NCSC Cloud Security Principles: Webex Meetings

Building confidence that cloud services handle data in line with customer expectations is an important step in moving to a cloud first[1] world. To help customers in this task, the NCSC published a framework which is centred on 14 cloud security principles. Each principle captures a different aspect of security as it relates to cloud services. The principles serve both consumers and suppliers in providing a framework to articulate important security capabilities in a consistent and structured fashion.

This document provides details of how the Cisco Webex Meetings service meets each of the 14 cloud security principles. The document includes the NCSC description of each principle, along with its intended goals before then providing details of how it is met by the Webex Meetings service. Where applicable, each principle is accompanied by a cross-reference to applicable controls from the Cloud Computing Compliance Controls Catalogue (C5).

[1] https://www.gov.uk/guidance/government-cloud-first-policy

Independent Assurance

In addition to complying with our stringent internal standards, Cisco Webex also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Webex maintains the following industry standard certifications:

- ISO/IEC 27001:2013, 27017:2015, and 27018:2019
- Service Organization Controls (SOC) 2 Type II
- FedRAMP certified (visit cisco.com/go/fedramp for more details, scope, and availability) Note: FedRAMP certified Webex service is only available to U.S government and education customers
- Cloud Computing Compliance Controls Catalogue (C5)
- Privacy Shield Framework

Customer Responsibilities

Cisco services are designed with the assumption that certain policies, procedures, and controls are implemented by its customers. In certain situations, the application of specific policies, procedures, and controls by the customer is necessary to achieve certain control objectives. Customers that use Cisco Webex should maintain sufficient controls to provide reasonable assurance of the following:

- Customers are responsible for complying with the Cisco Acceptable Use Policy.
- Customers are responsible for performing patches to their software and third-party software.
- Customers are responsible for the security compliance and governance of their user accounts, account settings, and other information within their environment.
- Customers are responsible for user generated content and personably identifiable information they share with other parties.
- Customers are responsible for establishing password configurations settings and authentication requirements that meet their company, industry, and regulatory requirements.
- Customers are responsible for authorization of the related privileges meetings. The roles are host, alternate host, presenter, panelist, attendee, and site administrator.
- Site Administrators are responsible for managing the customer's account, enforcing the customer's own policies, and enforcing Cisco Webex policies and end user agreements.
- Customers are responsible for verifying attachments or links before opening them, being aware of the sensitivity of the content you wish to share and being aware of whether the meeting is recorded.
- Customers should incorporate appropriate protection against web application vulnerabilities on all public facing services, using methods such as input validations, parameterisation, tokens, stored procedures, or escaping the input before data is processed.
- Customers are responsible for installing and configuring antivirus software and network firewalls for systems that interface with Cisco Webex systems.
- Customers are responsible for using secure network protocols (i.e. TLS and SSH) for all of their connections and communications to their applications and integrations.

- Customers are responsible performing security testing, such as penetration and vulnerability testing, of their systems, applications, integrations and bots.
- Customers are responsible for ensuring appropriate logging for events such as administrator activity, system errors, authentication checks, data deletions etc. is in place to support monitoring, and incident response processes.
- Customers (Controller) are responsible for personal data collected by Cisco (Processor).

Principle 1 - Data in Transit Protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

This should be achieved through a combination of:

- **Network protection** - denying your attacker the ability to intercept data.
- **Encryption** - denying your attacker the ability to read data.

Goals

- Data in transit is protected between your end user device(s) and the service.
- Data in transit is protected internally within the service.
- Data in transit is protected between the service and other services (e.g. where APIs are exposed).

Cisco Response

All communications between Cisco Webex applications and Cisco Webex Cloud occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol with high strength cipher suites. The current list of offered cipher suites is included in the Cisco Webex Meetings Security Whitepaper.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted. Cisco Webex supports optional end-to-end encryption. When configured, the Cisco Webex service does not have access to the encryption keys used by meeting participants and cannot decrypt the media streams.

