Kiteworks

GUIDE

CMMC 2.0 Compliance Mapping for Sensitive Data Exchanges

Introduction to CMMC

The U.S. Department of Defense (DoD) takes a supply-chain risk-management approach to improving cybersecurity by requiring all third-party partners to obtain the Cybersecurity Maturity Model Certification (CMMC). The CMMC is designed to ensure the protection of sensitive national security information such as Controlled Unclassified Information (CUI) and Federal Contract information (FCI). The certification applies to all DoD contractors and subcontractors, and a contractor that fails to maintain compliance will be unable to bid for DoD contracts.

Under DFARS and DoD rules and policies, the DoD implemented cybersecurity controls in the CMMC standard to protect CUI and FCI. Thus, the CMMC measures an organization's ability to protect FCI and CUI. FCI is information not intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government. CUI is information that requires safeguarding or dissemination controls according to and consistent with federal laws, regulations, and government-wide policies.

CMMC 2.0

CMMC 2.0 is the updated and comprehensive framework to protect the defense industrial base from frequent and complex cyberattacks. This streamlined version was released in late 2021 to focus on the most critical security and compliance requirements. It reduced compliance levels from five to three, and third-party assessments are only required for Level 2 and 3 partners that manage critical national security information. The model aligns with the widely accepted Federal Information Processing Standards (FIPS) 200 security-related areas and the National Institute of Standards & Technology (NIST) SP 800-171 and 800-172 control families.

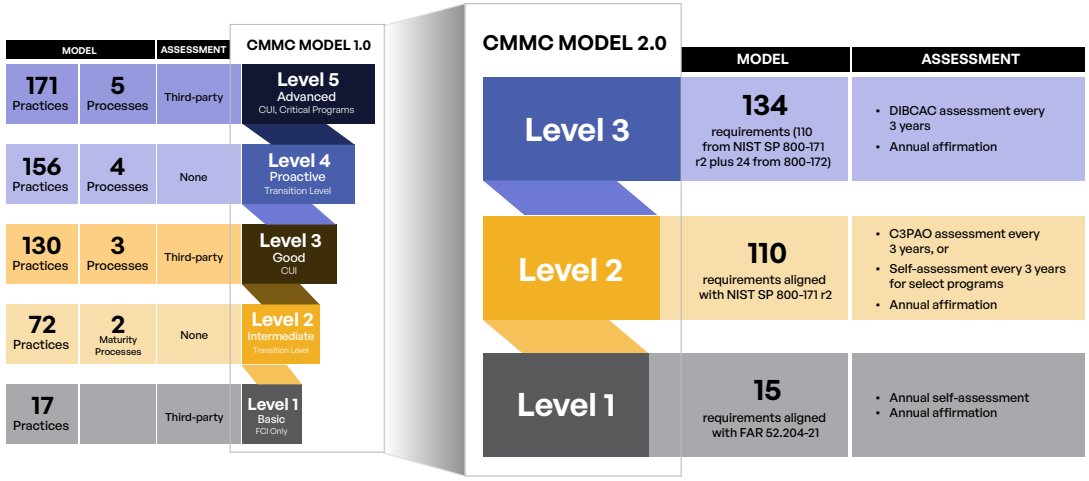

Figure 1. Comparison of CMMC 1.0 and 2.0.

The Kiteworks Platform

Kiteworks' FedRAMP- and FIPS-140-3-compliant platform for privacy and compliance governance enables organizations to send, share, receive, and store sensitive data. Integrating communication channels such as secure email, file sharing, file transfer, managed file transfer, web forms, and application programming interfaces (APIs), the Kiteworks platform creates Private Data Networks that track, control, and secure confidential digital communications while unifying visibility and metadata. Capabilities in the Kiteworks platform include:

Secure Email

Kiteworks locks down private email communications and ensures regulatory compliance. Users simply send emails and attachments from any location or device, and the Kiteworks platform automatically protects them.

Secure File Sharing

Kiteworks enables government employees and federal contractors to access and share CUI securely, reducing the risk of data breaches, malware attacks, and data loss.

Managed File Transfer

Government agencies and businesses transferring confidential files can streamline, automate, and secure large-scale file transfers and establish policy controls to prevent compliance violations.

Web Forms

Government agency employees and contractors and third-party business users can upload sensitive information that is governed by privacy and compliance policies.

