us

Table of Contents

Section I

Independent Service Auditor's Report

ACCEDERE

Independent Service Auditor's Report

To: The Management of Cisco Webex Cloud Services
Location: San Jose, CA, USA

Scope

We have examined Cisco WebEx LLC's WebEx messenger, WebEx meeting center, WebEx training center, WebEx event center, WebEx support center accompanying assertion titled "Cisco Webex Cloud Services Management Assertion of …" that the controls within design of Cisco WebEx Cloud Services were effective throughout the period November 16, 2016 to November 15, 2017, to provide reasonable assurance that Cisco Webex Cloud service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100 A, *2016 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Cisco Webex Cloud Responsibilities

Cisco Webex Cloud 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 Webex Cloud service commitments and system requirements were achieved. Cisco Webex Cloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cisco Webex Cloud is responsible for selecting, and identifying in its assertion, the applicable trust service 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 Webex Cloud 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 Webex Cloud service commitments and system requirements based on the applicable trust services criteria.
- Cisco Webex Cloud Services ISO 27001:2013 audit conducted by DNV GL and the related evidence

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 Cisco Webex Cloud Services were effective throughout the period November 16, 2016 to November 15, 2017, to provide reasonable assurance that Cisco Webex Cloud service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Accedere Inc.
Certified Public Accountants
CPA License No: FRM 5000337
Denver, Colorado, USA
Place of Issue: Denver, CO
Date: June 29, 2018

Stamp & Signature
Ashwin Chaudhary
CPA, CISSP, CISA, CISM, CRISC,
CGEIT, CCSK, ISO 27001LA, PMP.
info@accedere.us

Annexure to Cisco Webex Cloud Services SOC 3 Report

25 May 2018

DNV GL and Accedere Inc. participated in the SOC 3 attestation of Cisco Webex Cloud Services.

The ISO 27001:2013 Audit evidences were shared and used for evaluation of controls which formed the basis for the SOC 3 attestation, to support the applicable criteria for the principles in Trust Services Criteria (TSC) 2016 for Security, Confidentiality and Privacy.

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

Section II

Management Assertion

Cisco Webex Cloud Services Management Assertion for WebEx messenger, WebEx meeting center, WebEx training center, WebEx event center, WebEx support center

We are responsible for designing, implementing, operating, and maintaining effective controls within Cisco Webex Cloud Services system throughout the period November 16, 2016 to November 15, 2017 to provide reasonable assurance that Cisco Webex Cloud service commitments and system requirements relevant to security, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in Section III 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 November 16, 2016 to November 15, 2017, to provide reasonable assurance that Cisco Webex Cloud service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2016 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Cisco Webex Cloud 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.

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 November 16, 2016 to November 15, 2017 to provide reasonable assurance that Cisco Webex Cloud service commitments and system requirements were achieved based on the applicable trust services criteria.

Cisco Systems, Inc.

Section III

Cisco WebEx LLC's

WebEx messenger, WebEx meeting center, WebEx training center, WebEx event center, WebEx support center (Webex Cloud Services)

Scope and Purpose

This Service Organization Controls (SOC) report is an examination of controls at Cisco Systems, Inc. relevant to the security, confidentiality, and privacy of the services performed by the Cisco WebEx Cloud Services 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 Cloud Services system design and implementation to meet the criteria for the security, 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, Confidentiality, and Privacy* only, it does not encompass all aspects of the services or procedures performed by Cisco WebEx LLC.

The scope of this report is limited to Cisco WebEx Cloud Services operations including equipment owned by Cisco and operated by permanent, temporary and contract Cisco personnel used for Cisco WebEx Cloud Services operations. Except were specified in the contract operating processes for customers, partners and colocation facilities are beyond the scope of this report.

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

Overview of Cisco WebEx LLC

Company Background

Cisco Systems, Inc. (Cisco) (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.

Cisco WebEx LLC is an organization in the Cisco Systems, Inc. family that produces, sells, and manages cloud-based collaboration solutions. The Cloud Collaboration Technology Group (CCTG) business unit provides on-demand, on-line audio/video conference and collaboration services. Cisco WebEx LLC provides the overall organizational processes and structure, and maintains overall responsibility for the business units, including CCTG, under its management.

Cisco WebEx LLC Organization

The following are the roles accountable to the security, confidentiality, and privacy of Cisco WebEx LLC:

- Vice President and General Manager, Cisco Cloud Collaboration Applications
- Vice President, Engineering, Cisco Cloud Collaboration Applications
- Vice President, Product Management, Cisco Cloud Collaboration Applications

These roles are responsible for working with Information Security (InfoSec) Cloud Security team and the Security and Trust Organization (S&TO) where there is a shared responsibility and governance for Cisco WebEx Services for which, every Cisco WebEx Cloud Services team member is responsible.

Information Security Organization

Cisco WebEx InfoSec Cloud Security Organization

- Compliance team – responsible for the governance of Cisco WebEx Cloud Services within the Cisco InfoSec Cloud team. This team is responsible for maintenance of Cisco WebEx Cloud Services Information Security Management System (ISMS)
- Security operations team – responsible for the operations of security compliance such as baseline configuration management and vulnerability management
- Chief Information Security Officer (CISO) – accountable to information security for the entirety of the Cisco WebEx LLC organization

The CCTG Governance Committee comprised of InfoSec and Cisco WebEx Cloud Services leaders is accountable for the overall governance framework, planning, directing, and controlling the security and risk aspects of business operations. The organizational structure assigns roles and responsibilities to provide oversight to confirm adequate resourcing, efficiency of operation, and segregation of incompatible duties.

The engineering, operations, and security governance group are responsible for the three key functional roles of the Cisco WebEx operation. The engineering team is responsible for the design, development, and reliability of Cisco WebEx Services. The operations team is responsible for the production environment including daily operations and maintenance, monitoring the platform components, repair, patches, and availability. Security governance group is responsible for establishing security baselines and ensuring adherence to security policies, standards, processes, and compliance requirements.
The security governance group is sponsored by the Information Security (InfoSec) organization. (Relevant to criteria CC1.2, CC1.3)

Cisco Systems, Inc. Computer Security Incident Response Team (CSIRT)

Cisco Systems, Inc. and the Security and Trust Organization (S&TO) have developed an Incident Response Plan which provides a high-level approach for how the incident response capability fits into the overall organization and describes the structure and organization of the incident response capabilities.
The incident handling methodology consists of the following phases:

- Incident Preparation
- Incident Detection and Analysis
- Incident Containment, Eradication, and Recovery
- Post Incident Activity and Evidence Collection

CSIRT provides a global staff of on-call security investigators. These investigators scrutinize security incidents in Cisco WebEx Cloud Services production environment and coordinate a response. As necessary, investigators provide forensic investigations support, coordinating with Cisco Systems, Inc. Legal, HR, and external entities, including law enforcement.