Encrypted media can be transported over UDP, TCP or TLS, User Datagram Protocol (UDP) is the preferred transport protocol for media. Media packets are encrypted using either AES 128 or AES 256. Webex video devices and 3rd party video devices that support media encryption with SRTP use AES-GCM-128-HMAC-SHA1. Webex applications use AES-GCM-256. The initial key exchange occurs over a TLS-secured channel.

C5 Control Mapping

KRY-01 to KRY-04

Principle 2 - Asset Protection and Resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

Physical location and legal jurisdiction

In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.

You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of user data could result in legal and regulatory sanction, or reputational damage.

Goals

You should understand:

- In which countries your data will be stored, processed and managed. You should also consider how this affects your compliance with relevant legislation e.g. Data Protection Act (DPA).
- Whether the legal jurisdiction(s) within which the service provider operates are acceptable to you.

Cisco Response

The Webex Meetings service leverages its own data centres which are located across the globe. The exact locations are outlined in the Webex Meetings Privacy Data Sheet. User-generated information (as defined below) is stored in the data centre provided during the ordering process. Billing and Webex analytics data is stored in the United States. User-generated information is defined as:

- Meeting and Call Recordings
- Transcriptions of Call Recordings
- Uploaded Files (for Webex Events and Training only)

Cisco's global privacy program and policies have been approved by the Dutch, Polish, Spanish, and other relevant European privacy regulators as providing adequate safeguards for the protection of privacy, fundamental rights, and freedoms of individuals for transfers of personal information protected under European law. Cisco's Binding Corporate Rules – Controller (BCR-C) – provide that transfers made by Cisco worldwide of European personal information benefit from adequate safeguards.

Additional details can be found in the Cisco Webex Meetings Privacy data sheet.

C5 Control Mapping

COM-01, RB-03

Data Centre Security

Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.

Goals

You should be confident that the physical security measures employed by the provider are sufficient for your intended use of the service.

Cisco Response

Physical security at the data centre includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco data centres, access is controlled through a combination of badge readers and biometric controls. In addition, environmental controls (for example, temperature sensors and fire-suppression systems) and service continuity infrastructure (for example, power backup) help ensure that systems run without interruption.

Within the data centres, there 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 racks are locked. Only Cisco security personnel and authorised visitors accompanied by Cisco personnel can enter the data centres.

C5 Control Mapping

PS-01 to PS-05, BCM-05

Data at Rest Protection

To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it’s held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.

Goals

You should have sufficient confidence that storage media containing your data are protected from unauthorised access.

Cisco Response

Within the Webex Meetings platform, all user passwords are stored using SHA-2 with salts. Other passwords such as for meetings or recordings are also encrypted at rest.

Network Based Recordings are encrypted at both the file and logical volume level. The file key is 256-bit block AES GCM. This file key is then encrypted with a master key based on AES HMAC-SHA256 which is rotated based on policy and saved to a database. Cisco maintains these keys for the customer.

C5 Control Mapping

KRY-03, RB-23

Data Sanitisation

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.

Inadequate sanitisation of data could result in:

- your data being retained by the service provider indefinitely.
- your data being accessible to other users of the service as resources are reused.
- your data being lost or disclosed on discarded, lost or stolen media.

Goals

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.

Cisco Response

Cisco maintains a robust media handling and data destruction policy. Flash memory is sanitised (securely erased) and hard disk drives are degaussed. Where hardware can be reused, hard drives are wiped, degaussed, reformatted and a request is submitted to the logistics team and approved by the manager to put the asset back in service. Where hardware cannot be reused, it is destroyed. Cisco processes align to the NIST 800-88 standard.

C5 Control Mapping

AM-06 and AM-07, PI-05

Equipment Disposal

Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.

Goals

Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.

Cisco Response

All production media is tracked and monitored regularly with management review through the Data Centre Infrastructure Management tool which identifies asset type, serial number, rack location, etc. An internal ticket must be submitted to and approved by the Data Centre Operations Manager before the data centre asset can be disposed. Retired servers and the like are sanitised / degaussed and then physically destroyed. A certificate of disposal is provided by an e-waste vendor ensuring all hardware was destroyed.

