Kiteworks

COMPLIANCE GUIDE

Kiteworks' Guide to Defence Standard 05-138

Technical Compliance Requirements for Managing Sensitive Defence Information in UK Supply Chains

Introduction

Defence Standard 05-138 Issue 4, promulgated by the UK Ministry of Defence on 14 May 2024 (published on GOV.UK 23 May 2024), establishes comprehensive cyber security requirements for defence suppliers handling sensitive government data. This standard delineates the mandatory technical and organizational controls necessary to protect defence-related information throughout the supply chain. The standard is structured around four Objectives and four Cyber Risk Profiles (CRPs):

Objectives: A – Managing security risk; B – Protecting against cyber attack; C – Detecting cyber security events; D – Minimising the impact of cyber security incidents

Cyber Risk Profiles: Level 0 "Basic" (3 controls); Level 1 "Foundational" (101 controls); Level 2 "Advanced" (139 controls); Level 3 "Expert" (144 controls)

Defence Standard 05-138 is built on the UK government's Cyber Essentials scheme as its universal baseline: Control 0001 (Cyber Essentials certification) applies at every risk level, while Control 0002 (Cyber Essentials Plus certification) is additionally required for suppliers operating at Level 2 (Advanced) and Level 3 (Expert). Kiteworks holds Cyber Essentials Plus certification, meaning it has already met the independent technical verification standard required of the highest-risk defence suppliers under DEF STAN 05-138. The standard applies to all suppliers, subcontractors, and third parties where DEFCON 658 is incorporated into the relevant MOD contract. Applicability and the depth of controls required are scaled by the Cyber Risk Profile (Level 0–3) assigned by the MOD delivery team — not by the classification of the data handled. The standard's scope is the supplier's overarching corporate or enterprise environment; it does not address MOD data classification, which is governed separately. Three controls apply universally at every risk level: Cyber Essentials certification (Control 0001), UK GDPR compliance (Control 2314), and resilient networks and systems (Control 2500). Controls described in this guide such as board-level governance, automated asset inventories, and data loss prevention apply at Levels 2 and 3 only; the applicable depth of requirements is determined by the Cyber Risk Profile assigned to each contract.

Defence Standard 05-138 mandates suppliers implement robust technical measures including multi-factor authentication for critical systems, encryption for data at rest and in transit, monthly vulnerability scanning, and continuous monitoring of security controls. Organizational requirements encompass board-level cyber security governance, periodic risk assessments, comprehensive asset inventories, and formal incident response procedures. Suppliers must maintain audit logs for minimum 12-month periods, conduct annual penetration testing, and implement data loss prevention controls.

The standard specifies strict identity management protocols, requiring automated mechanisms to support system-account management (Control 2209, applicable at Level 3), privileged access controls, and service account governance. Data protection obligations include encryption using nationally approved algorithms such as FIPS 140-2, secure key management through hardware security modules, and implementation of DMARC, DKIM, and SPF for email authentication. Cross-border data transfer restrictions on defence information may also apply under UK GDPR and contract-specific Security Aspects Letters, though these obligations are not part of Def Stan 05-138 Issue 4 itself.

Enforcement occurs through contractual obligations, with suppliers required to demonstrate compliance before contract award and throughout the contract life cycle. Noncompliance may result in contract termination and exclusion from future defence procurement opportunities. Serious breaches involving classified information may also carry legal consequences under UK law, including the Official Secrets Act, though this is not a consequence prescribed by Def Stan 05-138 itself. Note: Def Stan 05-138 Issue 4 does not itself prescribe a specific incident reporting timeline; that obligation flows from DEFCON 658, UK GDPR Article 33 (72 hours for personal data breaches), or the Security Aspects Letter specific to each contract. Suppliers must cooperate fully with Ministry of Defence investigations.

This guide showcases how Kiteworks can help organizations comply with specific sections of Defence Standard 05-138 to achieve data governance of their critical unstructured data.

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP Moderate Authorized (US Federal Cloud) and FIPS 140-3 Level 1 validated file sharing and governance platform enables organizations to share sensitive information quickly and securely while maintaining full visibility and control over their file-sharing activities. The Kiteworks platform provides:

Protection of Unstructured Data

Kiteworks provides comprehensive protection for unstructured data through its advanced firewall and zero-trust file sharing capabilities. The platform's double encryption at rest and TLS 1.3/1.2 encryption in transit ensure sensitive unstructured data remains secure throughout its life cycle. Built-in antivirus scanning, data loss prevention (DLP) integration, and advanced threat prevention (ATP) capabilities protect against malware and data breaches across all communication channels.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced data governance capabilities into a single platform. The Data Policy Engine enforces attribute-based access controls (ABAC) and role-based access controls (RBAC) across all data exchange methods. Whether employees send and receive data via email, file share, automated file transfer, APIs, or web forms, comprehensive audit logs capture every action for compliance reporting and forensic analysis.

Simplicity and Ease of Use

Kiteworks offers a user-friendly interface that simplifies secure file sharing and collaboration while maintaining enterprise-grade security. The platform enables users to easily send, receive, and manage sensitive data without compromising security through a native mobile app and web interface. Intuitive design and seamless integration with existing workflows through LDAP, Active Directory, SAML 2.0, and SCIM support ensures high user adoption rates across defence organizations.

Defence-Grade Security Architecture

Kiteworks implements a hardened virtual appliance architecture with embedded network and web application firewalls specifically designed for defence environments. The platform's tiered internal services follow zero-trust principles, treating all communications as untrusted. Combined with FIPS 140-3 validated encryption, hardware security module (HSM) integration, and customer-owned encryption keys, Kiteworks provides the military-grade security required for Defence Standard 05-138 compliance while maintaining operational efficiency.

Cyber Risk Profile Requirements

Control	Requirement	Kiteworks Solution
1200 Risk management	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. This includes an overall organisational approach to risk management.	Kiteworks supports compliance through its Data Policy Engine (DPE), which provides an attribute-based access policy engine that evaluates rules with boolean condition trees across content, user, and geolocation attributes to produce block, safe-view, safe-edit, apply-tag decisions, and approval requirements. The platform's risk and DLP policy engine enables administrators to define risk policies with rules, directives, approvers, tag and form triggers, and automated actions on content. The platform follows standards and best practices, designed and developed according to years of experience and formal industry standards such as the NIST CSF, providing a comprehensive organizational approach to risk management that helps identify, assess, understand, and remediate security risks.
1202 Periodically assess risk	The Supplier shall periodically assess the risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, resulting from the operation of organisational systems and the associated processing, storage, or transmission of Data.	Kiteworks enables periodic risk assessment through compliance reporting dashboards that generate, update, export, and snapshot compliance reports with per-control status and linked risk policies and tags. The platform maintains comprehensive audit logs with SIEM feeds, automatically cleaning, normalizing, standardizing, and aggregating log data into a single stream. Threat reports and insider threat dashboards generate insider and outsider threat reports covering communications, top actors, and country activity with CSV export capabilities. Security Analytics features allow organizations to use the CISO Dashboard and Splunk App visualizations to show suspicious traffic patterns, including anomalies in download locations, traffic levels, user activities, and individual file activities. These capabilities enable organizations to continuously assess risks to operations, assets, and individuals by providing visibility into system usage patterns, potential threats, and compliance status across all data processing, storage, and transmission activities.
1204 Threat intelligence capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	Kiteworks implements comprehensive threat intelligence capabilities through Advanced Threat Prevention (ATP) Integration via ICAP protocol, supporting Trellix threat detection and response products and Check Point Harmony Endpoint using native APIs. Threat Intelligence Notifications provide real-time alerts when the Kiteworks security team identifies security threats that may impact systems, displayed via banners at the top of each admin console page. The platform integrates with Trellix Helix Connect (formerly FireEye Helix), submitting files to Trellix Malware Analysis (formerly FireEye AX) and Trellix Intelligent Virtual Execution (IVX) for detonation, tracking submission and analysis status with configurable priority and mode. Check Point Threat Prevention integration uploads and queries file verdicts via Check Point Threat Prevention API with cookie-based session reuse. These threat intelligence capabilities guide risk assessments, inform security architecture decisions, support threat hunting activities, generate system security alerts and advisories, and enhance response and recovery activities by providing actionable intelligence about emerging threats and vulnerabilities.
1206 Internal controls assurance	The Supplier shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed timeframes.	Kiteworks provides ongoing monitoring of security controls through Risky Settings detection and dashboard, which automatically detects potentially risky settings when an admin user makes changes away from safe defaults, typically requiring authorization sign-off before settings can be saved. The Risky Settings dashboard summarizes all checked settings and marks their current status as safe, authorized, or warning. An admin activity audit trail supports list, detail, and CSV export endpoints for forensic review of all administrative actions. Compliance reporting dashboards for frameworks like CMMC provide compliance report metadata, CMMC practices, glossary, and compliancy status details for per-framework compliance dashboards. These features enable continuous monitoring of control effectiveness, recording of deficiencies, reporting to leadership, and tracking of mitigation activities within agreed timeframes.

Control	Requirement	Kiteworks Solution
1301 Automated asset inventory management	The Supplier shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support business Functions and protect Data.	Kiteworks employs automated discovery and management tools through ACFS clustered filesystem volume management, which adds host disks, assigns storage roles to cluster nodes, creates and removes ACFS volumes, and monitors mount health. The platform's cluster node topology and routing capabilities discover nodes, network interfaces, reachable IPs, and manage inter-node routing including default routes and route validation. Storage capacity and disk monitoring reports filesystem usage by type, DB storage, disk types, NFS mountpoints, and boot metrics for admin health views. Node health metrics and service dashboard expose per-node metrics including DB, web, jobs, SFTP, resources, and cluster service status with associated actions through the admin console. These automated tools maintain an up-to-date, complete, and accurate inventory of systems, infrastructure components, storage resources, and service states that support business functions and protect data, providing readily available visibility into the entire deployment infrastructure.
2200 Identity and access control	The Supplier shall understand, document and manage (i.e. create, review and disable) access to networks, information systems, and removable storage media & devices supporting Functions and protection of Data. All accounts and identities, including users, system and automated functions that can access Data or systems are appropriately verified, authenticated and authorised.	Kiteworks provides comprehensive identity and access control through multiple forms of authentication supported in a single system instance. The platform integrates with one or more LDAP and Microsoft Active Directory sources, providing automatic user onboarding, offboarding, and role updates. SAML 2.0 Single Sign-on (SSO) support enables integration with any SAML 2.0 compliant identity provider such as Microsoft Entra ID. SCIM Support ensures compliance with the System for Cross-identity Management using REST API, allowing Kiteworks accounts to be centrally managed through any external Identity Management solution supporting SCIM 2.0. These capabilities ensure all accounts and identities, including users, system accounts, and automated functions accessing data or systems, are appropriately verified, authenticated, and authorized. The platform documents and manages access through centralized identity systems, supporting the complete life cycle of user access including creation, review, and disabling of accounts across networks, information systems, and storage devices.
2201 Access control – multi-factor authentication	The Supplier shall implement multi-factor authentication (MFA) mechanisms to control access to critical or sensitive systems, and organisational operations. Factors can include: i) Something you know (e.g. password/ personal identification number (PIN)) ii) Something you have (e.g. cryptographic identification device, token) iii) Something you are (e.g. biometric).	Kiteworks implements comprehensive multi-factor authentication mechanisms supporting all three authentication factors. The platform provides two-factor and multi-factor authentication via RADIUS protocol, PIV/CAC cards for cryptographic identification devices, Kiteworks native email-based One Time Password (OTP), Kiteworks native SMS-based OTP, and Time-based OTP following industry standard RFC 6238. The platform supports RFC 6238 standard enabling external authenticators including Google Authenticator, Microsoft Authenticator, and Authy. Personal Identity Verification (PIV) cards issued by U.S. federal agencies and Common Access Cards (CAC) issued by U.S. Department of War are supported for government users. A two-factor authentication toggle at the profile level allows organizations to require or allow 2FA for users via settings. These MFA mechanisms control access to critical and sensitive systems by combining something users know (passwords), something they have (tokens, cards, mobile devices), and supporting integration with biometric systems through standards-based protocols.
2202 Device management	The Supplier shall fully understand and trust the devices that are used to access the network and information systems that support Functions and process Data.	Registered devices with remote wipe functionality allow devices to be registered per install tag and marked for remote wipe, with wipe flag read/set capabilities and session termination on user deletion. The platform tracks mobile and desktop client support by type (mobile/desktop), registers mobile push tokens, and supports folder mobile-sync lists. Remote wipe of client devices can be admin-triggered to remove user content on devices when security concerns arise. Device registration, logout, and consent features enable users to manage registration tokens, log out specific devices, and record device consent. These capabilities provide organizations with complete visibility and control over all devices accessing the system, ensuring only trusted devices can access network and information systems that support functions and process data, with the ability to immediately revoke access and wipe data from compromised or untrusted devices.