Application Programming Interfaces (APIs)

Organizations can develop custom data applications and integrations on the Kiteworks platform that enable them to manage the risk of data breaches and compliance violations.

The following analysis of CMMC 2.0 reveals that Kiteworks supports nearly 90% of CMMC 2.0 Level 2 requirements out of the box (see Appendix).

For contractors and subcontractors doing business with the U.S. DoD, this translates into dramatically faster compliance audits and even expanded revenue opportunities. Further, once CMMC 2.0 goes into effect, businesses unable to demonstrate sensitive data exchange compliance with CMMC 2.0 cannot compete for and work on DoD projects.

Access Control

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 AC.L1-3.1.1	Authorized Access Control [CUI Data]	Limit information system access to authorized users, processes acting on behalf of authorize users, and devices (including other systems)	Yes, supports compliance	The Kiteworks platform enforces strict access controls to protect all data, including CUI. It supports multiple authentication methods such as credential-based authentication, certificate-based authentication, multi-factor authentication (MFA), SAML 2.0 Single Sign-On (SSO), Kerberos SSO, OAuth, LDAP/Microsoft Active Directory integration, Azure Active Directory (Azure AD), and locally managed users and credentials.
Level 1 AC.L1-3.1.2	Transaction and Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute	Yes, supports compliance	System administrators and data owners control access through detailed role-based permissions, assigning roles like Owner, Manager, Collaborator, Downloader, Viewer, or Uploader to files and folders, which limits users to the types of transactions and functions they are permitted to execute.
Level 1 AC.L1-3.1.20	External Connections [CUI Data]	Verify and control/limit connections to and use of external information systems	Yes, supports compliance	The Kiteworks platform provides controlled access to cloud enterprise content management systems like Google Drive, Box, Dropbox, Microsoft OneDrive, and Microsoft SharePoint Online.
Level 1 AC.L1-3.1.22	Control Public Information [CUI Data]	Control information posted or processed on publicly accessible information systems	Yes, supports compliance	The Kiteworks platform can be deployed as a private or hybrid cloud or as a private hosted deployment in an isolated environment or AWS, per FedRAMP requirements.
Level 2 AC.L2-3.1.3	Control CUI Flow	Control the flow of CUI in accordance with approved authorizations	Yes, supports compliance	Administrators and data owners control the flow of CUI using zero-trust data exchanges (attribute-based access controls). These policies enforce dynamic access controls based on data attributes (such as folder paths or sensitivity labels), user attributes (like domain or profile), and the actions being performed, ensuring CUI is handled according to approved authorizations.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AC.L2-3.1.4	Separation of Duties	Separate the duties of individuals to reduce the risk of malevolent activity without collusion	Yes, supports compliance	Administrators can define different roles and access levels for CUI, reducing the risk of collusion.
Level 2 AC.L2-3.1.5	Least Privilege	Employ the principle of least privilege, including for specific security functions and privileged accounts	Yes, supports compliance	The platform supports customizable admin roles with hierarchical permissions. By defining access policies based on roles, IP addresses, geographic locations, domains, and time-based restrictions, the platform enforces the principle of least privilege for both users and administrators.
Level 2 AC.L2-3.1.6	Non-Privileged Account Use	Use non-privileged accounts or roles when accessing non-security functions	Yes, supports compliance	The Kiteworks platform prevents non-privileged users from executing administrative functions. The platform also logs all access to security functions, enabling the execution of those functions to be audited.
Level 2 AC.L2-3.1.7	Privileged Functions	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs	Yes, supports compliance	The Kiteworks platform enables administrators to define different types of accounts and access privileges, ensuring that non-privileged users never access privileged data or controls. All administrative actions are captured in comprehensive audit logs, ensuring that any execution of privileged functions is tracked and supporting accountability and compliance requirements.
Level 2 AC.L2-3.1.8	Unsuccessful Logon Attempts	Limit unsuccessful logon attempts	Yes, supports compliance	The Kiteworks platform enables system administrators to set a limit for unsuccessful logon attempts. When that limit is reached, that account can be locked, and an alert sent to administrators and security professionals.
Level 2 AC.L2-3.1.9	Privacy and Security Notices	Provide privacy and security notices consistent with applicable CUI rules	Yes, supports compliance	The Kiteworks platform can be customized to display privacy and security notices required by an organization.
Level 2 AC.L2-3.1.10	Session Lock	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	Partially supports compliance	The Kiteworks platform locks sessions after a period of inactivity, though it does not use pattern-hiding displays.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AC.L2-3.1.11	Session Termination	Terminate (automatically) a user session after a defined condition	Yes, supports compliance	The Kiteworks platform enables system administrators to define policies that automatically log users out after a set amount of idle time. System administrators can monitor and manually terminate active sessions.
Level 2 AC.L2-3.1.12	Control Remote Access	Monitor and control remote access sessions	Yes, supports compliance	The Kiteworks platform monitors and logs all remote access to CUI. All remote access is governed through strict access control policies. System administrators can monitor and manually terminate active sessions.
Level 2 AC.L2-3.1.13	Remote Access Confidentiality	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions	Yes, supports compliance	The platform employs cryptographic mechanisms like TLS 1.3 and 1.2 to protect the confidentiality of remote access sessions. Data at rest is double-encrypted using AES-256 encryption at both the file and disk levels. Customers own their encryption keys, and the platform supports integration with Hardware Security Modules (HSMs) for key management, ensuring only authorized users can decrypt sensitive data.
Level 2 AC.L2-3.1.14	Remote Access Routing	Route remote access via managed access control points	Yes, supports compliance	The Kiteworks platform enables system administrators to control which nodes (servers) are available for client access (HTTPS or SFTP).
Level 2 AC.L2-3.1.15	Privileged Remote Access	Authorize remote execution of privileged commands and remote access to security-relevant information	Yes, supports compliance	The Kiteworks platform provides a separate administrative interface that requires authentication and provides its own IP access restrictions.
Level 2 AC.L2-3.1.16	Wireless Access Authorization	Authorize wireless access prior to allowing such connections	Out of scope	N/A
Level 2 AC.L2-3.1.17	Wireless Access Protection	Protect wireless access using authentication and encryption	Out of scope	N/A

