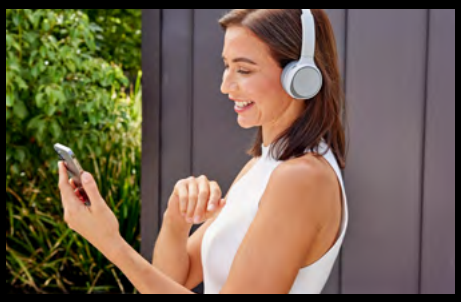
Solution Brief

webex by CISCO

Webex completes IRAP assessment to the ‘PROTECTED’ level

IRAP, the Infosec Registered Assessors Program, is a program instituted by the Australian government to ensure that information and communications technology including cloud services is high quality and compliant for industries and government agencies. IRAP assessors examine integrity, confidentiality, and data availability of cloud services.



Integrity

Webex uses various authentication methods to validate each user, making sure that only intended parties receive the information.

Confidentiality

All Webex traffic in transit and at rest is encrypted end-to-end making data unreadable by anyone not authorized, even if it is stolen.

Availability of data

Data centres in Melbourne and Sydney are protected 24/7 through physical and software monitoring and controls.

67,500

cybercrimes reported to the the Australian Cyber Security Centre

13%

increase in cybercrime from 2020 to 2021

Protecting valuable information is more necessary than ever before

Cybercrime is a severe problem around the world. Cyber criminals are making threats and attacks in all areas of our digital ecosystem. Many countries have instituted regulations to protect citizens, governments, and businesses from these attacks. Australia has created guidelines and assessments for protecting information and mitigating security risks to empower everyone to connect online safely and confidently. IRAP assessors review technologies and services to assure compliance with Australia's cyber security standards. Their intent is to maximize the security of government data when it is communicated, processed, and stored.

Webex completed the IRAP assessment

Webex by Cisco is a Cloud Service Provider (CSP) and has been verified as compliant with the Australian Cyber Security Centre's (ACSC) Information Security Manual (ISM).

The IRAP Assessment covered the Webex Suite of services which includes the following:

- Webex App
- Webex Messaging
- Webex Calling (Multitenant)
- Webex Control Hub
- Webex Calling (Dedicated Instance)
- Webex For Developers
- Webex Meetings

The certifications that Webex has attained and are relevant to the assessment include:

- Soc 2 type 2
- ISO/IEC 27001:2013

$33B

losses from cybercrime in Australia

68%

of Australian consumers encountered a tech support scam over the past 12 months

For the assessment, IRAP assessors examined the security and privacy processes, controls, and physical operations of Webex data centres. The examinations included assessments of intrusion detection, encryption processes, cross-domain and network security, access control, and information security risk management of the Webex services. The assessors concluded that Webex complies with requirements in the Australia government information security manual up to the applicable PROTECTED level controls. The Webex architecture and components and controls are inherently secure and protect information.

Webex implements security throughout the platform

One of the most important aspects of Webex is that we integrate security and privacy from the earliest stages of development, making sure it is built in by design, not bolted on after the fact. Our design teams start with security for every feature. And each feature is continually tested for possible breaches or intrusion from external sources.

Authentication

Authentication of users is done by various methods enabling only approved users into any meeting or conversation. Multifactor authentication, Single sign on, and Zero Trust authentication can be used for Webex collaboration. With Zero Trust Security, Cisco has established an open, standard based form of end-to-end encryption with Cisco independent identity verification (Whitepaper). The process by which users or meeting attendees are allowed to participate and receive information is called authentication. Users must verify who they are and that they are the intended recipient before receiving the communication

25%

of Australians who engaged with cyber criminals had money stolen

Updating all software and systems is one of the best ways to prevent cybercrime.

Encryption

Webex's end-to-end encryption is the most comprehensive available. With end-to-end encrypted options for meetings, meeting participants generate and exchange their own keys, and Cisco or anyone else cannot access their meeting content. In addition, customers can manage their own messaging keys in the cloud or hold them on premises. Encoding of data is necessary to prevent stolen information from being understood. Encryption allows only intended parties the ability to decode and understand the information being sent.

Data Loss Prevention

You can protect meetings and messaging data using near real-time DLP (Data Loss Prevention) with options that will redact or delete unintended messages, files, transcripts, and recordings and notify users or administrators of any violation. Or you can take advantage of real-time DLP for messaging that allows files to be scanned and deleted before they are received by others. Webex is the only collaboration solution that enables customers to use their existing DLP tools and policies for meetings, recordings, and transcripts. Webex supports a full range of DLP solutions from many vendors.

External Enforcement

Webex enforces compliance policies that you decide for your organization. These policies are persistent if your users are collaborating internally or externally. Other collaboration systems have no way to enforce compliance rules when collaborating with external users. The external user's compliance rules would have to comply with your company rules when they are collaborating and there is no method to verify this. A key differentiator for Webex is the ability to monitor information that is shared in spaces created by people in other organizations, providing a seamless but secure external collaboration experience.

Backing up files is the best way to protect against Malware and Ransomware

Mobile Security

No matter which device you are using, mobile content created in Webex is encrypted end to end – even the cached content. Our built-in native Mobile Device Management (MDM) capabilities ensure secure access for your devices. MDM keeps personal apps separate from your organization's business apps. It also removes the business apps when someone leaves the organization, or a device is stolen.

The ACSC recommends using Multi-factor Authentication to authorize user accounts

Webex is committed to keep your data close

With data centres in Melbourne and Sydney, Webex provides some processing and storage of user generated content within Australia. Although this does not guarantee complete privacy, it reduces the risk of foreign intervention. For this reason, more organizations are requiring data to be stored within their country giving local access and adherence to local regulations.

For Cisco, security is more than a compliance obligation, it is a business imperative. We have established long-standing security, data protection, and privacy programs. As connectivity and technology become even more foundational to people's economic, social, and cultural lives, Cisco's commitment to protect our customers is stronger than ever and we will keep advancing our security and privacy measures in this constantly evolving world. Cisco remains intently committed to complying with governments' security measures and assuring the delivery of a user-friendly security platform for all users, all devices, and all applications.

For more information
Please visit Secure Collaboration

September 2022