Control	Requirement	Kiteworks Solution
2203 Privileged user management	The Supplier shall closely manage privileged user access and actions to networks and information systems supporting Functions and that protect Data.	Kiteworks closely manages privileged user access through delegated admin roles with configurable component scope, supporting admin role CRUD operations (add/delete/rename) and editing of admin permissions and role components for delegated administration. The platform enables segregation of administrative duties via a separate set of admin roles that control access to administrative features. Separation of duties is implemented through 8 default admin roles that meet security policies and regulations requiring separation of admin duties in most circumstances. The system enforces separation of admin duties using administrator roles including built-in system admin, helpdesk admin, and custom-defined roles. Configurable Administrator Roles allow organizations to define precise privileged access based on specific administrative functions needed. This granular approach to privileged user management ensures that administrative access is limited to only the specific functions required for each role, with all privileged actions tracked and auditable, protecting the networks and information systems that support business functions and data protection.
2204 Principle of least functionality	The Supplier shall ensure that all information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, programmes and services that are not integral to the operation of that information system.	Kiteworks implements the principle of least functionality through its embedded network firewall that provides a completely hands-off security mechanism blocking all unused ports from outside traffic. The platform is deployed as a hardened virtual appliance containing all necessary files and software to run Kiteworks securely within many layers of protection that minimize the attack surface. The minimized attack surface and perimeter protection approach protects the perimeter of the hardened virtual appliance by restricting access to only essential capabilities. The system is configured to prohibit non-essential functions, with all unnecessary ports, protocols, and services disabled by default. Only the specific ports and protocols required for Kiteworks operations are enabled, such as HTTPS for web access, SFTP for managed file transfer, and specific ports for email gateway functions when configured. This architecture ensures information systems provide only the essential capabilities needed for secure content communication and collaboration while restricting all non-integral functions.
2205 Least privilege	The Supplier shall closely manage all user accounts and employ the principle of least privilege to networks and information systems supporting all Functions and protecting all Data.	Kiteworks enforces the principle of least privilege throughout the platform, where all users initially have no privileges and only receive privileges for functionality when assigned a user profile, receiving privileges for data access only by invitation from users who manage the data. The platform implements comprehensive RBAC and ABAC governance controls where every operation respects the organization's governance framework, with AI operations through the MCP Server inheriting authenticated user roles and permissions. Role-based access controls (RBAC), attribute-based access controls (ABAC), permissions, and least-privileged defaults are implemented through the Data Policy Engine, with ABAC policies called data policies. Within Kiteworks, these controls ensure users can only access the minimum resources and data necessary to perform their assigned functions. The system closely manages all user accounts by starting with zero permissions and requiring explicit grants for each capability, ensuring that access to networks and information systems supporting all functions and protecting all data follows strict least-privilege principles.
2206 Least privilege – audit system	The Supplier shall limit access to systems' audit/security logging data and functionality to privileged user groups that have a confirmed requirement in accordance with the principle of least privilege.	Kiteworks limits audit and security logging access through Admin Role-Based Access to Tracking Data, where roles provide separation of duties ensuring individuals see only data appropriate based on policies and compliance regulations. The Compliance Role can access Files and Mail, Tracking Dashboard, Compliance Reports, and Risk Policies apps, while other roles have different access levels. The platform maintains a persistent audit event log with per-event enrichment, persisting events with entity resolution for files, folders, users, mail, attachments, and comments with default single-line descriptions per event type. Anonymized Audit Logs are implemented by default to ensure privacy standards and regulations compliance, performing anonymization using UUIDs with administrators able to convert UUIDs to email addresses only when detailed information is required. The DLI (Data Leak Investigator) Administrator role can run eDiscovery reports for all activities, emails, and files accessed by specific users, but this privileged access is restricted to only those with confirmed requirements for security investigations.

Control	Requirement	Kiteworks Solution
2207 Separation of duties	The Supplier shall develop a policy and implement a separation of duties methodology for standard and privileged accounts which support Functions and protect Data.	Kiteworks implements comprehensive separation of duties through default admin roles designed to meet security policies and regulations. The platform provides 8 default admin roles that satisfy separation requirements in most circumstances, with custom roles available for tailoring to specific customer requirements. Admin roles enable segregation of administrative duties via a separate set of admin roles controlling access to administrative features. Custom Admin roles can be defined by a System Admin to customize separation of administrative duties to exact deployment requirements, easily created by copying any existing role and modifying its granular permissions. The platform models delegated admin roles with per-component permissions, implementing role-based admin rights scoped to individual admin components, along with clone-role ranks and admin menu constants. This separation of duties methodology ensures standard and privileged accounts supporting functions and protecting data operate under clearly defined boundaries with no single account having excessive privileges.
2208 Identity and Access Management (IdAM)	The Supplier shall closely manage and maintain identity and access control for users/admins, devices and systems accessing their networks and information systems supporting business Functions and protecting all Data.	Kiteworks provides comprehensive Identity and Access Management through integration with a broad set of identity management and authentication systems. Enterprise authentication integrations include LDAP/Microsoft Active Directory, SAML 2.0/Microsoft Entra ID, Kerberos, and SSO/2FA/MFA with support for the RADIUS protocol. SCIM Support enables compliance with System for Cross-identity Management using REST API, allowing Kiteworks accounts to be centrally managed through any external Identity Management solution supporting SCIM 2.0. Automation of User Profile Assignment reads user attributes from multiple LDAP and SAML 2.0 sources including Microsoft Entra ID, using attribute values to map user profiles matching centrally defined roles. User life-cycle administration supports activate, suspend, deactivate, delete, and reactivate users, along with password reset, password setting, TOS acceptance, and data cleanup/retention on user removal. This comprehensive IdAM approach closely manages and maintains identity and access control for all users, admins, devices and systems accessing networks and information systems that support business functions and protect data.
2209 Limit access to authorised entities	The Supplier shall implement automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users.	Kiteworks implements comprehensive automated mechanisms for system account management through SCIM Support, enabling compliance with System for Cross-identity Management via REST API and allowing centralized account management through any external Identity Management solution supporting SCIM 2.0. LDAP/Active Directory integration with one or more sources provides automatic user onboarding, offboarding, and role updates into the Kiteworks system. OAuth 2.0 client and token management supports full OAuth client life cycle including insert, update, enable, disable, and delete operations with access/refresh token issuance, hashed token lookup, scoped tokens, and per-profile client assignment. Service account governance through SCIM compliance allows Kiteworks accounts to be centrally managed, ensuring processes acting on behalf of authorized users are properly controlled. These automated mechanisms ensure that all system accounts, including automated processes and service accounts, are managed consistently with proper authorization, authentication, and life-cycle management supporting the limitation of access to only authorized entities.
2210 Limit to authorised transactions	The Supplier shall issue, manage, verify, revoke, and audit identities and credentials to authorised transactions,[1] users, and processes.	Kiteworks comprehensively manages identities and credentials for authorized transactions through multiple authentication forms supported in a single system instance. Admin roles implemented via the Data Policy Engine enable segregation of administrative duties with separate admin roles controlling access to administrative features and transactions. OAuth 2.0 authorization server with PKCE implements OAuth flows with access/refresh tokens, auth codes, client credentials, scopes, and PKCE code_challenge support through a dedicated OAuthStorage backend. All transactions are tracked through a persistent activity and audit log where events are persisted as Activities with structured per-event data, permission tagging, and filterable retrieval for audit trails. This comprehensive approach ensures the platform can issue credentials for authorized users and processes, manage their life cycle, verify authenticity of transactions, revoke access when needed, and maintain complete audit trails of all identity and credential usage for authorized transactions.