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AC.L2-3.1.18	Mobile Device Connection	Control connection of mobile devices	Yes, supports compliance	The Kiteworks platform enables and disables access from the Kiteworks mobile app. System administrators can also manage and terminate user sessions. If a mobile device is lost or stolen, system administrators can perform a remote wipe of all CUI in the Kiteworks secure container on the device.
Level 2 AC.L2-3.1.19	Encrypt CUI on Mobile	Encrypt CUI on mobile devices and mobile computing platforms	Yes, supports compliance	The Kiteworks platform encrypts CUI at rest on mobile devices and mobile computing platforms. In addition, it stores CUI in a secure container, protecting CUI on a mobile device from unauthorized access, data corruption, and malware.
Level 2 AC.L2-3.1.21	Portable Storage Use	Limit use of portable storage devices on external systems	Out of scope	N/A

Awareness and Training

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AT.L2-3.2.1	Role-Based Risk Awareness	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems	Yes, supports compliance	Kiteworks FedRAMP operations managers and administration personnel are trained in the security risks and applicable policies, standards, and procedures related to the platform. The system warns customer admins of potentially risky settings, such as access controls that fail to follow the principle of least privilege.
Level 2 AT.L2-3.2.2	Role-Based Training	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities	Partially supports compliance	Kiteworks FedRAMP operations personnel are trained in the security risks and applicable policies, standards, and procedures related to the platform.
Level 2 AT.L2-3.2.3	Insider Threat Awareness	Provide security awareness training on recognizing and reporting potential indicators of insider threat	Partially supports compliance	Kiteworks FedRAMP operations personnel must regularly pass security awareness training.