Cisco Systems, Inc. Product Security Incident Response Team (PSIRT)

Cisco WebEx LLC has established the external and internal incident reporting process to effectively provide all users a path for alerting the appropriate security incident response teams.
The PSIRT is Cisco Systems, Inc. official interface with the public security vulnerabilities.
The on-call Cisco Systems, Inc. PSIRT works 24 hours with company customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco WebEx Services.
In situations that require reporting to a government agency, the CSIRT and the Cisco WebEx Cloud Services supports the reporting.
Internal users can make reports to an internal mailer to CSIRT by submitting an incident reporting form provided on the Cisco Systems, Inc. intranet. (Relevant to criteria CC1.2, CC2.2, CC2.3, CC2.4, CC3.2, CC7.4)
Cisco WebEx LLC integrates audit review, analysis, and reporting processes to support organizational processes for investigation and respond to suspicious activities by leveraging Cisco WebEx Cloud Services security incident and event monitoring tools.

Cisco WebEx Cloud Services Overview

Cisco WebEx Cloud Services 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 Cloud Services offering hosts audio and video conferencing with data sharing, and chat. Cisco WebEx Services offers its customers several types of conference services through ISPs and partners. These services provide different conference formats correspondent with customer needs. Services include the following:

- **WebEx Meeting Center** – WebEx Meeting Center is a Web and Video Conferencing that enables people to easily meet, collaborate, and stay productive anywhere, anytime, on any device
- **WebEx Event Center** – WebEx Event Center makes it easy and cost-effective to enhance 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)
- **WebEx Training Center** – WebEx Training Center is a hosted online training solution that makes it easy to deliver highly effective, live instruction - to anyone, anywhere
- **WebEx Support Center** (including WebEx Remote Access) – WebEx Support Center provides real-time IT support and customer service to employees and customers anywhere in the world
- **Cisco Collaboration Meeting Rooms Cloud –** Collaboration Meeting Rooms (CMR) is a video conferencing feature in the WebEx Meeting Center subscription from the Cisco Collaboration Cloud
- **WebEx Cloud Connected Audio –** Cloud Connected Audio (CCA) is an enterprise audio conferencing solution for WebEx meetings that extends IP Telephony
- **WebEx Messenger** – WebEx Messenger delivers Enterprise Instant Messaging (EIM) services securely over the Internet

Cisco WebEx Cloud Services are installed on computer clusters located in data centers distributed around the world. Each service cluster in the data center connects to the larger Cisco WebEx Cloud Service network which provides configuration, conference management, and security. The Cisco WebEx Cloud Service network for each cluster connects to the Cisco network which provides additional security and separation for the Cisco WebEx Cloud Service production environment. (Relevant to criteria CC2.1, CC5.1)

Cisco WebEx Cloud Services System and Boundary Definition

The WebEx Network illustrated in Figure 1, represents the traffic flow from the customers and WebEx Cloud Services administrative personnel into the Cisco WebEx Cloud Services data center.

Customer traffic originating on a WebEx 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 Cloud Services network environment. Cisco WebEx Cloud Services 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 WebEx processing. The SSL accelerator terminates the session preventing direct connection between the user and the Cisco WebEx Cloud Services environment. Firewalls are installed between all Cisco WebEx production network segments.

Cisco WebEx Cloud Services administrative traffic follows a similar course as WebEx customer traffic. Cisco WebEx Cloud Services administration is segmented by function. Administration is role-based such that an administrator access approval is granted to a specific function in the network. (See Access Management) (Relevant to criteria CC2.1, CC5.1)

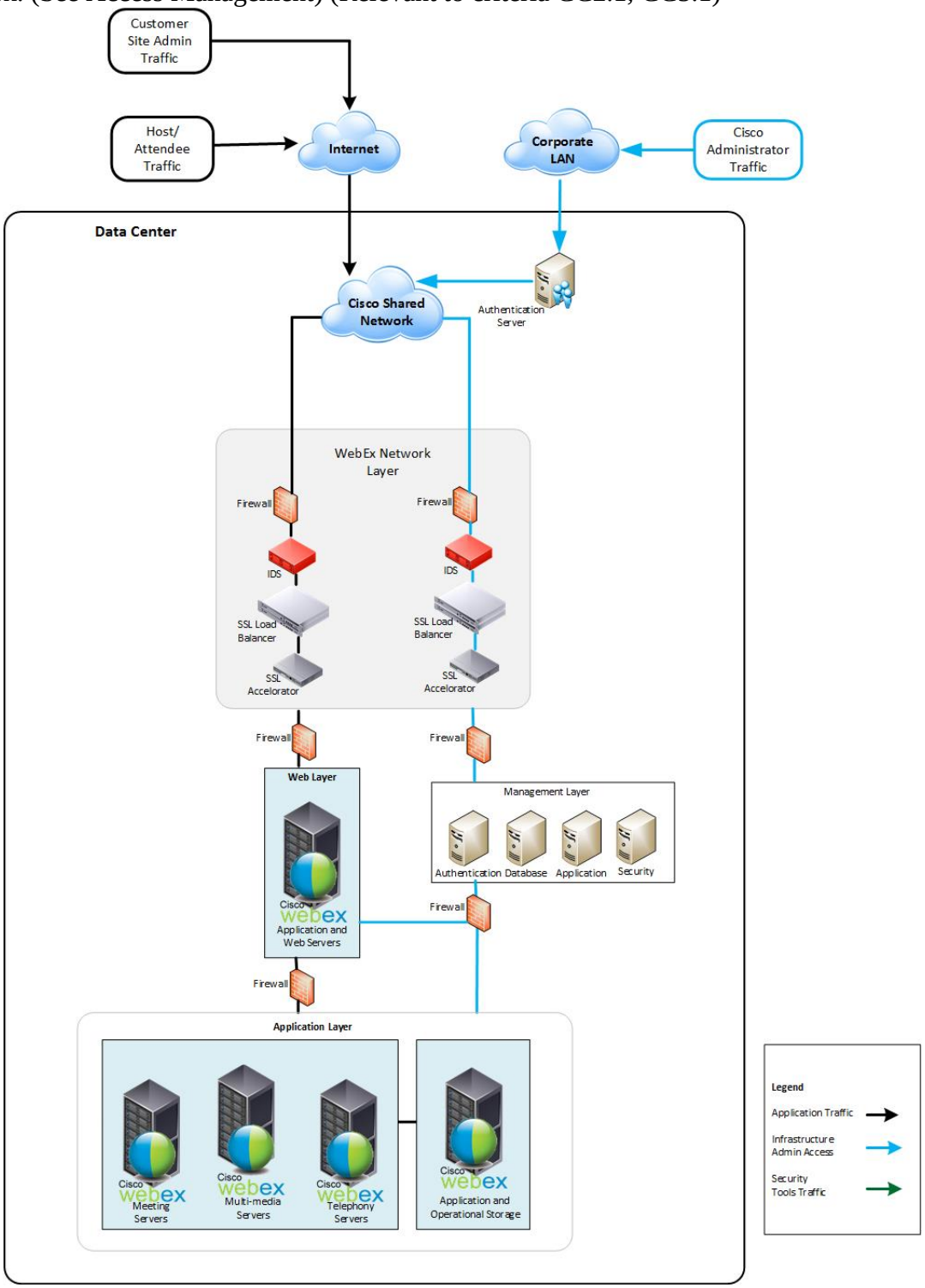

Figure 1 WebEx Network

Cisco telecommunications and networking uses various mechanisms, devices, software, and protocols across interrelated and integrated programs designed to protect its customers and its data.