Control	Requirement	Kiteworks Solution
2211 Secure first-time password management	The Supplier shall employ secure practices for the secure storage, transmission, and management of first-time and one-time passwords. These practices include, but are not limited to: i) Secure storage of first-time password prior to use ii) Secure transmission of first-time and one-time passwords to their new user iii) Require first-time and one-time passwords are immediately changed after first logon.	Kiteworks employs secure practices for first-time and one-time password management through multiple mechanisms. The platform provides Kiteworks native email-based One-time Password (OTP) as a multi-factor authentication method, sending one-time passwords to users via email as the second authentication factor. Kiteworks native SMS-based OTP sends data via email while also sending recipients a one-time password via SMS text message to access data. Password policy and account lockout enforcement includes password history, complexity requirements, max-attempt lockout, and CAPTCHA challenges. Shortlink-based verification and password reset through VerificationCodeLink and PasswordSetLink with createVerificationCode/ createPasswordSetCode support provides secure one-time URLs for user flows. These mechanisms ensure secure storage of passwords before use, secure transmission to new users via encrypted channels, and enforcement of immediate password changes after first logon through the password policy system, meeting all requirements for secure first-time password management.
2212 Automated password management	The Supplier shall employ automated mechanisms for the generation, protection, storage, rotation, transmission, cryptographic protection and management of passwords for staff and systems.	Kiteworks employs comprehensive automated password management mechanisms including password policy enforcement covering minimum length, digits, case requirements, special characters, history, expiration, and change attempts. Encrypted auth-token payload handling ensures web authentication tokens are decrypted server-side with an IV-based symmetric scheme before session context is established. Password history and password policy features track per-user password history to enforce reuse policies and record failed password change counts. The encrypted DB password vault generates and persists encrypted passwords for DB users, reads passwords by key, and retrieves credentials from remote hosts. These automated mechanisms ensure passwords for both staff and systems are cryptographically protected during generation, storage, and transmission. The system automatically enforces rotation based on expiration policies, maintains encrypted storage of all passwords, and manages the complete password life cycle through automated processes that eliminate manual password handling vulnerabilities.
2213 Automated password quality check	The Supplier shall deploy technical controls to manage the quality of credentials across all identifiers. The technical controls should reflect industry standard requirements such as password length, complexity requirements (e.g. uppercase, lowercase, numbers and symbols), reuse history, prevent reuse of identifiers for a defined period, banned words and insecure pattern recognition (e.g. 1234), as appropriate.	Kiteworks deploys comprehensive technical controls for credential quality management through configurable password policy enforcement covering minimum length, digits, case requirements, special characters, history, expiration, and change attempts. Password history enforcement checks new passwords against stored password history and validates current passwords on changes to prevent reuse. Password complexity and expiration policy enforces password rules via a policy validator and flags expired passwords, blocking login until reset. The parameter validation framework provides a composable validator library including Str/Int/List/Set/Length/Min/Max/Enum/And validators with decorator-based function argument enforcement. These technical controls reflect industry standard requirements by enforcing password length, requiring combinations of uppercase, lowercase, numbers and symbols, maintaining reuse history to prevent recycling passwords, and detecting insecure patterns. The system automatically validates credential quality across all identifiers, ensuring only passwords meeting defined security standards are accepted.
2214 Repeated unsuccessful logon handling	The Supplier shall employ policies and processes to appropriately manage unsuccessful login attempts to standard and privileged accounts. The Supplier shall lock accounts after at most ten unsuccessful login attempts for a minimum of 15 minutes; the duration of which should increase between multiple account lockouts.	Kiteworks employs comprehensive policies for managing unsuccessful login attempts through account lockout and failed-login protection that tracks failed login attempts, lockout status, and sends account-locked notification emails. Account lockout and session timeout settings expose cookie timeout, max login attempts, lockout cooldown, and activation code lifetime with email notifications handling lockout and deactivation. Failed login detection and account lockout capabilities track failed login attempts, lock and unlock user accounts, and support admin unlock and concurrent login gating. Account lockout with automatic unlock locks users after configured failed login attempts and unlocks them after the cooldown period via batch job. The system can be configured to lock accounts after a specified number of unsuccessful attempts (meeting the requirement of at most ten), maintain lockout for configurable durations (supporting the minimum 15 minutes requirement), and increase lockout duration between multiple account lockouts, applying these policies consistently to both standard and privileged accounts.

Control	Requirement	Kiteworks Solution
2215 Replay-resistant authentication	The Supplier shall enforce technical control to protect against the capture of transmitted authentication or access control information and its subsequent retransmission i.e. replay attacks.	Kiteworks enforces comprehensive technical controls against replay attacks through OAuth 2.0 token authentication with refresh tokens, where the platform authenticates API clients via OAuth access tokens and refresh tokens with token issuance, scope tracking, and verification handled by a dedicated OAuth connector. JWT assertion grant authentication supports JWT-based client/user authentication with public key retrieval, issuer/audience verification, and replay protection via jti (JWT ID) tracking that prevents token reuse. Encrypted auth-token payload handling ensures web authentication tokens are decrypted server-side with an IV-based symmetric scheme before session context is established, preventing token interception and reuse. Session tokens with encrypted cargo use a cryptographic token class that creates and decodes encrypted cargo tokens using per-request keys. These mechanisms collectively protect against capture and retransmission of authentication information by using time-limited tokens, tracking token usage, encrypting authentication payloads, and generating unique per-request cryptographic materials.
2216 Privilege failure handling	The Supplier shall prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Kiteworks prevents non-privileged users from executing privileged functions through comprehensive admin roles implemented via the Data Policy Engine, enabling segregation of administrative duties via a separate set of admin roles that control access to administrative features. Role-based access control with admin roles uses Role and AdminRole entities plus UserAdminRole assignments to model RBAC and delegated administration, ensuring only authorized users can execute privileged functions. The platform captures all privileged function execution through a persistent audit event log with per-event enrichment, where the event service persists events with entity resolution for files, folders, users, mail, attachments, and comments with default single-line descriptions per event type. Admin activity audit logging through ActivityAdmin and Activity entities captures per-event messages, users, permissions, direct/indirect users, and success status for admin audit trails. This ensures all attempts to execute privileged functions are logged whether successful or not, providing complete visibility into privilege usage and preventing unauthorized privilege escalation.
2217 Service accounts	The Supplier shall inventory all generic, service and system accounts used on the network. Every account shall be owned by a single named individual who is responsible and accountable for the account and its usage.	Kiteworks maintains comprehensive inventory and ownership of all accounts through its authentication system supporting multiple forms of authentication in a single system. Admin roles implemented through the Data Policy Engine enable segregation of administrative duties via separate admin roles controlling access to administrative features, ensuring clear ownership and accountability. User life-cycle administration supports user creation, activation, verification, deactivation, deletion, unlock, and reactivation flows with LDAP/SSO conversion and password history enforcement, maintaining a complete inventory of all accounts. The persistent activity and audit log persists all events as Activities with structured per-event data, permission tagging, and filterable retrieval for audit trails, providing accountability tracking for all account usage. This approach ensures every generic, service, and system account is inventoried with a clear ownership model where named individuals are assigned responsibility for accounts, with all account activities tracked in the audit system for accountability purposes.
2218 System users and processes	The Supplier shall identify system users, processes acting on behalf of users, and devices.	Kiteworks comprehensively identifies system users, processes, and devices through its authentication system supporting multiple forms of authentication in a single system instance. The platform maintains registered devices with remote wipe capabilities, where devices are registered per install tag and can be marked for remote wipe, with wipe flag read/set and session termination on user deletion. Mobile and desktop sync clients with remote wipe are tracked through Client, MobileInfo, MobileSyncItem, SyncedObject, SyncFolder, and ClientInstallsWipe entities plus RemoteWipeFlag providing installed-client registration and remote wipe capabilities. OAuth 2.0 authorization server functionality provides full OAuth2 server support for authorize/token/revoke/resource endpoints and pluggable grant and response types, enabling identification and tracking of processes acting on behalf of users. This comprehensive approach ensures all system users are authenticated and identified, all processes acting on their behalf are tracked through OAuth mechanisms, and all devices accessing the system are registered and monitored.

Control	Requirement	Kiteworks Solution
2300 **Data security**	The Supplier shall appropriately protect data stored or transmitted electronically from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on Functions or Data. Such protection extends to how authorised users, devices and systems access critical data necessary for the operation of Functions and use of Data. Additionally, covers information that would assist an attacker, such as design details of networks and information systems.	Kiteworks protects data through comprehensive RBAC and ABAC Governance Controls where every AI operation through the MCP Server respects the organization's governance framework. Role-based access control ensures AI operations inherit authenticated user's roles and permissions, preventing AI from accessing resources outside user authorization. Attribute-based access control dynamically evaluates file attributes (classification, sensitivity labels, metadata), user attributes (department, clearance level), and contextual attributes (time, location, device, geography) to enforce fine-grained access decisions. Encryption at Rest provides File and Disk Double Encryption, double-encrypting customer files to minimize attack surface available to intruders who gain operating system access. TLS Certificate Validation provides comprehensive validation protecting against man-in-the-middle attacks with automatic certificate validation of remote Kiteworks servers using trusted certificate authorities and connection abort on validation failure. Zero Trust Mode for Intrusion Detection and Prevention blocks all IP addresses by default except those explicitly listed in the Allowed IP List, protecting against unauthorized access while securing critical system design information.
2302 **Data in transit**	The Supplier shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the Functions and all Data. This includes the transfer of data to third parties.	Kiteworks provides comprehensive protection for data in transit through Encryption in Transit using TLS 1.3 and 1.2. Customers can enable TLS 1.3 only, 1.2 only, or both, with AES-256 encryption by default and the option of AES-128. TLS Certificate Validation ensures comprehensive validation protecting against man-in-the-middle attacks and secure communication through automatic certificate validation of remote Kiteworks servers using trusted certificate authorities. Direct Kiteworks-to-Kiteworks integration (vault-to-vault) enables organizations and trading partners running MFT Server to directly and securely connect their Kiteworks applications, bypassing relatively less secure intermediary transfer protocols such as SFTP. FTPS with TLS 1.2 option provides enforcement of TLS 1.2 for FTPS connections when needed for compatibility with legacy FTPS servers that do not fully support TLS 1.3. These encryption and control mechanisms protect all data in transit including transfers to third parties, ensuring data important to business functions remains secure during transmission.
2303 **Management of established network connections**	The Supplier shall terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Kiteworks manages established network connections through comprehensive session management capabilities. Account lockout and session timeouts expose security user settings including cookie timeout, max login attempts, lockout cooldown, and activation code lifetime, with email notifications handling lockout and deactivation events. Concurrent session enforcement and remote wipe track concurrent sessions per user/token and support admin-initiated remote wipe of client installations. Session management with concurrent login control uses a sessions table with expires index and access_tokens login_state including 'concurrent' to detect and manage concurrent logins. SFTP managed file transfer profiles expose an SFTP allowance flag and user records carry an SFTP username populated from profile configuration, ensuring controlled access to file transfer sessions. These mechanisms ensure network connections are properly terminated at session end or after defined inactivity periods, preventing unauthorized access through stale connections and managing concurrent access attempts across all communication channels.
2305 **Remote Access – VPN (Virtual Private Network)**	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Kiteworks enforces comprehensive remote access controls through multi-factor authentication (MFA) supporting two-factor and multi-factor authentication via RADIUS protocol, PIV/CAC cards, Kiteworks native email-based OTP, Kiteworks native SMS-based OTP, and Time-based OTP following industry standard RFC 6238. Encryption in Transit ensures all data transmitted is protected using TLS 1.3 and 1.2, with customers able to enable TLS 1.3 only, 1.2 only, or both, using AES-256 by default with the option of AES-128. Zero Trust Mode for Intrusion Detection and Prevention blocks all IP addresses by default except those explicitly mentioned in the Allowed IP List, effectively preventing split-tunneling by ensuring connections only come from approved sources. Geofencing capabilities restrict sign-ins based on individual user settings, user profiles, or system level settings applying to all users. These controls ensure MFA is required before remote access, all transmitted data is encrypted, and connections are restricted to organization-controlled channels preventing data leakage through split-tunneling.