Audit and Accountability

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AU.L2-3.3.1	System Auditing	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	Yes, supports compliance	Kiteworks provides comprehensive, detailed, and timely audit logs that capture all user and system activities without throttling. Logs include user authentication attempts, file access, sharing activities, and administrative actions. They can be exported to SIEM systems in real time via multiple syslog feeds.
Level 2 AU.L2-3.3.2	User Accountability	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions	Yes, supports compliance	The platform assigns unique user IDs and maintains detailed audit logs that ensure all actions can be uniquely traced to individual users. Activities such as authentication attempts, file access, edits, deletions, and sharing are recorded.
Level 2 AU.L2-3.3.3	Event Review	Review and update logged events	Yes, supports compliance	The logs can be reviewed but not updated or deleted.
Level 2 AU.L2-3.3.4	Audit Failure Alerting	Alert in the event of an audit logging process failure	Yes, supports compliance	The Kiteworks platform alerts administrators in the event of a logging process failure.
Level 2 AU.L2-3.3.5	Audit Correlation	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity	Yes, supports compliance	Kiteworks facilitates the correlation of audit records through consolidated and normalized logs, simplifying analysis. Integration with SIEM tools and built-in detection mechanisms support the investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 AU.L2-3.3.6	Reduction and Reporting	Provide audit record reduction and report generation to support on-demand analysis and reporting	Yes, supports compliance	The Kiteworks platform provides comprehensive audit logs that can be exported to a SIEM system and analyzed in on-demand reports. Logs include data-specific audit record fields such as username, email addresses, IP address, file or folder names, and event type. Kiteworks also provides a CISO Dashboard, highlighting systems issues or interest to CISOs and other security stakeholders and providing an easily readable, visual presentation of activity and anomalous behavior.
Level 2 AU.L2-3.3.7	Authoritative Time Source	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records	Yes, supports compliance	The Kiteworks platform integrates with Network Time Protocol (NTP) servers to provide authoritative time stamps for audit records.
Level 2 AU.L2-3.3.8	Audit Protection	Protect audit information and audit logging tools from unauthorized access, modification, and deletion	Yes, supports compliance	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
Level 2 AU.L2-3.3.9	Audit Management	Limit management of audit logging functionality to a subset of privileged users	Yes, supports compliance	Logs in the Kiteworks platform are protected from editing and deletion.

Configuration Management

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 CM.L2-3.4.1	System Baselining	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles	Yes, supports compliance	The Kiteworks platform provides one-click compliance reports that can be used to track the baseline configuration of the Kiteworks system.
Level 2 CM.L2-3.4.2	Security Configuration Enforcement	Establish and enforce security configuration settings for information technology products employed in organizational systems	Yes, supports compliance	System administrators on the Kiteworks platform can configure security settings for the platform. Administrators can also configure security settings for users and their mobile devices when those users access CUI under the platform's management.
Level 2 CM.L2-3.4.3	System Change Management	Track, review, approve or disapprove, and log changes to organizational systems	Yes, supports compliance	The Kiteworks platform enables system administrators to track, review, and control all changes made to the platform.
Level 2 CM.L2-3.4.4	Security Impact Analysis	Analyze the security impact of changes prior to implementation	Yes, supports compliance	The Kiteworks platform provides compliance audits that report configuration changes that degrade security below recommended levels.
Level 2 CM.L2-3.4.5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems	Yes, supports compliance	The Kiteworks platform enforces and logs all logical access restrictions applied to CUI under management.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 CM.L2-3.4.6	Least Functionality	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities	Yes, supports compliance	The Kiteworks hardened appliance exposes only a few essential ports and services. The system provides no operating system access for users or administrators.
Level 2 CM.L2-3.4.7	Nonessential Functionality	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services	Yes, supports compliance	The Kiteworks platform ships as a hardened appliance with nonessential services disabled. All unused ports are blocked. We also provide the ability to enable/disable SFTP/SSH access.
Level 2 CM.L2-3.4.8	Application Execution Policy	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software	Yes, supports compliance	The Kiteworks platform enforces whitelisting of apps on mobile devices accessing the platform.
Level 2 CM.L2-3.4.9	User-installed Software	Control and monitor user-installed software	Yes, supports compliance	The Kiteworks platform allows you to control what plugins and apps are made available to the end-user. The platform also enforces mobile app whitelisting, preventing unauthorized third-party apps from accessing CUI.