C5 Control Mapping

AM-06 and AM-07, PI-05

Physical Resilience and Availability

Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.

Goals

You should be sufficiently confident that the availability commitments of the service, including their ability to recover from outages, meets your business needs.

Cisco Response

The Cisco Webex Meetings service environment consists of server clusters to manage shared computing resources over the network. The Cisco data centres' global site backups and high-availability design enables the geographic failover of the Cisco Webex Meetings services. There are no single points of failure in the platform. There are geographically diverse failover clusters that can immediately resume the duties of primary clusters to prevent any discontinuity of service.

Cisco Webex has a live service status portal published at https://status.webex.com which provides an overview of the various Webex components and their respective service status. It also includes details of upcoming maintenance activities and their corresponding impact to customer experience. Webex offers service level guarantees but these are dependent on contractual agreements.

C5 Control Mapping

BCM-01 to BCM-05, RB-01, RB-02, RB-06 to RB-09

Principle 3 – Separation Between Users

A malicious or compromised user of the service should not be able to affect the service or data of another.

Goals

You:

- Understand the types of user you share the service or platform with.
- Have confidence that the service provides sufficient separation of your data and service from other users of the service.
- Have confidence that management of your service is kept separate from other users (covered separately as part of Principle 9).

Cisco Response

Individual tenants are logically separated based on organisational ID. Additional compensating controls include the use of encryption and separated identity / access management (each customer domain in the multi-tenant environment is a unique instance, with a separate identity store, access control, & encryption keys).

C5 Control Mapping

RB-23

Principle 4 - Governance Framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats.

Goals

You should have sufficient confidence that the service has a governance framework and processes which are appropriate for your intended use.

Cisco Response

Cisco Webex Meetings is ISO/IEC 27001:2013, 27017:2015, and 27018:2019 certified, and has SOC2 Type II and Cloud Computing Compliance Controls Catalogue (C5) attestations.

Cisco Management, in conjunction with the groups it creates, is responsible for creating, maintaining and monitoring the polices, 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 unauthorised use and disposition. Compliance with Cisco policies and standards is required and verified. Leading the priority and focus on security is the Collaboration Governance Committee (GC). The GC is comprised of Cisco Webex security and product leaders. The GC is accountable for the overall governance framework, planning, directing and controlling the security and risk aspects of business operations. The GC assigns roles and responsibilities to provide oversight to confirm adequate resourcing, efficiency of operation and separation of duties. The key roles and responsibilities of the committee are:

- **Chief Security Office (CSO)** - Accountable to the information security for Cisco Webex.
- **Cisco Collaboration Security and Privacy team** – responsible to the Cisco Collaboration business units to oversee and support their adherence to security and privacy business standards, secure service development and secure service operations. As part of this responsibility they

provide oversight and support for internal and external audits, and any required compliance governance – including our Information Security Management Systems (ISMS). While this group is dedicated to the Collaboration business units, they are part of and work hand in hand with the overall Cisco Security & Trust Organisation.

- **Cisco Collaboration Security Compliance and Assurance team** - Delegated responsibility for facilitating governance of Cisco Webex products within the Cisco Collaboration Security organisation. This team is responsible for the maintenance of the Information Security Management System (ISMS)
- **Cisco Webex product leadership team** - Responsible for the implementation and execution of security processes and procedures.

C5 Control Mapping

OIS-01 to OIS-07, SA-01 to SA-03, SPN-01 to SPN-03

Principle 5 - Operational Security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

Configuration and Change Management

You should have an accurate picture of the assets which make up the service, along with their configurations and dependencies.

Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected.

Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.

Goals

You should have confidence that:

- The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime.
- Changes to the service are assessed for potential security impact. Then managed and tracked through to completion.