Cisco WebEx Cloud Services uses a wide spectrum of intrusion detection system (IDS), varying from devices to software applications that monitors the network systems for malicious activity or policy violations.

Cisco WebEx network infrastructure components add protection between WebEx Cloud Services production components and external and internal users. The network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco WebEx data center is continuously monitored using an intrusion detection system (IDS). The Cisco WebEx 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:

- **Firewalls –** Filter traffic through Cisco Access Control Lists (ACL). ACL filters ensure that only traffic from approved source IP addresses are allowed
- **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 WebEx Cloud Services application processors
- **SSL Accelerator –** Negotiates SSL connection with Cisco WebEx Cloud Services application processors. Terminates traffic

Core Cisco WebEx Cloud Services production components include the following:

- **Application and Web Servers** – provide authentication of customer users and site administration; Meeting portals for scheduling, editing, and attending meetings; and static content for pages. Customers are displayed a different Cisco WebEx Cloud Services landing page 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 WebEx application hosted on a users' browser

Internal WebEx Services users perform a variety of functions for Cisco WebEx LLC operations. Management Layer section in the drawing indicates functions internal users are subject to, manage, or apply in the Cisco WebEx Cloud Service environment. An overview of the functions is as follows:

- **Authentication** – WebEx 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

Customer Data Flow

Cisco WebEx Services defines three, core user roles pertinent to the flow of customer data in the system: site administrator, host, and attendee. The site administrator is responsible for managing the customer's WebEx site including its configuration and creating hosts. A host is an end user to whom the site admin grants permission to create Cisco WebEx Cloud Service meetings. Attendees are meeting participants who may or may not be configured users. Customer data in the system takes two forms: configuration data including personal data that is used for establishing connections and conference data which can include voice and video, shared applications such as spreadsheets, white board, chat, etc. Figure 2 shows how customer data flows in the Cisco Cloud Service WebEx environment. (Relevant to criteria CC2.1, CC5.1)

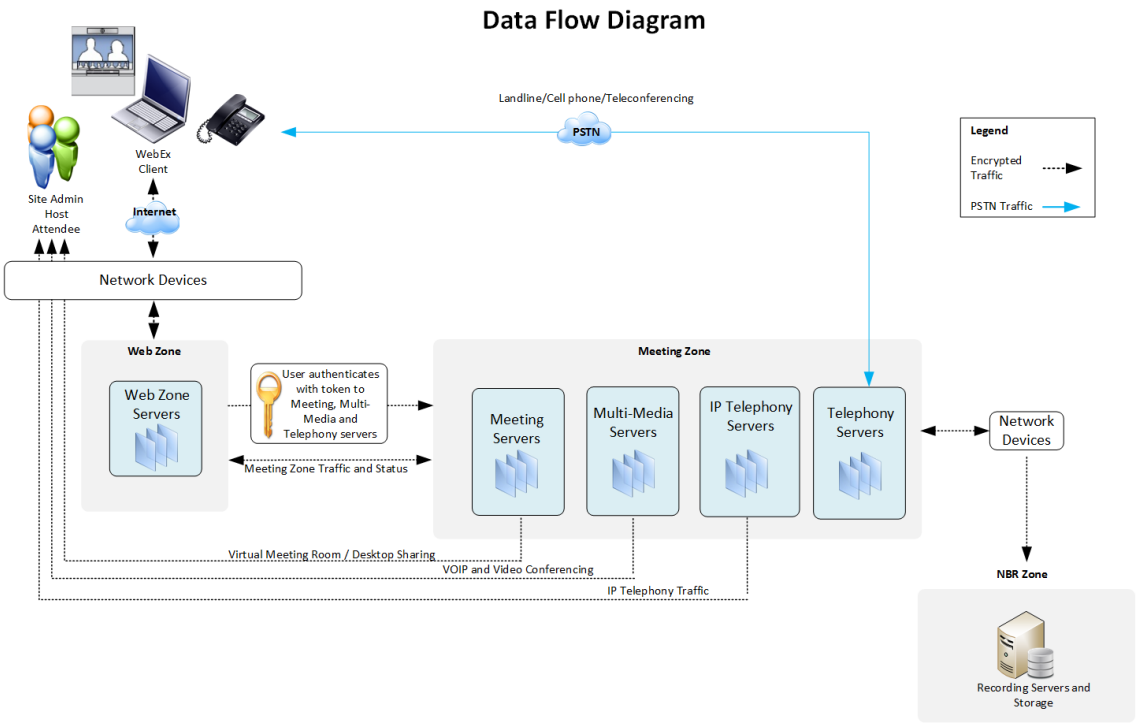

Figure 2 Data Flow

Site Administration Flow

Once a customer has designated a person to perform the site administration role, Cisco WebEx Services provides that person appropriate credentials to access the Cisco WebEx Cloud Service

portal to the customer's site. The person uses the information provided to access the portal, then configures the customer's site including creating users and uploading a certificate for authentication. The configuration information is stored in the Web zone shown in Figure 2.

