Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports CPS234 Compliance of the Australian Prudential Regulation Authority

A Comprehensive Solution for Protecting Sensitive Digital Assets to Enhance Compliance and Security

CPS234 is an Australian regulation by the Australian Prudential Regulation Authority (APRA) since July 1, 2019, to strengthen the resilience of APRA-regulated entities (banks, insurance, superannuation funds) against cyber threats. It mandates these entities to implement cyberattack protection measures. IRAP is an Australian Cyber Security Centre program providing assurance to the government that its ICT systems are secure. CPS234 and IRAP are separate programs, but APRA-regulated entities can use IRAP assessments to demonstrate compliance with CPS234. Both programs aim to improve information security in Australia. Kiteworks directly supports an organisation's ability to be compliant in their sensitive file and email data that are communicated internally and externally. Here's how:

Establish Access Control Policies and Asset Management

To become an APRA-regulated entity, an organisation must have clearly defined information security-related roles and responsibilities of the board, senior management, governing bodies, and individuals. Kiteworks supports compliance by enabling admins to set up granular controls to protect sensitive content based on roles and responsibilities to enforce compliance policies. Access control can be further managed within compliance with geofencing, app enablement, file type filtering, and email forwarding control. This enables business owners to easily manage content, folders, invitations, and access controls to ensure CPS234 compliance of all content.

Maintain Security and Enable Operations With Flexible Deployment

Regulations require organisations to maintain an information security capability commensurate with the size and extent of threats to their information assets. Kiteworks supports this mandate by offering valuable flexible deployment options for organisations with varying budgets. Kiteworks' platform is flexible and supports on-premises, private cloud, hybrid, hosted, and even FedRAMP private cloud deployment options tailored to specific requirements. The platform's ability to find the perfect balance between privacy, compliance, scalability, and costs minimizes security vulnerabilities and reduces maintenance costs.

Protect Content and Ensure Regular Testing

Organisations must implement controls to protect their information assets commensurate with the criticality and sensitivity of those information assets and undertake systematic testing and assurance regarding the effectiveness of those controls. Kiteworks supports compliance by providing organisations the ability to increase control and governance over their sensitive digital assets. By unifying security for third-party communications, including email, file sharing, mobile, managed file transfer, and SFTP, Kiteworks provides centralized governance and protection of sensitive digital assets, making it an ideal solution for organisations handling sensitive email and file data that requires strict security controls to prevent unauthorized access, disclosure, or modification. Plus, Kiteworks enforces a strict secure software development life cycle including extensive security code reviews, regular penetration testing, and a bounty program to keep data protected.

An embedded network firewall and WAF, zero-trust access, and minimized attack surface all work to significantly reduce security risk. Kiteworks also manages one-click updates for customers that have been tested for compatibility of the patch with other system components, allowing timely patches to the operating system, databases, and open-source libraries.

Report Security Incidents Efficiently

Additionally, organisations must notify the APRA of material information security incidents. Kiteworks supports this mandate with anomaly detection that allows for immediate insight into unauthorized access. AI technology detects suspicious events, such as possible exfiltration, and sends an alert via email and audit logs. Through the platform's immutable audit logs, organisations can trust that attacks are detected sooner and maintain the correct chain of evidence to perform forensics. This enables efficient mandatory reporting of any data violations to the APRA in a timely manner.

Kiteworks enables organisations to establish access control policies and asset management, maintain security and enable operations with flexible deployment, protect content, and ensure regular testing, as well as report security incidents efficiently. Kiteworks provides granular controls to protect sensitive content based on roles and responsibilities, offers flexible deployment options, unifies security for third-party communications, and includes AI technology for anomaly detection. It also enforces a secure software development life cycle and provides immutable audit logs for efficient mandatory reporting.