Cisco Response

Cisco Webex Meetings SaaS Operations Centre (SOC) manages changes to the Webex platform. This includes that each change is tested, approved, and reviewed to assure the continued function in accordance with platform specifications. Change requests are logged, categorised and prioritised according to a formal change management process. Responsibilities are assigned to help ensure the proper segregation of duties for the initiation, review, approval and implementation of change requests. New approved systems or enhancements are submitted to the Webex Meetings SOC for migration into production. The change approval process is restricted to a workflow management system. Only authenticated and authorised users can respond to approval requests.

C5 Control Mapping

AM-01 to AM-05, BEI-03 to BEI-12, RB-12

Vulnerability Management

Service providers should have a management processes in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.

Goals

You should have confidence that:

- Potential new threats, vulnerabilities or exploitation techniques which could affect your service are assessed and corrective action is taken.
- Relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored by the service provider.
- The severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations.
- Using a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed.
- You know service provider timescales for implementing mitigations and are happy with them.

Cisco Response

A security assessment program is in place to assess vulnerabilities in the Cisco Webex Meetings environment. Assessments are performed using vulnerability scanning and penetration testing. Vulnerability scanning finds vulnerabilities of the infrastructure and platform using automated tools. Scanning within the Webex platform is performed on an on-going basis. Penetration testing is performed annually by a third party. Results of these tests are made available upon request. Component-based penetration tests occur when there are significant changes. All vulnerabilities found using scanning or from penetration testing are entered into a repository where they are evaluated and categorised based on severity (e.g. by making use of Common Vulnerability Scoring System). False positives are identified and eliminated and the remaining issues are assigned to the responsible team for remediation with a target resolution date. After resolution is complete, the environment is retested to verify that the issue has been resolved.

C5 Control Mapping

RB-17, RB-18, RB-19, RB-21

Protective Monitoring

A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data.

Goals

You should have confidence that:

- The service generates adequate audit events to support effective identification of suspicious activity.
- These events are analysed to identify potential compromises or inappropriate use of your service.
- The service provider takes prompt and appropriate action to address incidents.

Cisco Response

Cisco has implemented key operational metrics and alarms across the Webex Meetings production network using a variety of automated monitoring systems to detect outages, service latency, security incidents and other unusual or unauthorised activities and events. Alarms are configured to notify operational and management personnel when warning thresholds are met, indicating potential service latency, server unavailability, or other factors affecting availability and functionality.

Cisco policy establishes the requirements for logging data, which includes requirements for event types, time synchronisation, content and other key information. Logs are centralised for aggregation, correlation, continuity and retention. When a potential problem is identified, a message is sent to the Platform team and Cisco CSIRT. The Cisco CSIRT team will track the issue until resolution.

C5 Control Mapping

RB-10, RB-13, RB-14, RB-15, RB-16

Incident Management

Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users.

These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.

Goals

You should have confidence that:

- Incident management processes are in place for the service and are actively deployed in response to security incidents.
- Pre-defined processes are in place for responding to common types of incident and attack.
- A defined process and contact route exists for reporting of security incidents by consumers and external entities.
- Security incidents of relevance to you will be reported in acceptable timescales and formats.

Cisco Response

Cisco has an established Computer Security Incident Response Team (CSIRT) that provides proactive threat analysis, incident detection, and coordinated incident response. CSIRT coordinates and investigates policy violations, unauthorized access to Cisco assets, malicious code related incidents, and other security incidents.

The CSIRT Incident Response Handbook establishes incident management procedures for collecting incident data; enabling efficient recovery from security incidents; preventing or minimizing disruption of critical computing services; minimizing the loss of proprietary and confidential information; and facilitating cooperation and information exchange among cross-functional groups that are responsible for security incident remediation. Cisco follows procedures for handling evidence through legally admissible court standards including chain of custody and documentation.

The Cisco Product Security Incident Response Team (PSIRT) manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Cisco customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks.

PSIRT receives reports about Cisco products security issues from many sources: industry, customers, engineers, product developers, hackers. Cisco has a confidential case system and an assessment CVSS that is used to rate the risk. The higher the score, the more risk the vulnerability. Cisco uses a 1- 10 scale. The further away the damage can be done to a device, the higher the score.