Control	Requirement	Kiteworks Solution
2306 Remote access sessions	The Supplier shall employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Kiteworks employs comprehensive cryptographic mechanisms to protect remote access session confidentiality. Encryption in Transit uses TLS 1.3 and 1.2, with customers able to enable TLS 1.3 only, 1.2 only, or both, using AES-256 by default with the option of AES-128. FIPS 140-3 Validated Encryption Option is available through the Kiteworks Government package with FIPS 140-3 certified encryption that has passed rigorous U.S. Government NIST Validation (certificate #4980). TLS Certificate Validation provides comprehensive validation protecting against man-in-the-middle attacks through automatic certificate validation of remote Kiteworks servers using trusted certificate authorities. OAuth 2.0 authorization server with PKCE implements custom OAuth request validation including client authentication, authorization code flow, scope validation, refresh tokens, PKCE challenge methods, and bearer token issuance. These cryptographic mechanisms ensure all remote access sessions are protected with industry-standard or government-validated encryption, maintaining confidentiality throughout the session life cycle.
2307 Managed access control points	The Supplier shall route remote access via managed access control points.	Kiteworks routes all remote access through managed access control points using Zero Trust Mode for Intrusion Detection and Prevention, where all IP addresses are blocked by default except those explicitly mentioned in the Allowed IP List. Geofencing capabilities restrict sign-ins based on settings at individual user level, user profile level, or system level applying to all users. IP address controls enable blocking or explicitly allowing user sign-in or unauthenticated access from specific IP addresses or IP address ranges. The embedded network firewall provides a completely hands-off security mechanism blocking all unused ports from outside traffic. These managed access control points ensure all remote access is routed through defined, monitored, and controlled entry points with comprehensive logging and access restrictions. The platform enforces routing through these control points by default-deny policies and explicit allowlisting, preventing bypass attempts and ensuring all remote connections pass through managed security controls.
2308 Stored data	The Supplier shall appropriately protect the confidentiality of soft and hard copies of data being stored for all Functions.	Kiteworks protects stored data confidentiality through Encryption at Rest with File and Disk Double Encryption, double-encrypting customer files to minimize attack surface available to intruders who gain operating system access. Customer-owned Keys ensure Kiteworks staff or outside actors like governments cannot decrypt customer private data for any reason, with customers owning their own encryption keys. Hardware Security Module (HSM) Integration with Thales Luna Network HSM and Amazon Web Services Key Management Service provides key management outside the Kiteworks appliances. Volume encryption with passphrase and KSM includes per-volume encryption passphrases and a dedicated Key Store Manager service exposing activate/deactivate/lock/unlock capabilities, passphrase rotation, and key slot encrypt/decrypt functions. This multi-layered approach ensures both soft copies (electronic files) and any hard copy data converted to electronic format are protected with strong encryption, customer-controlled keys, and enterprise-grade key management systems maintaining confidentiality for all stored data supporting business functions.
2309 Mobile data	The Supplier shall protect, such as through encryption, data important to the operation of Functions and all Data on mobile devices.	Kiteworks protects data on mobile devices through native apps for Android and iOS supporting secure email, secure file sharing, secure photos, and remote access to data file repositories via the Repositories Gateway. Mobile apps include security features such as jailbreak detection, Touch ID, Face ID, Fingerprints authentication, and a secure container for offline access with remote wipe capabilities. Secure container mobile client support distinguishes Secure Container and sync-client access to apply container-specific handling with appropriate security controls. Remote wipe of client devices enables admin-triggered removal of user content on devices when security concerns arise. Mobile device management provides admin-controlled MDM features for mobile clients accessing the platform. These protections ensure data important to business functions remains encrypted and secure on mobile devices, with the secure container providing encrypted storage for offline access while maintaining the ability to remotely wipe data if a device is lost, stolen, or compromised.

Control	Requirement	Kiteworks Solution
2310 Removable media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Kiteworks addresses removable media security through comprehensive controls. Encryption at Rest with File and Disk Double Encryption ensures any data that might be exported to removable media is already double-encrypted, minimizing attack surface if media is compromised. File type and MIME blacklist policy enforcement allows the object repository to enforce exclusion of disallowed MIME types, type groups, and file extensions as part of upload/policy checks, controlling what can be transferred. The persistent activity and audit log records all events as Activities with structured per-event data, permission tagging, and filterable retrieval providing audit trails of any data access that could involve removable media. Zero Trust Mode for Intrusion Detection and Prevention blocks all IP addresses by default except those explicitly mentioned in the Allowed IP List, helping prevent unauthorized systems with removable media from accessing the platform. While Kiteworks operates as a secure content platform rather than directly managing physical removable media, these controls ensure data protection and access restrictions that support organizational removable media policies.
2312 Security at alternate working locations	The Supplier shall employ technical security controls and educate users to reduce the security risks to employees while working outside the organisation's premise. Technical security controls for consideration may include, but are not limited to: i) Always-on VPN to protect data in-transit ii) Screen privacy protector to prevent shoulder surfing iii) Disabling USB ports on devices iv) Full disk encryption. User awareness topics may include, but are not limited to: i) Risks of using public Wi-Fi ii) Avoid taking confidential phone calls within earshot of unauthorised individuals iii) Shoulder surfing iv) Avoid leaving devices unattended.	Kiteworks employs technical security controls for alternate working locations through multi-factor authentication supporting two-factor and multi-factor authentication via RADIUS protocol, PIV/CAC cards, Kiteworks native email-based OTP, Kiteworks native SMS-based OTP, and Time-based OTP (RFC 6238). Encryption in Transit protects data using TLS 1.3 and 1.2 with AES-256 by default, securing connections even over untrusted networks. Mobile Apps for Android and iOS include security features like jailbreak detection, Touch ID, Face ID, Fingerprints authentication, and secure container for offline access with remote wipe capabilities, addressing device security at alternate locations. Zero Trust Mode blocks all IP addresses by default except those explicitly allowed, preventing access from unauthorized locations or compromised networks. These controls protect employees working outside organizational premises by ensuring strong authentication, encrypted communications, secure mobile access, and network-level protections against common risks associated with remote work environments including public Wi-Fi usage.
2313 Media/equipment sanitisation	The Supplier shall appropriately sanitise before reuse and / or disposal the devices, equipment, and removable storage media & devices holding data important to the operation of business Functions and that protect all Data.	Kiteworks provides secure data sanitization capabilities through comprehensive secure delete functionality. The platform implements secure delete features that enforce secure-delete behavior so file removals are shredded rather than simply unlinked from the filesystem. This ensures that when data is deleted, it cannot be recovered through forensic analysis or data recovery tools. The secure delete capability applies to all data stored within the Kiteworks platform, ensuring proper sanitization of storage media before reuse or disposal. While Kiteworks operates as a hardened virtual appliance and does not directly manage physical media sanitization, its secure delete features ensure that data within its control is properly sanitized, supporting organizational requirements for secure disposal of devices, equipment, and storage media that may have contained sensitive data important to business functions.
2315 Email authentication methods	The Supplier shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.	Kiteworks implements email authentication methods through comprehensive DKIM support. DKIM email signing enables upload of DKIM keys for email signing of outbound messages, ensuring message authenticity and integrity. DKIM key management for outbound email signing allows admins to upload, download, and set DKIM signing keys and selectors, protecting outbound email authenticity. The platform provides DKIM email signing with key generation and selectors, generating DKIM keys per domain/selector, enabling DKIM signing in sendmail, and publishing/reading selector TXT records. While SPF and DMARC are typically configured at the organizational email infrastructure level, Kiteworks' DKIM implementation ensures that emails sent through the platform are properly signed and authenticated, supporting the overall email authentication strategy. This helps verify the authenticity of email sources and protects against email spoofing and phishing attacks targeting the organization.

Control	Requirement	Kiteworks Solution
2316 Personal and/ or Personally Identifiable Information (PII) processing/ transparency – control flow	The Supplier shall employ systems to monitor and control the flow of all Personal and/or Personally Identifiable Information (PII) and all government information (e.g. OFFICIAL and above) provided or produced during the contract throughout the information lifecycle in accordance with approved authorisations, required legislation and contractual requirements.	Kiteworks monitors and controls PII and government information flow through comprehensive RBAC and ABAC Governance Controls providing enterprise-grade governance with role-based and attribute-based access controls. The attribute-based access policy engine evaluates rules with boolean condition trees across content, user, and geolocation attributes to produce block, safe-view, safe-edit, apply-tag decisions, and approval requirements. Data classification tagging with Microsoft Information Protection integration extracts, creates, and applies tags to files, supporting tag sync and usage reporting in risk policies. Comprehensive audit logging through SIEM integration helps organizations detect, analyze, and respond to security threats, with SecOps teams using SIEM tools to ingest, consolidate, analyze, and report on log data. These systems ensure PII and government information flows are monitored throughout the information life cycle, controlled according to approved authorizations, and tracked to meet legislation and contractual requirements for data protection and transparency.
2318 Approved cryptographic methods	The Supplier shall employ appropriate nationally or departmentally approved cryptography when used to protect all Data (e.g. FIPS 140-2 or comparable standards).	Kiteworks employs nationally approved cryptographic methods through FIPS 140-3 Validated Encryption Option. The Kiteworks Government package offers FIPS 140-3 certified encryption that has passed rigorous U.S. Government NIST Validation (certificate #4980, module name: Kiteworks Cryptographic Module, initial validation 3 March 2025). Encryption at Rest provides File and Disk Double Encryption, double-encrypting customer files to minimize attack surface available to intruders accessing the operating system, implementing assumed-breach architecture where the system protects data even when attackers breach outer appliance layers. Encryption in Transit uses TLS 1.3 and 1.2 with customers able to enable TLS 1.3 only, 1.2 only, or both, using AES-256 by default with AES-128 option, and can optionally use FIPS 140-3 Validated encryption. These approved cryptographic methods meet or exceed FIPS 140-2 standards, ensuring all data is protected with nationally approved cryptography suitable for government and defense use cases.
2319 Securely manage cryptographic keys	The Supplier shall establish and manage cryptographic keys for cryptography employed in organisational systems using appropriate nationally or departmentally approved solutions (e.g. FIPS 140-2 or comparable standards).	Kiteworks establishes and manages cryptographic keys through Hardware Security Module (HSM) Integration with Thales Luna Network HSM and Amazon Web Services Key Management Service, providing key management outside Kiteworks appliances. The Kiteworks platform also supports Entrust nShield HSMs for additional flexibility in key management. Customer-owned Keys ensure Kiteworks staff or outside actors cannot decrypt customer private data for any reason, with customers owning their encryption keys, ensuring full control over data privacy and compliance with privacy regulations. Key Storage Module (KSM) with passphrase life cycle manages per-volume master/ super/file-encryption keys with scrypt/PBKDF2 derivation, passphrase rotation, backup, and secure delete capabilities. These nationally approved solutions meet FIPS 140-2 comparable standards, with HSM integration providing hardware-based key protection and management. The comprehensive key management approach ensures cryptographic keys are securely generated, stored, rotated, and destroyed according to approved standards.
2320 Data Loss Prevention (DLP)	The Supplier shall implement and maintain appropriate tooling to monitor and restrict the access and use of: i) Removable storage media and devices ii) External websites iii) Email.	Kiteworks implements comprehensive data loss prevention through integration with commercially available DLP solutions via the ICAP protocol. The Kiteworks DLP module enables organizations to secure shared information while monitoring and analyzing contents, filtering data files based on corporate policy, IP protection, and compliance requirements. The DLP rule engine with per-file flagging and quarantine allows admins to toggle DLP scanning, view DLP-flagged files, and manually adjust DLP flags on objects. DLP enforcement exceptions surface DLP scanning/prohibited errors and server-busy conditions to clients during upload and share operations. These DLP capabilities monitor and restrict data movement across all Kiteworks channels including email, file shares, and managed file transfer, providing visibility and control over sensitive data to prevent unauthorized access or exfiltration through removable media, external websites, or email channels. The integration approach allows organizations to leverage their existing DLP investments while extending protection to Kiteworks-managed content communications.