Cisco Entity Controls

Overview of Controls

The AICPA deems internal controls as processes that are developed and implemented by an entity's board of directors, management, and other personnel designed to provide reasonable assurance of achieving the entities objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

The AICPA further identifies five interrelated components in which to view these categories:

- **Control Environment** – The overarching tone of the organization affecting the control consciousness of its people. This is the foundation for all other components of internal control providing discipline and structure
- **Control Activities** – Policies and procedures that are established and executed to ensure that the actions identified by management as necessary to address risks to achieve the entity's control objectives are effectively carried out
- **Information and Communication** – Systems, both automated and manual, that are used to identify, capture and exchange information that allow entity personnel to carry out their responsibilities
- **Monitoring** – The process of assessing the quality and effectiveness of the internal controls over time
- **Risk Management** – The processes the entity uses to identify and analyze the risks to achieving its objectives that are the basis for determining how the risks are managed

Cisco Common Control Environment

Management, in conjunction with the groups it creates, is responsible for creating, maintaining, and monitoring the policies, standards, and procedures that constitute the internal controls deemed to provide reasonable assurance of the integrity and reliability of the production systems, and for the protection of customer information and assets against unauthorized use and disposition. Compliance with Cisco policies and standards is required and verified. A fundamental component of this oversight is the CCTG Governance Committee, a team of business management representatives, a set quarterly agenda for reporting, a process of review and risk assessment, and formal record of these elements. (Relevant to criteria CC1.1, CC1.2, CC1.3)

Information Security Management System (ISMS)

An Information Security Policy exists to support Cisco WebEx LLC in developing policies and procedures to protect security, confidentiality, and privacy of customer data, to ensure compliance to applicable legal requirements, contractual obligations, and any security requirements. Under the policy, Security and Trust and Information Security Cloud teams are

responsible for periodic assessment of the level of compliance to legal requirements, operational controls, and overall risk posture. Assessment reports are presented to the Information Security Management System (ISMS) Governance Committee and other appropriate levels of management which include:

- The importance/criticality of information resources
- The effectiveness of present information security arrangements
- Special circumstances that increase the probability of incidents occurring
- New threats and vulnerabilities
- Recommendation for ongoing improvements
- The status of current improvement activities

As is further detailed in the section Cisco WebEx Cloud Services Platform Controls, (Relevant to criteria CC1.2, CC2.4, CC2.5, CC4.1, and CC7.4) information technology is governed by ISMS processes and procedures including the following:

- Access Management
- Change Management
- Configuration Management
- Cisco Secure Development Lifecycle
- Data Center Security
- Incident Management
- Vulnerability Management
- Business Continuity Management

Internal Communication

The ISMS program uses a variety of mechanisms to communicate security requirements and expectations to its employees and contractors. The following assure that employees and contractors are informed and understand our security policies and expectations:

- Acknowledge the Cisco Code of Business Conduct (COBC)
- Take and pass the annual Security Awareness training course
- Read the Security Policies and Standards
- Read the CCTG ISMS Standard Manual
- Take and pass the Cisco Security Ninja Program

During onboarding and annually thereafter, the organization provides mandatory Annual Security Awareness training which reaffirms the location of all policies and standards. Annually, the Organization Business Unit leader will send an email containing:

- The importance of adhering to the Organization Information Systems Policy
- The importance of meeting the Organization Security Objectives
- The importance of the ISMS
- The importance of adhering to the ISMS
- The Organization's responsibilities under the applicable laws & regulations
- The criticality of continual improvement
- Link to CCTG ISMS Standard Manual, which contains:
  - The latest version of the CCTG Information Systems Policy
  - The latest version of the CCTG Security Objectives
  - Link to ISMS Policies and Standards intranet page
  - Link to the CCTG ISMS Roles and Responsibilities document containing roles, responsibilities, and authorities
- Quarterly, an ISMS GC representative will send an email to employees, contractors, consultants, temporaries, and other workers with selected relevant information.

ISMS program maintains resources to communicate internally all ISMS documentation, policies, and standards. These policies and standards are managed in the Cisco enterprise documentation control system.

External Communications

Cisco WebEx LLC has implemented various methods of external communication to support its customer base and the community. Communication is in place and can be found at the following:

- Operational issues, concerns, or questions: https://collaborationhelp.cisco.com
- Security White Papers: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf
- Vulnerabilities from PSIRT: https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html
- Privacy Statement and Supplements:
  https://www.cisco.com/web/siteassets/legal/privacy_full.html
  https://www.cisco.com/c/en/us/about/legal/privacy-full/webex-meeting-center-supplement.html
  https://www.cisco.com/c/en/us/about/legal/privacy-full/webex-messenger-supplement.html

- Cisco WebEx LLC (SaaS) Terms of Service to customers, external users, and partners: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf
- WebEx Configuration and System guides: https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

Supplier Management

Cisco WebEx LLC has a Supplier Management Program. Suppliers are evaluated as part of the Cisco CASPR/CASPRX process. The CASPR assessments evaluate the security risks to Cisco and provide recommendations. The benefits include the validation of security compliant architecture (with policy and standards), a proactive and predictable process, and the protection of Cisco data and brand.

Suppliers enter into an agreement which covers supplier duties, services, license and intellectual property rights, confidentiality, integrity, and availability. Agreements include security requirements and Service Level Agreements. (Relevant to criteria CC2.3, CC5.1, CC5.4, CC6.2)

Suppliers are required to report information security events. An annual review occurs for all key suppliers. Reviews cover the handling of non-public information, and legal review, the budget for the previous and next year, the security of the system, external certifications, as well as pertinent organizational structure reviews if they will affect the stability of the vendor. (Relevant to criteria C1.4, C1.5, C1.6, P6.1)

Suppliers for Cisco WebEx Cloud Services include only data center co-locations and staff augmentation. The risk assessments conducted annually include an internal audit and risk assessment for all data center co-location suppliers.

Personnel Management

Cisco human resource policies, procedures, and guidelines apply to all Cisco WebEx permanent, temporary, and contract personnel. Human resources requirements includes Background checks, Code of Business Conduct, and Education and Training.

Cisco requires that new-hire 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. (Relevant to criteria CC1.4, CC2.2, CC2.3, CC2.5)

The confidentiality policies and restrictions identify and address the following:

- Requirement to protect confidential company, former employer, and third party information and inventions
- Duration of coverage
- Terms for information to be returned or destroyed at contract cessation
- Expected actions to be taken in case of a breach of the contract or policies

Background Checks

Employees and contractors are required to pass a background check before being granted access to facilities, systems, and sensitive information. Background checks are performed during the hiring phase and are a condition of employment except where prohibited by local or national law. (Relevant to criteria CC1.4)

Nondisclosure Agreement

All WebEx personnel and non-personnel who require access to WebEx facilities, systems, and sensitive information are required to sign a nondisclosure agreement before being granted access. (Relevant to criteria CC1.4, CC2.4, P6.2)

Code of Business Conduct

Cisco requires all permanent new-hires to certify that they have reviewed, understood, and agreed to the confidentiality and data protection policies and guidelines as set forth in the Cisco Code of Business Conduct (COBC). The COBC sets guiding principles governing Cisco personnel behavior with respect to ethics, legal compliance, safeguarding proprietary and confidential information, conflicts of interest and other relevant areas. Employees are required to review and acknowledge the Cisco Code of Business Conduct annually. Contractors are required to review and agree to a confidentiality agreement with their employer as a condition of working at Cisco. (Relevant to criteria CC1.4, CC2.2, CC2.3, CC2.4, CC2.5, P6.2)