The Cisco Security Centre details the process for reporting security incidents.

C5 Control Mapping

RB-19, RB-20, SIM-01 to SIM-07

Principle 6 - Personnel Security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles.

Goals

You should be confident that:

- The level of security screening conducted on service provider staff with access to your information, or with ability to affect your service, is appropriate.
- The minimum number of people necessary have access to your information or could affect your service.

Cisco Response

Cisco human resource policies apply to all Cisco permanent, temporary and contract personnel. Personnel management requirements include background checks, Code of Business Conduct review, and education and training. Background checks are conducted on anyone who requires badge access to Cisco facilities, intranet access or any access to Cisco's confidential, proprietary or intellectual data. These checks are applied to both Cisco employees and non-employees (e.g., temporary workers, contractors, consultants). Cisco complies with all applicable laws including fair employment practices and equal employment opportunity, when conducting background checks.

Employees that require privileged access to Webex Meetings must formally request access. Access requests are submitted through an internal ticket management system and must be accompanied by a proper business justification. Access is role-based; users are granted access via a functional security group. User access rights are reviewed at a minimum of four times annually during the formal RBAC review. The process confirms that managers have adequately modified rights based on role changes within the organisation, confirms that no terminated credentials exist in the access groups.

C5 Control Mapping

HR-01 to HR-05

Principle 7 - Secure Development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

Goals

You should be confident that:

- New and evolving threats are reviewed and the service improved in line with them.
- Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.

- Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Cisco Response

Cisco Webex products are 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 defence-in-depth and provides a holistic approach to product resilient. CSDL is a process to ensure Cisco develops cloud solutions that adhere to the Cisco and industry security standards. CSDL compliance is calculated based on information provided by product teams. It is measured based upon compliance to Product Security Baseline (PSB) requirements and is monitored over time. Compliance with CSDL cannot be waived. One of the PSB indicates the need to build a threat model that take into consideration various threats and how to protect against them. Specifically for cloud products, CSDL for Cloud requires a Cloud Approval to Operate (CATO). 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 PSB requirements are implemented and attainment of the CATO approval to operate is achieved. The third phase is the governance and maintenance of the CATO on an annual basis. CSDL conforms with the guidelines of ISO 27034.

C5 Control Mapping

BEI-01 to BEI-12

Principle 8 - Supply Chain Security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

Cloud services often rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Goals

You understand and accept:

- How your information is shared with, or accessible to, third party suppliers and their supply chains.
- How the service provider's procurement processes place security requirements on third party suppliers.
- How the service provider manages security risks from third party suppliers.
- How the service provider manages the conformance of their suppliers with security requirements.
- How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

Cisco Response

Cisco's Supplier Management Program begins with the corporate controls governing the procurement organisation. Suppliers enter into an agreement which covers supplier duties, services, licensing and intellectual property rights, confidentiality, integrity, availability and privacy. Suppliers are required to report information security events. Agreements include security and data protection requirements and Service Level Agreements.

After complying with the corporate procurement process, Cisco products' key suppliers are subject to annual reviews. These cover the handling of non-public information, legal review, budget for the previous and next year, the security of the system, external certifications and pertinent organisational structure reviews if they will affect the stability of the vendor.

If a supplier is a Cloud Service Provider, the supplier is evaluated by Cisco's third-party security assessment program. This program is the CASPR/CASPRX (Cloud and Application Service Provider Remediation) process. CASPR/CASPRX assessments evaluate the security risks to Cisco from use of a supplier's product or service and provide recommendations. The benefits include validation of the supplier's security architecture for compliance with Cisco policies and standards, a proactive and predictable process, and the protection of Cisco data and brand.

The list of Cisco Webex Meetings third-party suppliers that process customer personal data can be found in the Cisco Webex Meetings privacy data sheet.

C5 Control Mapping

DLL-01 and DLL-02

Principle 9 - Secure User Management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

Authentication of users to management interfaces and support channels

In order to maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.