Control	Requirement	Kiteworks Solution
2321 Publicly accessible data	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.	Kiteworks supports management of publicly accessible data through role-based access control with admin roles implementing RBAC and ABAC controls with permissions and least-privileged defaults. The Data Policy Engine combines Kiteworks data access controls including ABAC and RBAC controls to designate authorized individuals who can make information publicly accessible. Audit log search and export via Solr builds filtered queries over event streams, creates audit log reports, and supports keyword/time/policy/object filters and CSV export for reviewing content access and sharing activities. These capabilities enable organizations to designate specific individuals authorized to share content publicly, implement controls ensuring only approved content becomes publicly accessible, maintain audit trails of all public sharing activities for periodic review, and quickly identify and remove any non-public information that may have been inadvertently shared. The granular permission system ensures only trained, authorized users can create public links or share content externally.
2322 Mobile devices/ Bring Your Own Device (BYOD)	The Supplier shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.	Kiteworks ensures mobile devices are appropriately configured and managed through multiple controls. The mobile app feature toggle provides a system feature flag to enable or disable mobile app access, giving organizations control over mobile access. Mobile device management provides admin-controlled MDM features for mobile clients accessing the platform, supporting industry-recognized MDM solutions. Remote wipe of registered devices allows devices registered per install tag to be marked for remote wipe, with wipe flag read/set capabilities and session termination on user deletion. These capabilities ensure that both corporate-owned and BYOD devices accessing corporate data through Kiteworks are properly managed, with the ability to enforce security policies, control access, and remotely wipe corporate data from devices when necessary. The platform's mobile security features integrate with organizational MDM solutions to provide comprehensive mobile device management aligned with security requirements.
2323 Secure destruction	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.	Kiteworks implements secure data destruction through a retention cleanup and expiry engine that executes expiry and permanent-delete tasks over tenant objects, tracks results, and logs execution summary. Legal hold and data retention on user deletion preserves content when users are removed according to legal requirements. Secure delete of files ensures file removals are shredded rather than simply unlinked, providing cryptographic erasure. These procedures ensure all data is securely destroyed when no longer needed or at contract expiration/termination. The platform confirms erasure from systems and servers including all copies, provides audit logs that can serve as attestation of destruction when required by contract, and ensures secure disposal of data according to defined retention policies unless explicitly required to retain by country legislation or Authority instructions.

Control	Requirement	Kiteworks Solution
2401 Secure configuration	The Supplier shall securely configure the network and information systems that support the operation of business Functions and that protect Data.	Kiteworks ensures secure configuration through deployment as a hardened virtual appliance containing all necessary files and software to run Kiteworks securely within many layers of protection that minimize the attack surface. The embedded network firewall provides a completely hands-off security mechanism blocking all unused ports from outside traffic. Risky Settings Detection guides administrators through tightening existing security settings to reduce potential system exposure, displaying alerts upon each admin login until risky settings are confirmed or changed. The hardened appliance approach ensures secure baseline configuration by default, with the embedded firewall automatically configured to block unnecessary services and ports. The Risky Settings Detection actively monitors configuration changes and alerts administrators when settings deviate from secure defaults, ensuring ongoing configuration security. This multi-layered approach to secure configuration protects the network and information systems supporting business functions and data protection through defense-in-depth architecture.
2402 Vulnerability management	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a monthly basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.	Kiteworks implements comprehensive vulnerability management through DevSecOps "Shift Left" practices, moving test, quality, and performance evaluation as early as possible in development, often before code is written. This helps teams anticipate changes during development that could lead to security vulnerabilities. Automated and Manual Penetration Testing is conducted as part of the development process, including ongoing automated and periodic manual penetration testing for web, server, Repositories Gateway, mobile, and desktop clients. The platform performs regular vulnerability scanning and assessment throughout the development life cycle and in production. Patches and updates are prioritized based on CVSS scoring and risk assessment, with critical vulnerabilities addressed according to defined remediation timelines. The vulnerability management process includes identification through scanning and testing, reporting through security advisories, and remediation through regular platform updates distributed to customers, ensuring vulnerabilities are addressed in line with industry standards.
2403 Penetration testing	The Supplier shall conduct penetration testing (minimum every 12 months) against externally facing systems used to support the operation of Functions and that protect Data. The penetration testing programme shall be based upon industry standards and performed by subject matter experts. The Supplier shall ensure that any deficiencies identified are remediated in a timely manner in line with their risk to the network. The Supplier shall retain records including: i) The scope and methodology utilised ii) The number of critical, high, and medium severity findings iii) The name of the tester iv) The date of the testing v) Timelines and actions for a remedial plan.	Kiteworks conducts comprehensive penetration testing through Automated and Manual Penetration Testing as part of the development process. This includes ongoing automated and periodic manual penetration testing conducted for web, server, Repositories Gateway, mobile, and desktop clients. The platform also implements White and Black Box Bounty Programs where white box bounty hunters are contracted outside cybersecurity experts taught about Kiteworks internals before attempting system breaches, while black box bounty hunters are given no prior knowledge of Kiteworks, finding vulnerabilities opportunistically. Testing is performed by subject matter experts following industry standards, with findings documented including scope, methodology, severity classifications, tester information, and testing dates. Identified deficiencies are remediated according to risk-based timelines, with critical findings addressed urgently. Records of all penetration testing activities, findings, and remediation actions are maintained to demonstrate ongoing security assessment and improvement.

Control	Requirement	Kiteworks Solution
2404 Change management	The Supplier shall formally document, publish and review (minimum every 12 months) the change control procedures to manage changes to information systems, supporting infrastructure and facilities. The change management policy includes: i) Definitions of the types of change (e.g. standard, critical, emergency) with associated processes ii) Roles and responsibilities for those involved in the change or approving the change. Prior to implementing any changes, Supplier shall: i) Establish acceptance criteria for production change approval and implementation ii) Require stakeholder approval prior to any change implementation iii) Formally record the change in a centralised repository iv) Document business impact analysis outcomes and document back-out procedures should the change fail v) Keep a full audit trail of the change request, testing conducted, associated documentation, approvals and outcomes vi) Document and record security impact analysis outcomes along with any mitigating actions.	Kiteworks implements change management through comprehensive audit logging where SIEM systems help organizations detect, analyze, and respond to security threats, with SecOps teams using SIEM tools to ingest, consolidate, analyze, and report on log data from systems across the enterprise. Admin activity audit trail supports list, detail, and CSV export endpoints for forensic review of all administrative changes. One-click Updates allow the hardened virtual appliance to check for updates, with system admins able to click to download, cryptographically verify, and apply updates to the cluster automatically. Change control procedures are embedded in the platform's update process, with all changes tested through the comprehensive development and QA process before release. Updates are formally documented with release notes, security advisories where applicable, and detailed change logs. The audit system maintains full trails of change implementation including who applied updates, when they were applied, and system state before and after changes.
2405 Patch management	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.	Kiteworks maintains a robust patch management program through software update orchestration that manages multi-node software updates across clusters with pre-checks, package download, apply, and post-processing phases, tracking per-node status and stale-status recovery. Encrypted software patch management applies, reverts, and rolls back signed/encrypted patches with verification, decryption, and per-patch metadata, including RPM and diff patch modes. WAF signature auto-update tracks update availability/state for the WAF component and records check-update telemetry. The platform identifies vulnerabilities through continuous security monitoring, threat intelligence, and vulnerability scanning. Patches are tested through comprehensive QA processes before release, with critical security patches expedited through emergency release procedures. Updates are implemented automatically across clusters with built-in rollback capabilities if issues arise. Out-of-band emergency patching is supported through rapid patch development and deployment processes for critical vulnerabilities.
2406 Privacy warning notices – prior to access	The Supplier shall ensure that mechanisms are in place to ensure users accept appropriate warning notices prior to information system access. At a minimum users must be warned that: i) Use of the information system is monitored, recorded and subject to audit ii) Unauthorised usage of the information system is prohibited iii) Unauthorised usage of the information system use is subject to criminal and civil penalties iv) In continuing, the user affirms consent to monitoring and recording of their activities.	Kiteworks implements privacy warning notices through Terms-of-Service and EULA acknowledgement mechanisms. Admins can retrieve EULA content, capture TOS acknowledgements, and trigger explicit acknowledgements for sensitive configuration changes. The Terms of Service acceptance flow enforces Terms-of-Service steps at login and presents friendly TOS content to users. Terms of service acceptance functionality fetches and records user acceptance of terms of service. These mechanisms ensure users are presented with appropriate warning notices before accessing the information system, including notifications that system use is monitored, recorded, and subject to audit, that unauthorized usage is prohibited and subject to criminal and civil penalties, and that by continuing users consent to monitoring and recording of their activities. The platform maintains records of user acceptance providing evidence of informed consent to system monitoring and usage terms.

Control	Requirement	Kiteworks Solution
2407 Privacy warning notices – specific handling	The Supplier shall ensure that users accept appropriate warning notices prior to information system access where information systems contain information with specific handling requirements imposed by the UK or its International Partners. Such warnings must only be provided to authenticated users. At a minimum users must be warned that: i) The information system contains information with specific requirements imposed by the UK and/or international partner nations. ii) Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.	Kiteworks provides targeted privacy warnings through Terms of Service policies that enable organizations to present information users must review and accept before accessing system data. Terms can be global or different for different user profiles, such as no terms for employees but click-through legal notices for first-time external users. The Terms of Service acceptance gate requires user acceptance before completing authentication when policy mandates it, ensuring warnings are only shown to authenticated users. The platform supports ITAR and Export Control Compliance through Trusted Data Format (TDF), helping organizations comply with International Traffic in Arms Regulations and export control requirements by restricting access based on citizenship and nationality. These capabilities allow organizations to present specific warnings about UK or international partner handling requirements, export control restrictions, and licensing requirements to authenticated users before they access controlled information, with acceptance tracked and auditable.
2408 Screen locking/ timeouts	The Supplier shall have controls in place to automatically lock user sessions after a predefined period. The lock screen shall conceal all information previously displayed on the screen and prevent unauthorised viewing of data.	Kiteworks implements session locking and timeout controls through concurrent session termination and cookie timeout capabilities. Admins can terminate concurrent user sessions and tune cookie/session timeouts for security purposes. Account lockout and session timeout settings expose cookie timeout, max login attempts, lockout cooldown, and activation code lifetime configurations, with email notifications handling lockout and deactivation events. These controls automatically lock user sessions after predefined inactivity periods configured by administrators. When sessions timeout, users must re-authenticate to regain access, ensuring previously displayed information is no longer accessible and preventing unauthorized viewing of data. The timeout periods can be configured based on security requirements, with shorter timeouts for more sensitive environments. Session termination clears all session data from memory, requiring full re-authentication rather than simple screen unlocking, providing stronger security for inactive sessions.
2411 Secured internet access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.).	Kiteworks enforces secured internet access through multiple layers of protection. Antivirus scanning and quarantine with built-in WithSecure (formerly F-Secure Business) antivirus service scans files for malware on download and upload, supporting files of any size including those passing through Repositories Gateway or Email Protection Gateway. The embedded Web Application Firewall (WAF) provides zero-management barrier protection against suspicious network traffic, known attack signatures, SQL injection, exfiltration, and command and control attempts. Comprehensive audit logs with SIEM feeds maintain security and compliance-related activity logs fed to SIEMs in real time with no batch delay. Zero Trust Mode for Intrusion Detection and Prevention blocks all IP addresses by default except those explicitly allowed. These controls prevent malware infection, block malicious traffic, scan all downloads, terminate inactive sessions, and provide comprehensive auditing with security operator notifications. The platform supports allow/block listing and continuous monitoring to mitigate risks when legitimate business needs require specific access.