Education and Training

Cisco requires all WebEx permanent, temporary and contract personnel to take the following education and training:

- Security Awareness Training – annual training which features different security topics each year.
- Cisco Ninja White Belt Training – one time training on security fundamentals. (Relevant to criteria CC1.1, CC1.3, CC2.3)

Cisco Secure Development Lifecycle

Cisco WebEx is compliant with the Cisco Secure Development Lifecycle (CSDL).
The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle ensures defense-in-depth, and provides a holistic approach to product resiliency. CSDL is a process to ensure Cisco BUs develop cloud solutions adhere to the Cisco / Industry security standards. (Relevant to criteria CC7.1, CC7.2)
CSDL compliance is calculated based on information provided by the product teams and is measured based upon compliance to Product Security Baseline (PSB) requirement-level data and monitored over time. For cloud products CSDL requires a Cloud Approval to Operate (CATO). Compliance with CSDL cannot be waived. The CATO is Cisco's three-phase certification process. First is the discovery phase where registration and security planning occur. Second is the assessment phase where CSDL is invoked and driven to the attainment of the CATO certificate. The last phase is the governance and maintenance of the CATO. See Secure Design in platform controls.
More information regarding Cisco's Secure Development Lifecycle is available at: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html

Data Privacy & Protection

The Security & Trust Organization (S&TO) Data Privacy Office, headed by Cisco's Chief Privacy Officer, is responsible for Cisco Systems, Inc. assets and the S&TO Data Protection manages all aspects of data liability. This team is call the Data Privacy and Protection office (DPP). The Security & Trust Organization (S&TO) engages as a service to help employees examine their products and services to mitigate privacy risks, including global privacy compliance inquiries as well as understanding customer data and digitization strategies. (Relevant to criteria CC1.3, P5.1, P6.2)
Cisco WebEx LLC works with the DPP team to fully understand data privacy. In addition, every citizen of Cisco Systems, Inc. is continuously accountable to the protection of customer information. (Relevant to criteria P1.1, P1.2, P2.1, P3.1, P3.2, P4.1, P4.2, P4.3)
Policy, procedure, standards, guides and resources to enable complete understanding and enforcement of Cisco's data lifecycle include:

- Privacy and Data Protection
- Customer Data Protection
- Security Ninja White Belt (Data Privacy and Security Centric Training)
- Enterprise Records Management Policy
- Enterprise Record Retention Schedule
- Corporate Security Programs Organization's Data Protection Standard
- Corporate Backup Data Retention and Media Rotation Policy
- Legal Services (NDA and queries)

(Relevant to criteria P6.2, P6.3, P6.4, P6.5, P6.6)

To maintain consistency across the company and drive the appropriate protections for specific categories of data, Cisco Systems, Inc. has an enterprise-wide Common Data Taxonomy.

- Administrative Data
- Customer Data
- Entrusted Data
- Financing Data
- Telemetry Data
- Support Data
- Cisco Operations Data
- Cisco Strategic Data
- Human Resources Data

Consistent categorization of data allows Cisco to develop category-specific data protection requirements that reflect the company's obligations for such data. (Relevant to criteria P1.1, P1.2, P2.1, P3.1, P3.2, P4.1, P4.2, and P4.3)

Data Impact Analysis

Every product at Cisco undergoes a complete Data Impact Analysis, or DIA. This detailed and multiphase process can be summarized by the following mandatory initial questions:

- What data does your organization collect and or use?
- How is your data processed?
- Who accesses your data? Where is your data stored?
- What is the sensitivity, classification, and category of the PII data?
- What is the intended use for collecting this PII and are there other usages for it?
- What is the overall volume of this data, both traversing and in storage?
- What is the criticality of the underlying service or functions being performed by this application?

Cisco implements privacy criteria as a part of their Data Impact Assessment or DIA and as part of their Privacy Impact Assessment or PIA. Elements that are common in Cisco taxonomy and the *Trust Services Privacy Principle* include:

- Notice and communication of commitments and system requirements
- Notice to data subjects about privacy practices, commitments, and system requirements
- Choice and consent. Detail choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects
- Collection minimization
- Use, retention, and disposal; Cisco limits the use, retention, and enforces disposal of PII
- Access. Cisco provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments

Cisco WebEx Data Protection

Cisco WebEx LLC takes customer data protection seriously and it collects, uses, and processes customer information only in accordance with the *"Cisco Privacy Statement"*.
The Cisco WebEx LLC (SaaS) Terms of Service provides additional information:
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf
All data collected in Cisco WebEx Cloud Services is protected by several layers of security technologies and processes. Below are examples of controls placed in different layers of Cisco WebEx Cloud Services operations to protect customer data.

- **Physical access control** – Physical access is 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** – The Cisco WebEx Cloud Services network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco WebEx LLC data center is continuously monitored using an intrusion detection system (IDS). The Cisco WebEx Cloud Services 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, and databases, 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 also regularly reviewed for compliance. Cisco employees and contractors do not access customer data unless access is requested by the customer for support reasons

With the exception of CMR enabled devices, all data in-transit to and from the Cisco WebEx LLC data center to Cisco WebEx Services clients is encrypted. Additionally, in accordance with Cisco Systems, Inc. Cryptographic Key Management standard, passwords are encrypted.

Overview of Privacy Assessment

Cisco's offerings (clouds, products) and IT applications must meet customer and regulatory requirements regarding the processing of personal information. Cisco has developed a privacy impact assessment (PIA) process intended to:

- give relevant privacy guidance to development teams in an efficient and agile way that enables fast, informed decision-making
- flag potential privacy issues as early as possible in the development cycle

Scope of Privacy Assessment

The assessment process applies to all Cisco offerings and IT applications that collect, use, and distribute customer, employee, or 3rd party personal data. (Relevant to criteria P6.2, P6.3, P6.4, P6.5, P6.6)

Each assessment contains the following components:

- PIA - General Info - Provides basic information and whether or not personal information is collected, used or distributed
- PIA - Privacy Controls - Section that established what controls the Offering or Application provides to protect privacy data and meet additional regulations
- PIA - Privacy Data Inventory - Inventory of the privacy data elements, including appropriate metadata
- PIA - Supporting Documentation - Area provided to leave more information where necessary (2nd to last worksheet, after 3rd party worksheets)
- PIA - Assessment - Final worksheet completed by the Privacy Assessment team

Risk Management

CCTG is responsible for identifying the risks that threaten the achievement of the control objectives stated in the description of the system. Management owns risk. A governance committee comprised of representatives from Cisco WebEx LLC, Information Security and other business units meets quarterly to review risk.