Identification and Authentication

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 IA.L1-3.5.1	Identification [CUI Data]	Identify information system users, processes acting on behalf of users, or devices	Yes, supports compliance	The Kiteworks platform assigns individual users unique IDs and uses those IDs to track user activity on the platform across all devices.
Level 1 IA.L1-3.5.2	Authentication [CUI Data]	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems	Yes, supports compliance	Kiteworks assigns unique IDs to users and requires authentication before granting access. It supports various authentication methods, including credential-based, certificate-based, multi-factor authentication (MFA), SAML 2.0 SSO, Kerberos SSO, OAuth, LDAP/Active Directory integration, Azure AD, and time-based OTP authenticators.
Level 2 IA.L2-3.5.3	Multi-factor Authentication	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts	Yes, supports compliance	The platform supports and can enforce multi-factor authentication (MFA) for both privileged and non-privileged accounts using methods like RADIUS protocol, PIV/CAC cards, email-based OTP, SMS-based OTP, time-based OTP, and certificate-based authentication, enhancing security for all users.
Level 2 IA.L2-3.5.4	Replay-Resistant Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts	Yes, supports compliance	The Kiteworks platform can be configured to require multi-factor authentication for any administrative session. Multi-factor authentication is also enforced through one-time passcodes via email. Alternatively, multi-factor authentication is enforced through integration with third-party authentication solutions that support SMS-based passcodes or the RADIUS protocol. It can also be configured to time out those sessions after a threshold of idle time has been reached. This prevents old credential replay. Kiteworks also supports PIV/CAC cards, which use no credentials and are therefore not susceptible to replay.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 IA.L2-3.5.5	Identifier Reuse	Prevent reuse of identifiers for a defined period	Yes, supports compliance	The Kiteworks platform assigns each user a unique ID and tracks all activity on a per-user and per-file basis.
Level 2 IA.L2-3.5.6	Identifier Handling	Disable identifiers after a defined period of inactivity	Yes, supports compliance	The Kiteworks platform enables system administrators to set session timeout policies, disconnecting users after a defined period of inactivity. The platform can also remove end-user access altogether after a certain period of time if needed.
Level 2 IA.L2-3.5.7	Password Complexity	Enforce a minimum password complexity and change of characters when new passwords are created	Yes, supports compliance	The platform enables managers and system administrators to define password configuration requirements, including requirements for password complexity.
Level 2 IA.L2-3.5.8	Password Reuse	Prohibit password reuse for a specified number of generations	Yes, supports compliance	The Kiteworks platform can be configured to prohibit password reuse.
Level 2 IA.L2-3.5.9	Temporary Passwords	Allow temporary password use for system logons with an immediate change to a permanent password	Yes, supports compliance	The Kiteworks platform enables system administrators to reset user passwords and enforce password change upon next logon. Otherwise, users follow an account verification link or password reset link to set or reset their passwords.
Level 2 IA.L2-3.5.10	Cryptographically-Protected Passwords	Store and transmit only cryptographically protected passwords	Yes, supports compliance	The Kiteworks platform encrypts passwords in transit and at rest. Passwords at rest are stored as salted hashes. Passwords are never stored or transmitted insecurely.
Level 2 IA.L2-3.5.11	Obscure Feedback	Obscure feedback of authentication information	Yes, supports compliance	The Kiteworks platform transmits all authentication information using secure Transport Layer Security (TLS) connections. By default, passwords are not displayed in plain text on screens.

Incident Response

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 IR.L2-3.6.1	Incident Handling	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities	Partially supports compliance	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
Level 2 IR.L2-3.6.2	Incident Reporting	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization	Yes, supports compliance	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
Level 2 IR.L2-3.6.3	Incident Response Testing	Test the organizational incident response capability	Out of scope	N/A

Maintenance

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 MA.L2-3.7.1	Perform Maintenance	Perform maintenance on organizational systems	Yes, supports compliance	Kiteworks personnel perform maintenance on FedRAMP Kiteworks systems per documented and audited processes and procedures.
Level 2 MA.L2-3.7.2	System Maintenance Control	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance	Yes, supports compliance	Customer personnel can only perform maintenance using the secure, audited administrative user interface, and cannot obtain operating system access. For FedRAMP systems, the Kiteworks organization provides the controls on the tools, techniques, mechanism, and personnel as defined in the audited Kiteworks FedRAMP processes.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 MA.L2-3.7.3	Equipment Sanitation	Ensure equipment removed for offsite maintenance is sanitized of any CUI	Yes, supports compliance	The Kiteworks platform can perform a remote wipe of the secure containers on mobile devices that have been lost, stolen, or decommissioned.
Level 2 MA.L2-3.7.4	Media Inspection	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems	Yes, supports compliance	The Kiteworks platform scans CUI for viruses and other malware by default, using F-Secure Anti-Virus software. The platform integrates with Check Point SandBlast and APIs enable integration with other Advanced Threat Prevention technologies to scan CUI for advanced persistent threats and zero-day attacks.
Level 2 MA.L2-3.7.5	Nonlocal Maintenance	Require multi-factor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when non-local maintenance is complete	Yes, supports compliance	The Kiteworks platform can be configured to require multi-factor authentication for any administrative session. Multi-factor authentication is also enforced through one-time passcodes via email. Alternatively, multi-factor authentication is enforced through integration with third-party authentication solutions that support SMS-based passcodes or the RADIUS protocol. It can also be configured to time out those sessions after a threshold of idle time has been reached.
Level 2 MA.L2-3.7.6	Maintenance Personnel	Supervise the maintenance activities of maintenance personnel without required access authorization	Yes, supports compliance	The Kiteworks platform logs the activities of all users, including maintenance activities of users with varying degrees of privilege.

