

# Create a Private Content Network That Is IRAP Compliant With Kiteworks

Be Compliant When Communicating With, Between, and Within Australian Government Agencies

The Infosec Registered Assessors Program (IRAP), which is overseen by the Australian Cyber Security Centre (ACSC), helps protect Australian federal and state agencies against supply chain cyberattacks that can have far-reaching and malicious impact. Australian government agencies must use technologies that are IRAP assessed to ensure that sensitive data is protected and access to it is continuously tracked and controlled. At the same time, third parties like contractors, vendors, and suppliers conducting business with Australian government agencies must use technology solutions that have been assessed by independent IRAP assessors.

## Why Private Businesses Need IRAP-compliant Solutions

IRAP compliance demonstrates that people, processes, and technology in over 800 risk areas meet data privacy controls. If contractors, vendors, and suppliers rely on technology solutions that are not assessed to IRAP controls and standards, they must find alternative solutions that are IRAP compliant. Doing so can waste valuable time and resources, create complexities, and impede sales and delivery cycles. Solutions that can be IRAP assessed include ICT systems, cloud services, gateways, FedLink, and Gatekeeper Public Key Infrastructure Framework. Potential businesses affected by IRAP compliance include legal firms, business consultants, defense contractors, financial firms, retailers, and software and hardware suppliers, among others.

## Why Australian Government Agencies Need IRAP-compliant Solutions

The goal of IRAP is to maximize the security of data belonging to and shared with Australian federal, state, and local governments. IRAP delineates the governance controls for cloud services to assess security controls within their platforms and authorizes third-party assessors to provide independent assessments of information and communications infrastructure, suggest mitigations, and highlight risks. Australian government agencies must use IRAP-compliant solutions for sharing and transferring data within their individual agencies, between agencies, and with external third parties. This helps protect the integrity of the software supply chain for each agency within the Australian government.

**“Using Kiteworks and other IRAP-compliant solutions makes it easier for us to do business with Australian government agencies, as it provides assurance that the platform has appropriate and effective controls and that it has been validated independently against Australian government policies and guidelines.”**

**– Sunil Saale, Head of Cyber and Information Security, MinterEllison**

## FACT SHEET

### Create a Private Content Network That Is IRAP Compliant With Kiteworks

## What IRAP Means

IRAP compliance is achieved when a technology provider undergoes an in-depth assessment of their people, processes, and technology by a certified independent assessor. An IRAP assessment consists of two stages of audit. The first identifies security deficiencies while the second audit assesses residual compliance. When a solution is assessed to IRAP PROTECTED level, this means that data governance classifications and protections have been confirmed by the assessor to be in place and that the respective technology is approved for use in the supply chain for Australian federal, state, and local agencies—whether directly by government agencies themselves or by third parties communicating sensitive content with those agencies.

## What Is the IRAP-compliant Kiteworks Platform

With the Kiteworks platform, which is IRAP assessed to PROTECTED level data classification and delivers single-tenant hosting and geographic sovereignty of data governance, Australian government agencies and private sector companies conducting business with those agencies have a private content network (PCN). This PCN ensures that Australian government agencies and third parties communicating data with them are the only entities able to access their data—namely, there is no intermingling of data, metadata, or shared application resources. Powering the PCN is Kiteworks Secure Cloud Hosting With Premium Support that includes patching and update services, named service representatives, enhanced service-level agreements (SLAs), and other high-touch services.

## Schedule a Custom Demo Today

Schedule a custom demo of Kiteworks today to see how you can deploy a PCN and how the IRAP-compliant platform unifies, tracks, controls, and secures content moving into, within, and out of organizations: [info.kiteworks.com/demo-request](https://info.kiteworks.com/demo-request)

# Kiteworks

Copyright © 2022 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.