CCTG management commissions an independent group within Cisco Security & Trust Organization to perform periodic risk assessments. The risk assessment allows management to identify risks in its areas of responsibility and implement appropriate measures to address those risks. Management commissions the independent group to reevaluate the risk assessment at least annually.
Annually risk assessments and internal audits are conducted for WebEx Cloud Services operations and each WebEx Data Center.

Risk Assessment Methodology

The overall steps of the risk assessment include:

- Plan the risk assessment
- Establish context
- Perform assessment including risk identification, risk analysis, and risk evaluation
- Risk treatment
- Risk acceptance
- Communicate and consult on risk
- Monitor and review

Risks are analyzed for their possible impact and likelihood yielding a level of risk determination and a corresponding acceptance criteria. Risks are assessed and evaluated both at the global level and the site-specific level.
Risk treatment, following the risk assessment, evaluates cost effective controls or measures. Management uses the following risk treatment options to assist in the decision making process of treating residual risks:

- Risk Modification (Mitigate) – The level of risk should be managed by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable
- Risk Retention (Accept) – The business unit decides to accept the potential risk and continue operating with the risk. This acceptance is a conscious business decision based on a number of factors such as the organization's culture, risk appetite, and potential opportunity loss
- Risk Avoidance (Terminate) – When the identified risk is considered too high or the cost of implementing treatment options exceeds the benefits, a decision may be made to avoid the risk completely by withdrawing from a planned or existing activity or set of activities or changing the conditions under which the activity is operated
- Risk Sharing (Transfer) – The risk may be treated by transferring the risk using options such as purchasing insurance to compensate for the loss incurred if the risk materializes

Using the above criteria, the risk assessment team combines the evaluated controls with the risk treatment options and provides a risk assessment report to management. (Relevant to criteria CC3.1, CC3.2, CC4.1, CC6.2)

Incident Management

Information Security Incident Management

Cisco WebEx LLC follows the Cisco Global Data Computer Security Incident Management Policy and the documented incident response and escalation process. The policy and process define which employees, contractors, and third-parties to contact in case of an incident or awareness of a security weakness. It also defines the systematic steps in which the Cisco Information Security Team responds to a security incident including, but is not limited to, the identification and validation of an incident, damage control or remediation, service restoration, evidence collection and preservation, contact with authorities, and post-mortem evaluations. (Relevant to criteria CC2.4, CC2.5, CC3.2, CC5.1, CC5.8, CC6.2)
The security incident management team is responsible for:

- Identifying and reporting suspicious activity
- Monitoring and handling incidents that originate from intrusion detection/prevention systems, and other perimeter monitoring devices
- Executing the Security Incident Response Management process
- Performing Incident Response Testing
- Performing Incident Response Training
- Notifying customers

Event Logging

Cisco has established a *Security Logging Standard* that defines the requirements for logging data at Cisco. This policy establishes requirements for event types, time synchronization, content and other key information. Logs are centralized for aggregation, correlation, continuity, and retention.

This policy and standard includes requirements for:

- Security event logging and log content
- Security event alerting, analysis and reporting (monitoring)
- Log continuity management
- Integrity and protection of log information
- Audit record retention

Incident Monitoring

Cisco has established the *Global Data and Computer Security Incident Management Policy* that defines the roles and responsibilities of management for handling suspected and actual data breach, data loss, and computer security incidents at Cisco. This policy establishes requirements and procedures for incident detection, reporting, and response. (Relevant to criteria CC1.2, CC2.2, CC2.3, CC2.4, CC3.2, CC5.8, CC7.4)

The Cisco WebEx Cloud Service network utilizes IDS to protect against malicious code. IDS sensors are placed at a strategic point or points within the network to monitor traffic within the boundary and matches the traffic based on a library of known attacks. Once an attack is identified, or abnormal behavior is sensed, an alert is sent to the CSIRT team for corrective action.

The Cisco Network IDS is automatically updated whenever new releases are available in accordance with organizational configuration management policy and procedures.

Cisco Network IDS is configured to automatically scan traffic. It also raises an alert in the event that malware is identified. Alerts are sent to CSIRT for investigation and remediation. (Relevant to criteria CC2.4, CC3.1, CC4.1, CC5.6, CC5.8, CC6.1, CC7.2)

Incident Response

Cisco WebEx LLC has established an incident response procedure defining actions when an event has been evaluated and is considered an incident.

The Cisco WebEx Cloud Service has developed and maintained an Incident Response Management procedure that includes information security requirements needed for incident responses. The recommended process includes:

- **Preparation** – actions to take in the event an incident occurs
- **Prevention** – Implementing practices to security networks, systems, and applications
- **Incident Detection and Analysis** – develop comprehensive procedures with step-by-step instructions for handling incidents
- **Incident Notification** – notifying appropriate individuals who need to be involved
- **Incident Containment, Eradication, and Recovery** – steps to take once an event is determined to be an incident
- **Post Incident Activity and Evidence Collection** – actions to meet regulator or contractual requirements; to identify and take corrective actions; to retain and provide evidence as needed
- **Incident Response Process Improvement** – identify opportunities to improve security measures, the incident handling process itself, reflect on new threats, and improved technology
- **Incident Response Metrics** – identify, capture, and measure metrics to gauge the effectiveness of the incident response capability

Communications of Incidents

Cisco WebEx LLC has established the external and internal incident reporting process to effectively provide all users a path for alerting the appropriate security incident response teams. The PSIRT is Cisco Systems, Inc. official interface with the public security vulnerabilities. The on-call Cisco Systems, Inc. PSIRT works 24 hours with company customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco WebEx Services.

Cisco WebEx Cloud Services Platform Controls

Information Security Management System

The CCTG has established and maintains formal policies, standards, and procedures to delineate the minimum standards relevant to the design and operations of controls over the Cisco WebEx Cloud Services platform. CCTG has an Information Security Management System (ISMS) designed to meet ISO/IEC 27001:2013 requirements implemented and operating on an annual cycle. Policies are reviewed and approved on a periodic basis, published on the company intranet, and communicated to CCTG employees and contractors. Organizational roles, responsibilities, and competency requirements affecting the security, confidentiality, and privacy of the services are defined and assigned by CCTG and communicated to the CCTG organization. In addition to the Cloud Security Team, which is a part of the Cisco Information Security organization (InfoSec), organizational segregation of duties includes key Cisco WebEx LLC functional teams responsible for the daily operations and maintenance, which includes monitoring the network, support, patching systems, hardware installations, and maintaining availability of the Cisco WebEx Cloud Services platform.
CCTG evaluates its organizational structure, reporting lines, authorities, and responsibilities for appropriate scope, competence, and position within the organization on an annual basis as part of its business planning process. CCTG monitors global regulatory requirements to ensure relevant statutory, regulatory, and contractual requirements are identified, documented, and kept up to date through regular interaction with legal, operations, and compliance business units. (Relevant to criteria C.8.2, C1.1, CC3.1, CC3.3, CC4.1)

Infrastructure and Platform Security

Platform security encompasses the security of the network, systems, and the overall data center within the Cisco WebEx Cloud Services. All systems undergo a security review and an acceptance validation prior to production deployment.