Media Protection

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 MP.L1-3.8.3	Media Disposal [CUI Data]	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse	Yes, supports compliance	The Kiteworks platform can perform a remote wipe of CUI in the secure containers on mobile devices that have been lost, stolen, or decommissioned.
Level 2 MP.L2-3.8.1	Media Protection	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital	Yes, supports compliance	Kiteworks FedRAMP systems encrypt all CUI when stored on media, and physical media is procedurally controlled and audited in data centers used by Kiteworks.
Level 2 MP.L2-3.8.2	Media Access	Limit access to CUI on system media to authorized users	Yes, supports compliance	The Kiteworks platform protects CUI by encrypting data and enforcing access controls.
Level 2 MP.L2-3.8.4	Media Markings	Mark media with necessary CUI markings and distribution limitations	Yes, supports compliance	Users can mark CUI in file and folder names, and in email subject lines. Kiteworks also automates policies based on Microsoft MIP sensitivity labels, which can be used to mark CUI.
Level 2 MP.L2-3.8.5	Media Accountability	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas	Yes, supports compliance	The Kiteworks platform enforces access controls on mobile devices regardless of their location.
Level 2 MP.L2-3.8.6	Portable Storage Encryption	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards	Yes, supports compliance	The Kiteworks platform encrypts all CUI at rest with AES-256 encryption.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 MP.L2-3.8.7	Removable Media	Control the use of removable media on system components	Out of scope	N/A
Level 2 MP.L2-3.8.8	Shared Media	Prohibit the use of portable storage devices when such devices have no identifiable owner	Out of scope	N/A
Level 2 MP.L2-3.8.9	Protect Backups	Protect the confidentiality of backup CUI at storage locations	Yes, supports compliance	Kiteworks protects the confidentiality of FedRAMP system backups per documented and audited procedures. All CUI is encrypted with a key owned by the customer.

Personnel Security

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 PS.L2-3.9.1	Screen Individuals	Screen individuals prior to authorizing access to organizational systems containing CUI	Yes, supports compliance	Kiteworks FedRAMP personnel are screened U.S. citizens.
Level 2 PS.L2-3.9.2	Personnel Actions	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	Yes, supports compliance	The Kiteworks platform protects CUI even when employees or contractors are terminated or transferred. CUI can be remotely wiped from mobile devices, and access to private- or public-cloud repositories can be blocked.

Physical Protection

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 PE.L1-3.10.1	Limit Physical Access [CUI Data]	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited procedures that limit physical access.
Level 1 PE.L1-3.10.3	Escort Visitors [CUI Data]	Escort visitors and monitor visitor activity	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited procedures that include escorting and monitoring of visitors.
Level 1 PE.L1-3.10.4	Access Logs [CUI Data]	Maintain audit logs of physical access	Yes, supports compliance	Kiteworks maintains audit logs of all physical access of FedRAMP systems.
Level 1 PE.L1-3.10.5	Manage Physical Access [CUI Data]	Control and manage physical access devices	Yes, supports compliance	Kiteworks FedRAMP systems are deployed and managed in controlled environments with strict, audited procedures that control card readers, access cards, and other access devices.
Level 2 PE.L2-3.10.2	Monitor Facility	Protect and monitor the physical facility and support infrastructure for organizational systems	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited protection and monitoring.
Level 2 PE.L2-3.10.6	Alternative Work Sites	Enforce safeguarding measures for CUI at alternate work sites	Yes, supports compliance	The Kiteworks platform protects CUI at all locations. Remote access to CUI is secured with authentication controls along with other best practices, including the use of secure containers on mobile devices and encryption of all CUI in transit and at rest.