Control	Requirement	Kiteworks Solution
2413 Mobile code management	The Supplier shall define acceptable and unacceptable mobile code, and ensure controls are in place to identify, authorise, monitor, review and control the use of mobile code within the organisation.	Kiteworks manages mobile code risks through file type and MIME blacklist policy enforcement, where the object repository enforces exclusion of disallowed MIME types, type groups, and file extensions as part of upload and policy checks. The attribute-based access policy engine evaluates rules with boolean condition trees across content, user, and geolocation attributes to produce block, safe-view, safe-edit, apply-tag decisions, and approval requirements for potentially risky content. The persistent activity and audit log records all events as Activities with structured per-event data, permission tagging, and filterable retrieval for audit trails of all file activities including those containing mobile code. These controls enable organizations to define policies for acceptable and unacceptable mobile code types, automatically identify and block prohibited code during upload attempts, monitor all mobile code-related activities, and maintain comprehensive audit trails for review. The policy engine can be configured to require additional authorization for specific file types associated with mobile code.
2414 Communication authenticity protection	The Supplier shall use secure network management and communication protocols to protect session authenticity addressing communications protection at the session level.	Kiteworks protects communication authenticity through Encryption in Transit using TLS 1.3 and 1.2, with customers able to enable TLS 1.3 only, 1.2 only, or both, using AES-256 by default with AES-128 option. OAuth 2.0 token authentication with refresh tokens authenticates API clients via OAuth access tokens and refresh tokens, with token issuance, scope tracking, and verification handled by a dedicated OAuth connector protecting session authenticity. SAML 2.0 Single Sign-on (SSO) supports integration with any SAML 2.0 compliant identity provider such as Microsoft Entra ID, supporting both IdP-initiated and SP-initiated SSO flows with cryptographically protected assertions. These secure protocols ensure session authenticity is maintained throughout communications, with strong encryption protecting against session hijacking, man-in-the-middle attacks, and replay attacks. All network management and communication protocols used by the platform implement current security standards for authentication and session protection.
2415 Automatically identify and address misconfigurations and unauthorised components	The Supplier shall employ automated mechanisms to detect misconfigured or unauthorised system components.	Kiteworks employs automated mechanisms to detect misconfigurations through Risky Settings Detection, which guides administrators in tightening security settings to reduce potential system exposure. The system displays alerts upon each admin login when risky settings are detected until settings are confirmed or changed. Compliance Reports provide several reports showing compliance with regulations based on individual policy controls, currently supporting Audit Log, CMMC 2.0, Insider Threats, Outsider Threats, GDPR, and HIPAA compliance frameworks. AI-based Intrusion and Anomaly Detection maintains an evolving library of patterns detecting suspicious activities on the network and within the Kiteworks virtual appliance using artificial intelligence and other technologies. These patterns match network traffic, known attack signatures, exfiltration attempts, command and control attempts, and new code or changes to existing code. The automated detection capabilities continuously monitor for misconfigurations, unauthorized components, and anomalous behavior, alerting administrators to potential security issues requiring attention.
2416 Shared system resources	The supplier shall prevent unauthorised and unintended information transfer via shared system resources (e.g. registers, cache memory, main memory, hard disks).	Kiteworks prevents unauthorized information transfer via shared system resources through Single-tenant Private Cloud architecture. The platform is architected for single tenancy by design with no sharing of databases, file systems, application runtimes, or operating systems with other customers. While most SaaS providers use multi-tenant products for cost and maintenance benefits, Kiteworks chooses single-tenant architecture for enhanced security eliminating cross-tenant bugs and attack risks. Tiered Internal Services with Zero-trust Principles ensure each service treats communications from other services as untrusted, with code for each service running in silos without direct access to data or functions within other services. File and Disk Double Encryption double-encrypts customer files so even if attackers gain operating system access, they only have access to encrypted blobs decryptable only with file-level keys. This architecture prevents unauthorized information transfer through shared resources by eliminating resource sharing between customers and implementing strong isolation between internal components.

Control	Requirement	Kiteworks Solution
2417 Authorise remote execution of privileged commands	The Supplier shall ensure that all remote users acquire appropriate authorisation prior to accessing and/or executing privileged functions.	Kiteworks ensures remote privileged command authorization through Delegated administrator roles where administrators have access permissions for various tracking data based on customizable admin roles, implementing administrative separation of duties required for security and compliance policies. Admins do not have access to the data itself, even data they track. Multi-factor authentication (MFA) supports two-factor and multi-factor authentication via RADIUS protocol, PIV/CAC cards, Kiteworks native email-based OTP, Kiteworks native SMS-based OTP, and Time-based OTP (RFC 6238) ensuring strong authentication for privileged access. The No Kiteworks or Admin Access model ensures neither Kiteworks nor customers' IT admins can access or modify files, software, database, or operating system within the virtual appliance except when customers involve Kiteworks Support to resolve incidents. SSH daemon administration controls SSH banner, KEX/MAC algorithms, port, and per-host support SSH access with strict authorization requirements. All remote privileged function execution requires appropriate role-based authorization and strong authentication.
2418 Baseline configurations and inventories	The Supplier shall implement, update and document system hardening procedures. Implement, update and document baseline configurations settings for all information technology products deployed in organisational systems; this shall include the restriction of user actions and of unsupported software and hardware.	Kiteworks implements system hardening through deployment as a hardened virtual appliance containing all necessary files and software to run securely within many protection layers minimizing attack surface. The platform runs on a stripped-down Rocky Linux 8.10 operating system with unnecessary components removed and security hardening applied. The CMMC 2.0 Report Controls Addendum lists all CMMC control domains, evaluating current system configurations and presenting read-only views of relevant settings with compliance status determinations (Compliant, Not Compliant, or Review Manually). Baseline configurations are enforced through the hardened appliance approach, restricting user actions by design and preventing installation of unsupported software or hardware. System hardening procedures are continuously updated through the development process, with each release incorporating latest security best practices. Documentation of baseline configurations is provided through compliance reports and system documentation showing security settings and restrictions.
2419 Obscure authentication information	The Supplier shall configure systems to obscure authentication information, for example, passwords to ensure that they are not displayed as cleartext when a user is inputting their credentials.	Kiteworks implements secure credential handling through Credential-based authentication providing secure authentication using username and password credentials. User ID and Password credentials can be entered manually in login screens with autocomplete disabled for these fields across all browsers, preventing credentials from being auto-filled and stored to improve security and compliance. Password fields are configured to obscure input, displaying masked characters instead of cleartext as users type. Password policy enforcement through OAuth 2.0 enforces password history checks to prevent reuse and sets password expiration timestamps for users while ensuring passwords are never displayed in cleartext during the authentication process. The platform ensures all authentication information including passwords, tokens, and other credentials are obscured during input and never displayed as cleartext in any interface, log file, or system output, protecting authentication information from shoulder surfing and other observation attacks.
2420 Authentication feedback	The Supplier shall configure systems to minimise feedback information from failed logons to ensure that the system does not provide any information that would allow unauthorised individuals to compromise authentication mechanisms. e.g. explicitly stating that the password is the incorrect authentication component.	Kiteworks minimizes authentication feedback information through account lockout and failed-login protection that tracks failed login attempts and lockout status while sending generic account-locked notification emails without revealing specific failure reasons. Failed login detection and account lockout tracks attempts and locks/unlocks user accounts without providing details about which authentication component failed. IP Address Blocking Fail2Ban blocks access from IPs with excessive failed login attempts, common targets for attacks, based on IP blocks and geographic locations, banning IPs reactively without revealing why authentication failed. The system provides generic error messages for failed authentication attempts, not distinguishing between invalid usernames, incorrect passwords, or other authentication failures. This approach prevents attackers from using error messages to enumerate valid usernames or determine which part of their authentication attempt failed, significantly reducing information available for compromise attempts.

Control	Requirement	Kiteworks Solution
2421 Network Time Protocol (NTP)	The Supplier shall implement a Network Time Protocol (NTP) to a recognised authoritative source, to synchronise the clocks of every network device to ensure accurate and consistent timestamps for audit records on associated system logs.	Kiteworks implements comprehensive NTP time synchronization to ensure accurate timestamps across all systems. The platform manages NTP servers, validates server lists, performs immediate sync operations, and migrates pool configuration on OS upgrades. NTP clock-sync compliance checking verifies every node has NTP configured to satisfy compliance framework requirements. The NTP/Chrony time synchronization provides an abstract NTP manager with both ntpd and chrony implementations to list/set servers, sync time, and report status. This ensures all network devices and cluster nodes maintain synchronized clocks using recognized authoritative time sources. Accurate time synchronization is critical for audit log integrity, enabling proper correlation of events across distributed systems and ensuring timestamps in audit records are consistent and reliable. The platform supports configuration of multiple NTP servers for redundancy and can use standard NTP pools or organization-specific time servers.
2422 Physical and logical access restrictions	The Supplier shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.	Kiteworks enforces comprehensive access restrictions for system changes through role-based access control with admin roles. Administrators can create, update, delete, and template admin roles, configuring fine-grained per-component permissions for custom roles. The Principle of Least Privilege ensures all users initially have no privileges, receiving privileges for functionality only when assigned a user profile and for data access only by invitation from data managers. Delegated admin roles with configurable component scope support admin role CRUD operations and editing of admin permissions and role components for delegated administration. Authorization through the Data Policy Engine implements RBAC and ABAC with permissions and least-privileged defaults, with ABAC policies called data policies. These controls define and enforce who can make changes to organizational systems, document access permissions through role definitions, require approval through role assignment processes, and enforce restrictions preventing unauthorized system modifications. All administrative actions are logged for audit purposes.
2423 Trusted source repository	The Supplier shall identify, register and maintain an inventory of system components using automated tooling for those assets that support business Functions and protect Data in an asset register, and at a minimum, include data location and asset ownership information.	Kiteworks maintains automated inventory of system components through CMMC compliance reporting that updates CMMC compliance reports and tracks expired compliance audits as part of risk/compliance policy modules. The platform supports cloud storage connectors for S3, Atmos, Dropbox, OneDrive, Google Drive, Salesforce, and Box with EC sources using OAuth tokens, ec_objects path hashing, backend enums, and multi-instance object support. File indexing and full-text search status tracks content through transactions_index_status and index_status tables with LONGTEXT data and start_time tracking for search indexing. These automated tools identify and register system components including storage locations, connected repositories, and indexed content. The asset register maintains information about data locations across on-premises and cloud storage, ownership through access permissions and user associations, and component status through health monitoring. This automated inventory supports business functions by ensuring all data repositories and system components are tracked and manageable.
2424 Implement audit for stored credentials outside policy	The Supplier shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/ location/tools etc.) and quarterly audits are performed to ensure the control is consistently applied and functions appropriately.	Kiteworks ensures secure credential storage through Customer-owned Keys where Kiteworks staff or outside actors cannot decrypt customer private data for any reason, with customers owning their encryption keys, ensuring full control over data privacy. Hardware Security Module (HSM) Integration with Thales Luna Network HSM and AWS KMS provides key management outside Kiteworks appliances for enhanced security. Encrypted client secret storage encrypts OAuth/client secrets and backs up IV and passwords for credential recovery. The persistent audit event log with per-event enrichment persists events with entity resolution providing comprehensive audit capabilities for reviewing credential usage and access patterns. These mechanisms ensure administrator credentials are stored through approved secure storage (HSM/encrypted storage), with audit logs enabling quarterly reviews to verify controls are consistently applied. The audit system tracks all credential usage, allowing organizations to verify proper credential management and identify any policy violations.