Firewalls protect the network perimeter and firewalls. Access control lists (ACLs) segregate the different security zones. There are daily internal and external security scans of Cisco WebEx Cloud Services. All systems are hardened and patched as part of the regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

All access to network security and management tools is in accordance with Cisco Systems, Inc. Access Management Policy and restricted only to authorized support personnel. (Relevant to criteria C1.2, CC3.2, CC5.6, CC5.7)

Access Management

Authorization from designated organization officials, including human resources is required before Cisco Systems, Inc. user is provided with a Cisco Corporate Intranet account as part of the employee onboarding process. This provides the user access to the Cisco Corporate Intranet including email.

Internal Users:

Internal users are Cisco WebEx employees or contractors having access to Cisco WebEx production system. Internal users needing privileged access to Cisco WebEx Cloud Services must request access. The request to create, modify, or delete a privileged user account must come from the user themselves, the employee's HR designated manager or supervisor. The requestor must submit a ticket through a sanctioned workflow management system.

Cisco WebEx Cloud Services manages access for internal users via established requirements for administrative access to data and systems (devices, applications, and services) and proper controls for authentication, authorization, and auditing.

Access is role-based; users are granted access via a functional security group. To gain access, an internal user must have a Cisco account and a management authorized ticket must be submitted for any privileged user access.

Termination procedure ensures that the user's credentials are disabled on the day and at the time of termination.

User access rights are reviewed at a minimum of four times annually during the formal RBAC review. This process confirms that managers have adequately modified rights based on role changes within the organization, confirms that no terminated credentials exist in access groups, and validates completeness in the HR termination and management notification procedures. Any issue found would be remediated immediately. Formal changes to roles include notice to appropriate management.

Cisco WebEx LLC internal users must use a Cisco Systems, Inc. issued laptop to access the Cisco Systems, Inc. corporate network and the Cisco WebEx Services environment. (Relevant to criteria CC5.1, CC5.2, CC5.3, CC5.4)

Cisco WebEx Services Site Administration:

After customer sign up, Cisco WebEx Services grants the customer permission for a site administrator.

Cisco WebEx Services requires an administrator to manage the customer's Cisco WebEx site. It has created the site administrator role to fulfill this function. The customer is required to designate and register a site administrator who is then granted privilege to access the Cisco

WebEx Cloud Services portal and manage the customer's site. The customer is responsible authenticating and authorizing the site administrator. (Relevant to criteria CC 5.2 and CC 5.4) The site administrator is responsible for managing the customer's account, enforcing the customer's own policies, and enforcing Cisco WebEx LLC policies and end user agreements. The site administrator creates user accounts and sets user privilege in accordance with the customer's policies and practices. In addition, the site administrator manages the security configuration for their site. (Relevant to criteria P5.1, CC5.1, CC5.2, CC5.3, CC5.4)

Change Management

The Cisco WebEx Cloud Services Team manages all aspects of changes to Cisco WebEx Cloud Services. This includes that each change is tested, approved, and reviewed to assure continued function in accordance with platform specifications. (Relevant to criteria CC2.1, CC2.2, CC7.4) Change requests are logged, categorized, and prioritized according to a formal change management process. Responsibilities are assigned to ensure the proper segregation of duties for the initiation, review, approval, and implementation of change requests. In cases of emergency, any deviation from standard procedures is reviewed by appropriate levels of management, logged, implemented, and subsequently reviewed, and approved. Emergency change is evaluated as a part of the CAB (change advisory board).

New approved systems or enhancements are forwarded to the Cisco WebEx Cloud Services operations team for migration into production.

Change approval process is restricted to a workflow management system. Only authenticated and authorized users can respond to approval requests. Review of a planned change includes examination of the MOP (method of procedure). The MOP includes the install plan, work details, verification, back-out, and post-implementation review procedures. Engineering will not implement a production change until all approvals are registered in the system. The new systems or enhancements are tested in a pre-production environment and are released in phases to production. Additionally, all changes include a back-out plan. If changes do not meet the agreed quality checks, the engineer will roll back the change. A failed change is required to restart the approval process.

All migration is monitored and issues are escalated up through the various level of technical support. A team of infrastructure engineers and technical operations personnel is assembled to troubleshoot the issue. At the point when change is scheduled, notifications to the end-users inform stakeholders of planned system downtime and any potential impacts due to the change. Cisco WebEx uses policy-enforced maintenance windows to restrict changes in the production environment to a defined timeframe. All changes to the production environment that are outside of the maintenance window require emergency change escalation and approval. (Relevant to criteria CC7.3, CC7.4)

Configuration Management

Cisco WebEx Cloud Services utilizes secure baseline configurations on systems and servers. The baseline configuration is based upon the most current Center for Internet Security (CIS) Benchmark and represents the organization's minimum-security baseline for the technology specific secure installation and configuration of systems, a.k.a., the "hardened image". These hardened images follow the general rule of least functionality where ports, services, and default accounts are only used if required. Recorded as the annual baseline, these configuration plans are formally reviewed and approved as part of annual policy and procedure review.

In situations where the secure host baseline requires an out of cycle configuration change, updated hardened images are pushed to the production environment and undergo routine change management procedures. Operating systems, key components, and network devices are evaluated periodically to ensure conformance with the configuration baseline. Out-of-conformance items are identified, and the item is re-provisioned. (Relevant to criteria CC2.1, CC2.2, CC7.4, CC7.3)

Secure Design

Cryptography – Encryption at Run Time

All communications between Cisco WebEx Services applications and Cisco WebEx Cloud Services occur over encrypted channels. Cisco WebEx Cloud Services supports the Transport Layer Security (TLS) 1.0, TLS 1.1, and TLS 1.2 protocols and uses high-strength ciphers (for example, Advanced Encryption Standard (AES) 256). The Minimum Encryption standard and TLS Certificate standard are reviewed annually to ensure the highest appropriate ciphers
After a meeting is established over TLS, all media streams (audio Voice over Internet Protocol (VOIP), video, screen share, and document share) are encrypted. User Datagram Protocol (UDP) is the preferred protocol for transmitting media. In UDP, media packets are encrypted using AES 128. The initial key exchange happens on a TLS-secured channel. Additionally, each datagram uses hashed- based message authentication code (HMAC) for authentication and integrity.
Media streams flowing from a client to Cisco WebEx Cloud Services servers are decrypted after they cross the firewalls inside the Cisco WebEx Data Center systems. (Relevant to criteria C1.1, CC3.2, CC7.1, CC7.2)