Risk Assessment

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 RA.L2-3.11.1	Risk Assessments	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI	Out of scope	N/A
Level 2 RA.L2-3.11.2	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified	Yes, supports compliance	Kiteworks security engineers regularly scan the code base to discover new vulnerabilities.
Level 2 RA.L2-3.11.3	Vulnerability Remediation	Remediate vulnerabilities in accordance with risk assessments	Yes, supports compliance	Kiteworks security engineers prioritize and release fixes per a documented secure software development life cycle. Kiteworks products, whether hosted or deployed on the customer's premises, can detect the availability of new updates and apply them with a click. The Kiteworks organization offers updates as a service as part of the Premium Support package.

Security Assessment

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 CA.L2-3.12.1	Security Control Assessment	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-3 compliant, following all of the guidelines and reviews therein.
Level 2 CA.L2-3.12.2	Operational Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-3 compliant, following all of the guidelines and reviews therein.
Level 2 CA.L2-3.12.3	Security Control Monitoring	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls	Yes, supports compliance	Kiteworks FedRAMP security controls and incidents are audited yearly by the Third-Party Assessment Organization (3PAO).
Level 2 CA.L2-3.12.4	System Security Plan	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-3 compliant, following all of the guidelines and reviews therein.

System and Communications Protection

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 SC.L1-3.13.1	Boundary Protection [CUI Data]	Monitor, control, and protect organizational communications (i.e., Information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems	Yes, supports compliance	The platform monitors, controls, and protects communications at system boundaries using an embedded network firewall that blocks all unused ports and minimizes the attack surface. An embedded web application firewall (WAF) detects and blocks web and API attacks. IP address blocking mechanisms prevent unauthorized access after excessive failed login attempts. The platform employs a zero-trust architecture and enforces encryption in transit using TLS 1.3 and 1.2, ensuring the security of organizational communications.
Level 1 SC.L1-3.13.5	Public-Access System Separation [CUI Data]	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks	Yes, supports compliance	The Kiteworks platform tiered architecture allows web interfaces and other system functions to be deployed outside network DMZs for public access, while ensuring that application logic and CUI storage remain on internal networks.
Level 2 SC.L2-3.13.2	Security Engineering	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems	Yes, supports compliance	The Kiteworks platform has been designed and developed with information security in mind. The platform's tiered architecture separates functionality, improves scalability, and supports the enforcement of data sovereignty policies. The platform's source code is routinely analyzed for quality and security. The platform's availability on a private or hybrid cloud or as a private hosted deployment in an isolated environment on AWS enables customers to adopt the deployment model that best suits their security needs.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 SC.L2-3.13.3	Role Separation	Separate user functionality from system management functionality	Yes, supports compliance	The Kiteworks platform enforces security controls specific to user roles, including system administrators, CUI managers, and end-users. Unprivileged users never gain access to system management functionality. The Kiteworks platform prevents unauthorized access or sharing of CUI.
Level 2 SC.L2-3.13.4	Shared Resource Control	Prevent unauthorized and unintended information transfer via shared system resources	Yes, supports compliance	Only authorized users and processes can access and share CUI.
Level 2 SC.L2-3.13.6	Network Communication by Exception	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)	Yes, supports compliance	The Kiteworks platform supports the whitelisting and blacklisting of IP addresses and can be configured to deny network traffic by default.
Level 2 SC.L2-3.13.7	Split Tunneling	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling)	Out of scope	N/A
Level 2 SC.L2-3.13.8	Data in Transit	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards	Yes, supports compliance	The Kiteworks platform encrypts CUI in transit using Transport Layer Security. System administrators can configure the platform not to accept TLS 1.0 or 1.1 connections.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 SC.L2-3.13.9	Connections Termination	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity	Yes, supports compliance	The Kiteworks platform enables system administrators to set session timeout policies, disconnecting users after a defined period of inactivity.
Level 2 SC.L2-3.13.10	Key Management	Establish and manage cryptographic keys for cryptography employed in organizational systems	Yes, supports compliance	The Kiteworks platform uses keys to encrypt data in transit and at rest. Kiteworks customers have full ownership of their cryptographic keys. Keys can be managed directly within the Kiteworks platform or stored in a Hardware Security Module.
Level 2 SC.L2-3.13.11	CUI Encryption	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI	Yes, supports compliance	The Kiteworks platform is available in a FIPS 140-3 configuration.
Level 2 SC.L2-3.13.12	Collaborative Device Control	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device	Out of scope	N/A
Level 2 SC.L2-3.13.13	Mobile Code	Control and monitor the use of mobile code	Yes, supports compliance	Kiteworks uses secure coding practices and abides by OWASP Top 10 mitigation strategies. Our SDLC is rigorously reviewed and tested, as attested and verified through our SOC 2, FedRAMP, IRAP, and FIPS-140 certifications/audits.
Level 2 SC.L2-3.13.14	Voice over Internet Protocol	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies	Out of scope	N/A