These activities may be conducted through a service management web portal, or through other channels, such as telephone or email. They are likely to include such functions as provisioning new service elements, managing user accounts and managing consumer data.

Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data.

Goals

You should have sufficient confidence that:

- You are aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone phone, web portal, email etc.).
- Only authorised individuals from your organisation can use those mechanisms to affect your use of the service (Principle 10 can help you consider the strength of user identification and authentication in each of these mechanisms).

Cisco Response

Cisco Webex supports the use of Single Sign-On (SSO) using the SAML 2.0 protocol for authenticating users (both privileged users and 'regular' users) to the service. This protocol allows integration with third-party identity solutions such as Duo, PingFederate, OpenAM or Microsoft Active Director Federation Services. In addition to SSO via SAML, WebEx administrators can set a range of options for standard user passwords such as password aging, complexity, password blacklists etc.

Webex support is delivered via the Cisco Technical Assistance Centre (TAC). Support cases can be raised with TAC via the Cisco.com website, e-mail, chat or telephone. When a case is raised, the customer must have a valid support contract in place. General support and guidance will be provided to any member of the supported organisation but any support associated with administrative level issues will be limited to named site administrators. Support for the Webex Meetings service is all available online.

C5 Control Mapping

IDM-08

Separation and access control within management interfaces

Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another.

Your privileged administrative accounts probably have access to large volumes of data. Constraining the permissions of individual users to those absolutely necessary can help to limit the damage caused by malicious users, compromised credentials or compromised devices.

Role-based access control provides a mechanism to achieve this and is likely to be a particularly important capability for users managing larger deployments.

Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to one of these networks. Guidance on assessing the risks of exposing interfaces to different types of networks is provided under Principle 11.

Goals

You should:

- have confidence that other users cannot access, modify or otherwise affect your service management
- manage the risks of privileged access using a system such as the 'principle of least privilege'
- understand how management interfaces are protected (see Principle 11) and what functionality they expose

Cisco Response

Cisco Webex implements role-based access control which is built around five distinct roles; Host, Alternate Host, Presenter, Panellist, Attendee and Site Administrator. The user assigned to the 'Site Administrator' role creates user accounts and sets the user privileges in accordance with the organisation's policies and practices. In addition, the site administrator manages the security configuration for their site. Webex supports federated authentication for user Single Sign-On (SSO) using the SAML 2.0 protocol. SAML 2.0 enables integration into the customer's identity solution such as Microsoft Active Directory Federation Services, PingFederate and OpenAM. Multi-factor user authentication can be enabled through the use of SAML. Webex site administrators can carry out the following actions:

- Lock out an account after a configurable number of failed login attempts
- Automatically unlock a locked-out account after a specified time interval
- Deactivate accounts after a defined period of inactivity
- Require a user to change the password at the next login
- Lock or unlock a user account
- Activate or deactivate a user account
- Require security text on new account requests
- Require email confirmation of new accounts
- Allow self-registration (sign-up) for new accounts
- Configure rules for self-registration of new accounts
- Set a security option to automatically end a meeting if there is only one participant present
- Display caller ID for dial-in users when available

Full details of a range of site administration tasks can be found at https://help.webex.com/ld-nwespu1-CiscoWebexControlHub/Control-Hub

C5 Control Mapping

IDM-01, IDM-03, IDM-05, IDM-06. IDM-08, IDM-10 to IDM-12. KOS-02, KOS-03

Principle 10 – Identity and Authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service.

Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.

Goals

You should have confidence that identity and authentication controls ensure users are authorised to access specific interfaces.

Cisco Response

Webex Meetings supports both basic username and password authentication or federated authentication integration for SSO using SAML 2.0. Through this mechanisms, Webex Meetings can leverage existing customer identity management platforms, removing the burden of users having to maintain multiple identities. In addition, through this integration, multi-factor authentication solutions can also be used to remove the reliance on single-factor passwords. Detailed configuration guidance for a number of popular identity providers (IdPs) is provided at https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Cisco-Webex-Control-Hub

Principle 11 - External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant.