Data Center Security

Cisco WebEx Cloud Services uses switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the globe. The entire infrastructure within the Cisco WebEx Cloud Services is built with industry-standard enterprise security.
Additionally, Cisco WebEx Cloud Services operates network point-of- presence (iPoP) locations that facilitate backbone connections, Internet peering, global site backup, and caching technologies to enhance performance and availability for end users.
Cisco WebEx LLC owns and manages data centers in Mountain View, California and in Richardson and Allen, TX. All other data centers are owned and operated by other external third party owned hosting provider companies.
Cisco WebEx LLC monitors the effectiveness of internal control at the external third party owned data centers through regular internal and external audits and risk assessments of data center hosting operations and other procedures. (Relevant to criteria CC3.2, CC5.5)
Cisco Systems, Inc. has established standards and requirements to prevent unauthorized physical access, compromise, theft, or damage information processing facilities and to protect equipment and people against man-made or natural environmental hazards.
Annually, during the risk assessments and annual audit of each data center, ISO 270001 certifications and SOC2 Type II attestation reports are required to complete supplier management activities.

The Cisco WebEx Cloud Services data centers in-scope for this report:

Cisco-owned Data Center

- Mountain View, CA SJC02
- Richardson, TX, USA DFW01
- Allen, TX, USA DFW02

Colocation iPOP Data Centers

- San Jose, CA, USA (Equinix) SJC03
- Sydney, Australia (Equinix) SYD10
- Amsterdam, The Netherlands (Equinix) AMS10
- New York, USA (Telx) JFK10
- Chicago, USA (Telx) ORD10
- Los Angeles, CA, USA (CoreSite) LAX10
- Hong Kong (Pacnet) HKG10
- Dallas, TX, USA (Equinix) DFW10

Colocation Data Centers

- Ashburn, VA, USA (Equinix) IAD02
- Ashburn, VA, USA (Equinix) IAD03
- Tokyo, Japan (Equinix) NRT02
- Toronto, Canada (Equinix) YYZ01
- Singapore (Equinix) SIN01
- London 5, UK (Telehouse) LHR03
- Bangalore, India (Airtel) BLR03
- Almere, The Netherlands (Getronics) AMS01
- Tokyo, Japan (Equinix) NRT03
- Beijing, China (21ViaNet) PEK02

Physical security applies equally to Cisco WebEx LLC hosted facilities and any other external hosting provider.

Physical security at the data center includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco WebEx LLC data centers, access is controlled through a combination of badge readers and biometric controls. Within the data centers are also "trust zones," or segmented access to equipment based on infrastructure sensitivity. For example, databases are "caged", the network infrastructure has dedicated rooms, and locked racks. Only Cisco WebEx LLC security personnel and authorized visitors accompanied by Cisco WebEx LLC personnel can enter the data centers. (Relevant to criteria CC3.2, CC5.5)

Business Continuity Management

Cisco WebEx LLC has a formal business continuity plan (BCP) in place. The BCP establishes a process for responding to a catastrophic event. In some cases, the BCP can be relied upon in response to extended disruption of service as laid out in Cisco Systems, Inc. incident response plan (see also, Incident Response). The BCP describes the objectives, assumptions, responsibilities, and actions to be performed in such an event. The plan identifies teams, contacts, responsibilities, and action plans. Planning for the BCP begins with Business Impact Analysis (BIA). The plan is distributed to the Business Functional Team members, Functional Event Program Coordinator, the BCP Champion and Owner and any BCP Team Leads. (Relevant to criteria C1.4 and A1.1-A1.3, however Availability Criteria controls are not selected for the scope of this report.)

Global Site Backup Overview

The WebEx Global Site Backup (GSB) system ensures that you experience business continuation even in a disaster situation. Additional benefits include full redundancy for maintenance windows or other system outages. GSB provides each customer with a backup WebEx site. The GSB system provides real-time, two-way database data synchronization between the primary site and the backup site. All customers are supported with GSB.

A WebEx backup site is a separate site from the primary site. WebEx hosts the backup site on a different system and at a separate geographic location from the primary site.

Automatic Redirection

The GSB system automatically redirects you to your backup site in the event of the entire meeting system failure. If you started a meeting on your primary site and your primary site fails due to a whole system failure, you are automatically routed to the same scheduled meeting on your backup site.

- More information can be found at: https://collaborationhelp.cisco.com/article/en-us/31k2xo

Incident Management

Cisco WebEx LLC employs multiple technologies, procedures, and teams to ensure the secure operation of the Cisco WebEx Cloud Services platform, including:

- Leveraged monitoring systems and diagnostic procedures to manage incident resolution during business-impacting events. Staff operators provide 24-hour coverage to detect incidents and to manage the impact and resolution.

Cisco WebEx LLC has implemented key operational metrics and alarms across the production network using a variety of automated monitoring systems to detect outages, service latency, security incidents, and other unusual or unauthorized activities and conditions. Alarms are configured to notify operational and management personnel when warning thresholds indicating potential service latency, server unavailability, or other factors affecting availability and functionality are breeched. Personnel are on-call at all times to ensure that alarms are responded to in a timely manner.

Incidents and threshold warnings are logged in the incident tracking system. They are assigned a priority level and ownership and tracked through to appropriate resolution. (Relevant to criteria CC2.4, CC2.5, CC3.2, CC5.1, CC5.8, CC6.2)

Vulnerability Management

A vulnerability management program, managed by the InfoSec Cloud Security team, is in place to assess vulnerabilities in the Cisco WebEx Cloud Services environment. Assessments are performed on an on-going basis using a vulnerability scanner and penetration testing.

Beginning with an accurate inventory of all assets, vulnerability management process employs a vulnerability scanning tool to verify the security of the information system and applications. The WebEx infrastructure undergoes additional scheduled penetration testing. All vulnerabilities found using the scanner and penetration testing are entered into the vulnerability repository where they are evaluated (triaged) and categorized based on severity and their common vulnerability scoring system (CVSS) score and (false positives are eliminated). Vulnerabilities are assigned to the responsible team for remediation with a resolution date. After remediation is complete, the Cisco WebEx Cloud Services environment is scanned to verify that the issue has been resolved.

Penetration Testing (PenTest)

PenTests aim at finding security issues by using same tools and techniques as an attacker and are used to help secure products and services. A PenTest is defined as a legal and authorized attempt to find and successfully exploit systems, products, and services for the purpose of making them secure. PenTest goes a step beyond vulnerability assessment by stimulating hacker activity and delivering a live payload. Proof of Concept (PoC) attacks demonstrate that the capability to exploit is real.

Network PenTests are performed annually. Additionally, component based PenTests of Cisco WebEx Services occurs quarterly. All results from PenTests are analyzed for improvements in our Incident Management process.

End of Document