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 SC.L2-3.13.15	Communications Authenticity	Protect the authenticity of communications sessions	Yes, supports compliance	The Kiteworks platform protects the authenticity of communications sessions in compliance with NIST 800-53, SC-23. Specifically, the platform invalidates session identifiers upon user logout or other session termination, generates a unique session identifier for each session with predefined randomness requirements, recognizes only session identifiers that are system generated, and uses only predefined certificate authorities for verification of the establishment of protected sessions.
Level 2 SC.L2-3.13.16	Data at Rest	Protect the confidentiality of CUI at rest	Yes, supports compliance	The Kiteworks platform protects the confidentiality of CUI at rest through the enforcement of strict access controls and the use of AES-256 encryption. In addition, CUI at rest on mobile devices is stored in a secure container that shields the CUI from access from other applications and processes.

System and Information Integrity

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 1 SI.L1-3.14.1	Flaw Remediation [CUI Data]	Identify, report, and correct information and information system flaws in a timely manner	Yes, supports compliance	Kiteworks monitors and reviews vulnerabilities in the Kiteworks platform and prioritizes and resolves these vulnerabilities based on impact and severity.
Level 1 SI.L1-3.14.2	Malicious Code Protection [CUI Data]	Provide protection from malicious code at appropriate locations within organizational information systems	Yes, supports compliance	The Kiteworks platform protects against malicious code by scanning CUI entering or exiting the platform for viruses, advanced persistent threats, and zero-day attacks. On mobile devices, Kiteworks stores CUI in secure containers (protected areas of storage and memory) that shield CUI from malware infection.
Level 1 SI.L1-3.14.4	Update Malicious Code Protection	Update malicious code protection mechanisms when new releases are available	Yes, supports compliance	The Kiteworks platform automatically applies updates to integrated and embedded anti-malware solutions from F-Secure and Check Point.
Level 1 SI.L1-3.14.5	System & File Scanning [CUI Data]	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed	Yes, supports compliance	The Kiteworks platform scans all uploaded files for infections of malware and indications of zero-day threats. When integrated with a data loss prevention (DLP) service, the platform can also scan data and block or quarantine any CUI transmissions that might violate DLP policies.
Level 2 SI.L2-3.14.3	Security Alerts and Advisories	Monitor system security alerts and advisories and take action in response	Yes, supports compliance	The Kiteworks platform can be configured to export logs to SIEM systems being used for security monitoring and alerts.

CMMC 2.0	Name	Practice Description	Kiteworks Supports Compliance	Kiteworks Solution
Level 2 SI.L2-3.14.6	Monitor Communications for Attacks	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks	Yes, supports compliance	The Kiteworks platform monitors all communications under management for signs of malware and other security anomalies that could signal the presence of an attack.
Level 2 SI.L2-3.14.7	Identify Unauthorized Use	Identify unauthorized use of organizational systems	Yes, supports compliance	Kiteworks employs intrusion detection systems and anomaly detection mechanisms to identify unauthorized use of organizational systems. Comprehensive logging captures failed login attempts and other security-related events, while real-time notifications alert administrators to suspicious activities, enabling prompt response.

Appendix: Kiteworks Alignment With CMMC 2.0 Level 2 Practices

Practice Area	Kiteworks Compliant	Shared Responsibility	Out of Scope	Total
Access Control	18	1	3	22
Awareness and Training	1	2		3
Audit and Accountability	9			9
Configuration Management	9			9
Identification and Authentication	11			11
Incident Response	1	1	1	3
Maintenance	6			6
Media Protection	7		2	9
Personnel Security	2			2
Physical Protection	6			6
Risk Assessment	2		1	3
Security Assessment	4			4
System and Communications Protection	13		3	16
System and Information Integrity	7			7
Total	96	4	10	110

The information provided in this Guide does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this Guide are for general informational purposes only. Information in this Guide may not constitute the most up-to-date legal or other information. Add-on options are included in this Guide and are required to support compliance.