You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk.

Goals

You:

- understand what physical and logical interfaces your information is available from, and how access to your data is controlled
- have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10)

Cisco Response

The Webex Meetings service is accessed via the Internet using either a web browser or dedicated Webex Meetings application. Platform security encompasses the security of the network, systems, and the overall data centre within the Cisco Webex Cloud. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening, security patching, and vulnerability scanning and assessment.

Servers are hardened using the Security Technical Implementation Guidelines (STIGs) published by the National Institute of Standards and Technology (NIST). Firewalls protect the network perimeter and firewalls. Access Control Lists (ACLs) segregate the different security zones. Intrusion Detection Systems (IDSs) are in place, and activities are logged and monitored on a continuous basis. Daily internal and external security scans are conducted of Cisco Webex Cloud. All systems are hardened and patched as part of the regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

C5 Control Mapping

KOS-02 to KOS-06

Principle 12 - Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers.

Goals

You should:

- understand which service administration model is being used by the service provider to manage the service
- be content with any risks the service administration model in use brings to your data or use of the service

Cisco Response

Cisco Webex Meetings employs a 'service administration via bastion hosts' model, as defined by the NCSC. All administrative access to the Webex Meetings platform must be performed using a Cisco issued laptop with a Cisco IT approved operating system. The laptop must comply with Cisco IT Trusted Device Standard which includes mandatory endpoint anti-malware protection, data-at-rest protection and mobile device management.

C5 Control Mapping

IDM-05, IDM-08, KOS-04, RB-05, RB-15, RB-23

Principle 13 – Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

Goals

You should be:

- aware of the audit information that will be provided to you, how and when it will be made available, the format of the data, and the retention period associated with it
- confident that the audit information available will meet your needs for investigating misuse or incidents

Cisco Response

Webex Meetings captures a range of data related to the operation of the service within its native management console. Troubleshooting data associated with the quality of experience of Webex Meetings is included as well as a detailed audit trail of administrative changes applied to customers Webex Meetings site. Audit logs are retained for a minimum of 90 days which is extended to 12 months if the Pro Pack has been purchased. Webex audit logs can be exported in CSV format.

Principle 14 – Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

The extent of your responsibility will vary depending on the deployment models of the cloud service, and the scenario in which you intend to use the service. Specific features of individual services may also have bearing. For example, how a content delivery network protects your private key, or how a cloud payment provider detects fraudulent transactions, are important security considerations over and above the general considerations covered by the cloud security principles.

With IaaS and PaaS offerings, you are responsible for significant aspects of the security of your data and workloads. For example, if you procure an IaaS compute instance, you will normally be responsible for installing a modern operating system, configuring that operating system securely, securely deploying any applications and also maintaining that instance through applying patches or performing maintenance required.

Goals

You:

- understand any service configuration options available to you and the security implications of your choices
- understand the security requirements of your use of the service
- educate your staff using and managing the service in how to do so safely and securely

Cisco Response

Cisco Webex Meetings provides a range of security configuration options which are under the control and responsibility of the customer site administrator. To support customers to make informed decisions, Cisco maintains a set of best practices for both meeting hosts and site administrators. Many other guides are available at https://help.webex.com/en-us/ and include guidance and training materials for administrators and end-users.

References and Additional Sources of Evidence

There are a number of sources of additional evidence available including:

(Available from the Cisco Trust Portal)

- Cisco Webex Meetings Privacy Data Sheet
- Cisco Webex Meetings Privacy Data Map
- Cisco Webex Meetings and Teams SOC 2 Type II and C5 Report
- Cisco Webex Meetings and Teams ISO27001:2013 Certificate
- Cisco Webex Meetings Letter of Attestation (Penetration test results)

Available on Cisco.com

- Cisco Webex Meetings Security Whitepaper
- End-to-End Encryption Configuration Guide
- Webex Meetings Best Practices for Secure Meetings: Site Administration
- Webex Meetings Best Practices for Secure Meetings: Hosts
- Cisco Webex Help Center