Control	Requirement	Kiteworks Solution
2425 Use integrity verification tools	The Supplier shall implement an integrity verification tool to detect unauthorised changes to web-facing, critical software and firmware. Upon discovering discrepancies, the tool should automatically trigger the incident response process.	Kiteworks implements comprehensive integrity verification through AI-based Intrusion and Anomaly Detection maintaining evolving patterns detecting suspicious activities. These proprietary patterns match network traffic, known attack signatures, exfiltration attempts, command and control attempts, and critically, new code or changes to any existing code. Multiple tripwires within the virtual appliance slow down and make intrusion attempts difficult to hide. File Integrity Monitoring (FIM) enables admins to inspect file integrity monitoring results for tamper detection on the host system. Host-based intrusion detection through Wazuh/OSSEC controls the HIDS service, parses alerts, whitelists events, emails alerts, and logs failed SSH/SFTP logins as security events. When unauthorized changes are detected to web-facing components, critical software, or firmware, these tools automatically trigger incident response by generating alerts, logging security events, and notifying administrators. The multi-layered approach ensures comprehensive coverage of integrity verification across the platform.
2426 Anti-malware capabilities	The Supplier shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.	Kiteworks provides comprehensive anti-malware capabilities through built-in WithSecure (formerly F-Secure Business) antivirus service scanning files for malware on download and upload, supporting files of any size including those passing through Repositories Gateway or Email Protection Gateway. Multi-engine antivirus scanning integrates F-Secure/WithSecure local scanning engines and the WithSecure Atlant content-scanning platform, Check Point Threat Prevention, Trellix Malware Analysis (formerly FireEye AX) and on-demand sandbox detonation, and generic ICAP orchestrated via scan_utils framework. F-Secure/ WithSecure definition update tracking monitors AV database update status per node with repository recording attempted/successful update timestamps and upgrade telemetry. WithSecure Atlant content-scanning platform integration manages Atlant software upgrades, definition updates, licensing, and rescan of files whose scans expired or failed. The platform performs real-time scanning on upload/download, periodic rescanning of stored files, automatic signature updates, detection reporting through audit logs, and maintains current malware definitions ensuring anti-malware capabilities remain effective and up to date.
2427 Monitor/protect communications at boundaries	The Supplier shall monitor, control, and protect communications (information transmitted or received by organisational systems) at the external boundaries except as prohibited by Applicable Law and key internal boundaries of those organisational systems. This includes all staff including all remote workers to carry out their duties.	Kiteworks monitors, controls, and protects communications at boundaries through the embedded network firewall, providing hands-off security blocking all unused ports from outside traffic. The embedded Web Application Firewall (WAF) works in parallel with the network firewall as a zero-management mechanism. Email Protection Gateway (EPG) deploys between email servers and the internet, with all outbound and inbound email traffic passing through for policy evaluation and comprehensive traffic logging. Geofencing restricts sign-ins based on individual user settings, user profiles, or system-level settings applying to all users, allowing or denying access based on blocked IP addresses, blocked countries, or allowed IP addresses. These boundary protections monitor all communications at external interfaces, control access based on security policies, protect against unauthorized access and attacks, and apply equally to on-premises staff and remote workers, ensuring consistent security regardless of location.
2428 Verify/limit access to external system connections	The Supplier shall control and limit connections to external systems by an allow-list on the network boundary.	Kiteworks controls and limits external connections through comprehensive allow-listing mechanisms. IP address controls restrict administrative UI/portal access by setting an include IP list defining authorized sources. Zero Trust Mode for Intrusion Detection and Prevention implements default-deny architecture where all IP addresses are blocked by default, except those explicitly mentioned in the Allowed IP List. The zero-trust IP allow-list firewall manages whitelisted IPs, auto-generates nftables configuration, resolves services, and applies Fail2Ban integration for comprehensive zero-trust networking. These controls implement strict allow-listing at network boundaries, ensuring only pre-approved external systems can establish connections. The platform maintains and enforces these allow-lists automatically, blocking all unauthorized connection attempts while permitting legitimate business connections from approved sources. This approach provides granular control over external system access with comprehensive logging of all connection attempts.

Control	Requirement	Kiteworks Solution
2429 Verify/limit access from external system connections	The Supplier shall block unauthorised inbound connections by default. Inbound firewall rules are approved and documented by an authorised person, and include the business need within the documentation.	Kiteworks blocks unauthorized inbound connections by default through the embedded network firewall, providing hands-off security that blocks all unused ports from outside traffic. The IT department requires no additional management burden, as the firewall operates automatically. Zero Trust Mode for Intrusion Detection and Prevention implements comprehensive default-deny, blocking all IP addresses except those explicitly mentioned in the Allowed IP List. IP address controls enable blocking or explicitly allowing user sign-in or unauthenticated access from specific IP addresses or ranges. The hardened virtual appliance architecture ensures only essential services are exposed, with all other ports and services blocked by default. Firewall rules permitting specific inbound connections must be explicitly configured by authorized administrators, with changes logged in the audit system. This approach ensures all inbound connections are blocked unless specifically approved and documented for legitimate business purposes.
2501 Design for resilience	The Supplier shall design the network and information systems supporting their Functions and protect Data to be resilient to cyber security incidents and system failure. Systems shall be appropriately segregated and resource limitations mitigated.	Kiteworks designs for resilience through high-availability cluster and recovery capabilities allowing admins to trigger and monitor cluster recovery, reboot clusters, and check OS upgrade HA prechecks. Multi-location clustered storage with volume placement provides site configuration mapping hostnames to server locations, selecting available storage hosts per upload size, and exposing cluster roles and storage volumes. Tiered Internal Services with Zero-trust Principles ensure each service treats communications from other services as untrusted, with service code running in silos without direct access to data or functions within other services. This architecture provides resilience through redundancy across cluster nodes, geographic distribution of storage, service isolation preventing cascade failures, and automatic failover capabilities. System segregation through the tiered service model limits impact of any single component failure, while clustered architecture mitigates resource limitations by distributing load across multiple nodes.
2503 Resilience preparation with testing	The Supplier shall develop recovery plans for all systems that deliver Functions and protect Data. Recovery plans must also be tested at least annually with any deficiencies being recorded, risk assessed and resolved within defined timelines.	Kiteworks implements comprehensive recovery planning and testing through database backup to ACFS with retry and monitoring, creating database backups with retry logic, uploading to ACFS, tracking backup information, pruning stale backups, and restoring from subdirectories. Cluster health and precheck runner executes structured pre-check steps including roles healthy verification, volumes mounted confirmation, time sync validation, and Galera database health checks before risky operations. Database backup and EPGDB import/export enable admins to run database backups, export EPGDB archives, download them, and import EPGDB data for recovery scenarios. These capabilities support recovery plan development by providing automated backup processes, health verification procedures, and tested restore capabilities. The precheck system helps identify potential issues before they impact recovery, while backup/restore processes can be tested regularly to ensure recovery plans remain effective and deficiencies are identified for resolution.
2504 Backups	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation.	Kiteworks maintains secure backups through database backup to ACFS with retry and monitoring, creating backups with retry logic, uploading to ACFS, tracking backup info, pruning stale backups, and restoring from subdirectories. GPG-encrypted database backup and restore creates encrypted backups of EPGDB with embedded metadata, validates fingerprints against master, and performs pre-checks for disk space before restore operations. File fingerprinting using SHA3-256 creates bulk fingerprint jobs over files and surfaces summary counts for integrity tracking. These mechanisms ensure backups are accessible when needed, secured with GPG encryption meeting appropriate encryption standards, and validated through fingerprint verification and integrity checks. The automated backup processes maintain current backups of all data and configuration information required to recover operations while protecting backup data with strong encryption throughout its life cycle.

Control	Requirement	Kiteworks Solution
2505 **Resilient backups**	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.	Kiteworks provides resilient backups through cross-region replication with consistency checks implementing replication rules with thresholds/alerting, locked_locations, replication statistics, and ACFS consistency_checks/ inconsistencies with scheduled runner. Database backup to ACFS with retry and monitoring creates backups with retry, uploads to ACFS, tracks backup info, prunes stale backups, and restores from subdirectories. GPG-encrypted database backup and restore creates encrypted backups with embedded metadata, validates fingerprints, and performs pre-checks before restore. Location lock for replication maintenance allows administrators to lock/unlock storage locations during replication or migration operations and list currently locked locations. These capabilities provide encryption through GPG, integrity validation via consistency checks and fingerprints, offsite storage through cross-region replication, and support regular recovery testing through automated restore procedures with pre-checks ensuring backups remain viable and meet availability requirements.
2507 **Deny traffic by default at interfaces**	The Supplier shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.	Kiteworks implements deny-by-default traffic policies through the embedded network firewall that limits entry points to defined interfaces only, with even admins having no access to the operating system. Zero-trust network enforcement manages whitelisted IPs, auto-generates nftables configuration, resolves services, and applies Fail2Ban integration for comprehensive zero-trust networking. Firewall rules API provides uniform API to open/close ports and add inbound/outbound rules through iptables and nftables adapters. The platform blocks every network connectivity path and service by default, requiring explicit authorization to enable specific ports or services. Only connectivity paths with documented business needs are permitted, with all others blocked. The embedded firewall and zero-trust enforcement ensure traffic flow policy exceptions are actively managed, with the ability to remove access when business needs change, supporting proper change control and authorization processes.
2508 **Separate public and internal subnetworks**	The Supplier shall implement network segmentation for publicly accessible system components to ensure logical and/or physical separation from internal network components.	Kiteworks implements network segmentation through Tiered Internal Services with Zero-trust Principles where each service treats communications from other services as untrusted, with service code running in silos without direct access to data or functions within other services. Multi-location clustered storage with volume placement provides site configuration mapping hostnames to server locations, selecting available storage hosts per upload size, and exposing cluster roles and storage volumes supporting logical separation. EC proxy (edge connector) configuration enables configure, enable, disable, and tear down of EC proxy with IP range routing for edge connectivity, providing separation between external and internal components. This architecture ensures publicly accessible components like web interfaces and API endpoints are logically separated from internal components like databases and storage systems. The tiered service model enforces boundaries between public-facing and internal services, preventing direct access from external interfaces to core system components.
2509 **Managed email filtering**	The Supplier shall implement appropriate tooling or methods to detect, block and report malicious or spam emails coming into the network. Such tooling or methods may include learning capabilities for more effectively identifying legitimate communications.	Kiteworks implements comprehensive email filtering through the Email Policy Engine (EPG Rule Engine) allowing companies to define corporate rules about secure messaging gateway behavior. Rules can be defined based on recipient, sender, type of security, message data, hosts, and more to detect and block malicious or spam emails. Email protection gateway life-cycle management enables, disables, and migrates EPG subservices, pushes license and NIST rules to EPG, manages EPG tenants, toggles subservices, and monitors via Nagios. EPG Audit Logging captures all email traffic when deployed as a gateway between email servers and the internet, with all outbound and inbound traffic passing through for policy evaluation and logging, including reasons for policy-based encryption decisions. These capabilities detect malicious emails through policy rules, block spam and threats based on configured criteria, report all filtered emails through comprehensive audit logging, and can incorporate learning through policy refinement based on traffic patterns and threat intelligence.

Control	Requirement	Kiteworks Solution
2510 Diagnostic programmes	The Supplier shall check all media containing diagnostic and/or test programs for malicious code prior to use on the organisational network.	Kiteworks provides comprehensive malware checking for all content including diagnostic and test programs through antivirus scanning with bulk and on-demand triggers. Files expose AV status and can be scanned individually or in bulk at file and folder level via triggerScan/triggerBulkScan APIs. Multi-engine antivirus and content scanning provides pluggable security scan services with per-service options and per-file scan-result management with configurable ICAP/AV bypass. F-Secure/WithSecure antivirus engine updates AV definitions, schedules daily scans, manages AV proxy settings, and queries AV database/version information. These capabilities ensure any media containing diagnostic or test programs uploaded to the platform undergoes malware scanning before being made available for use. The multi-engine approach provides defense-in-depth against various malware types, while on-demand scanning allows administrators to verify content safety before deployment on organizational networks.
2512 MFA for remote maintenance activities	The Supplier shall require multi-factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Kiteworks enforces multi-factor authentication for remote maintenance through comprehensive MFA support including RADIUS protocol, PIV/CAC cards, Kiteworks native email-based OTP, Kiteworks native SMS-based OTP, and Time-based OTP following RFC 6238. Two-factor authentication toggle provides profile-level settings to require/allow 2FA for users via getTwoFactorAuth/setTwoFactorAuth configurations. The No Admin Access model ensures the only exception for system access occurs when customers involve Kiteworks Support to resolve incidents. In such cases, the customer admin temporarily opens a secure port enabling Kiteworks Support engineers to log in with short-lived access that expires, uses one-time passwords, requires permission from both Kiteworks support organization and customer system admin, and is fully logged. This ensures all remote maintenance requires MFA, sessions are properly terminated when complete, and comprehensive audit trails document all maintenance activities.
3100 Security monitoring	The Supplier shall monitor the security status of the networks and systems supporting the operation of business Functions and protection of Data in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	Kiteworks provides comprehensive security monitoring through Comprehensive Audit Logs with SIEM Feeds maintaining log data for security and compliance activities. Kiteworks automatically cleans, normalizes, standardizes, and aggregates data into a single log stream. Real-time SIEM Feed delivers the comprehensive audit log in real time to external SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk[2] via syslog, with a native Splunk App using Splunk Forwarder also provided. Security Analytics through the CISO Dashboard and Splunk App visualizations show suspicious traffic patterns including anomalies in download locations, traffic levels, user activities, and individual file activities across all data exchange channels including email, file shares, SFTP, and MFT. This continuous monitoring detects potential security problems, tracks protective measure effectiveness, and provides visibility into security status across networks and systems supporting business functions and data protection.
3101 Monitor security controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) Security events covered ii) Frequency of monitoring iii) Clearly defined roles and responsibilities iv) Escalation matrix.	Kiteworks establishes comprehensive security event monitoring through Comprehensive Audit Logs maintaining log data for all security and compliance activities. The platform automatically cleans, normalizes, standardizes, and aggregates this data into a single stream covering all security events including authentication attempts, data access, administrative changes, policy violations, and system anomalies. SIEM feeds through standard syslogs support multiple syslogs in an organization and the Splunk Universal Forwarder for real-time monitoring frequency. The persistent activity and audit log captures all events as Activities with structured per-event data, permission tagging, and filterable retrieval documenting security events covered. Role-based access to audit data defines responsibilities, with different admin roles having appropriate access to security monitoring data. The system supports escalation through alerting mechanisms and integration with organizational SIEM systems that implement escalation matrices based on event severity and type.

Control	Requirement	Kiteworks Solution
3102 Continuously monitor security controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24×7×365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24×7×365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Kiteworks enables 24×7×365 continuous security monitoring through Comprehensive Audit Logs with SIEM Feeds, helping organizations detect, analyze, and respond to security threats. SecOps teams use SIEM tools to ingest, consolidate, analyze, and report on log data from systems across the enterprise. Real-time SIEM Feed delivers comprehensive audit logs continuously to external SIEM systems like QRadar, LogRhythm, ArcSight, and Splunk via syslog and native Splunk Forwarder. Embedded Managed Detection and Response provides product-focused MDR embedded in Kiteworks Enterprise subscription with built-in threat detection and telemetry connecting to Kiteworks 24×7 headquarters security staff tightly coupled to security development engineers. This ensures continuous monitoring of all production and non-production environments, provides tools for correlation and analysis, covers all security event types, maintains real-time monitoring frequency, defines roles through integration with organizational SOC teams, and supports escalation matrices through SIEM integration and MDR services.
3103 Securing logs	The Supplier shall hold logging data securely and grant read access only to accounts with business needs. The Supplier shall protect audit tools from unauthorised access, modification and deletion. Logging data shall be retained and protected from deletion to a documented retention period, after which it shall be deleted.	Kiteworks secures logging data through Trusted Audit Logs, converting logs to various human-readable formats for administrative reporting that is filterable and searchable, and report generation/export for compliance audits. Admin Role-Based Access to Tracking Data provides separation of duties, ensuring individuals see only data appropriate based on policies and compliance regulations, restricting log access to accounts with legitimate business needs. Audit log retention and partitioning captures event_log table size, partitions, and audit log statistics for audit retention reporting, supporting documented retention periods. The platform protects audit tools from unauthorized access through role-based controls, prevents modification of log data through immutable storage, and implements retention policies that protect logs from deletion during the retention period while enabling proper deletion after expiration. This comprehensive approach ensures logging data security, access control, and life-cycle management aligned with compliance requirements.
3104 Security event triage	The Supplier shall provide evidence from their monitoring tool of security incidents to verify the reliability of identified and triggered alerts for triage.	Kiteworks provides comprehensive evidence for security event triage through Security Analytics using the CISO Dashboard and Splunk App visualizations showing suspicious traffic patterns including anomalies in download locations, traffic levels, user activities, and individual file activities across all data exchange channels. The CISO Dashboard surfaces file scan details, geo-located events, communication flows, IP-to-server mappings, and top user activities providing detailed evidence for incident verification. AI-based log analysis alerts on suspicious downloads, with Kiteworks' single stream incorporated into existing security dashboards providing immediate security benefit without adding to security team workload. These tools generate evidence including specific event details, timestamps, user identities, source locations, and activity patterns that security teams use to verify alert reliability and prioritize triage efforts. The detailed forensic data available through dashboards and exports supports incident investigation and response decision-making.
3105 Identifying security incidents	The Supplier shall contextualise alerts with knowledge of the threat and their systems, and engage Incident Response when an incident (confirmed or otherwise) is identified.	Kiteworks contextualizes security alerts through AI-based Intrusion and Anomaly Detection, maintaining an evolving library of patterns detecting suspicious activities on the network and within the virtual appliance using artificial intelligence and other technologies. Embedded Managed Detection and Response provides product-focused MDR embedded in Kiteworks Enterprise subscription with built-in threat detection and telemetry connecting to Kiteworks 24×7 headquarters security staff tightly coupled to security development engineers. Host-based intrusion detection through Wazuh/OSSEC controls the HIDS service, parses alerts, whitelists events, emails alerts, and logs failed SSH/SFTP logins as security events. These systems contextualize alerts by correlating detected patterns with known threats, system baselines, and threat intelligence. When incidents are identified, the MDR service engages incident response through direct connection to security staff who can rapidly assess and respond to threats with deep product knowledge.

Control	Requirement	Kiteworks Solution
3107 **Create, retain and correlate audit logs**	The Supplier shall generate event logs for systems that support the operation of Functions and protection of Data. The following criteria apply: i) Logs are archived for a minimum of 12 months ii) Logs capture (as a minimum) date, time (from a single NTP source), user ID, device accessed and port used iii) Logs capture key security event types (e.g. critical files accessed, user accounts generated, multiple failed login attempts, logging failures from devices, events related to systems that have an internet connection) iv) Access to modify system logs is restricted v) Logs and security event logs can be made available upon request vi) Store audit records in a repository that is part of a physically different system vii) The Supplier shall ensure that systems logs are reviewed at least weekly to identify system failures, faults, or potential security incidents and corrective actions are taken to resolve or address issues within a reasonable timeframe viii) Review, at least every 6 months the event types selected for logging purposes to ensure these still meet business requirements ix) Capture the operational status of the logging system and alert on any failures which impact the system's operational capacity.	Kiteworks generates comprehensive event logs through Comprehensive Audit Logs maintaining all security and compliance activities, automatically cleaning, normalizing, standardizing, and aggregating data into a single stream. The audit log shows Date, User, Activity, and IP Address fields with additional key-value pairs containing activity-specific metadata. Topics logged include all data actions: Views when users view files/folders, Downloads tracking all file download instances, Uploads when users upload files, and Edits when files are modified. NTP time synchronization manages NTP servers, validates lists, performs immediate sync, and migrates pool configuration, ensuring consistent timestamps from a single source. Logs capture all required security events including file access, account management, failed logins, and system events. Access to modify logs is restricted through role-based controls, logs can be exported on request via syslog or CSV, and are typically stored in external SIEM systems meeting physical separation requirements. The platform supports regular review cycles and monitors logging system operational status with alerts for failures.
3108 **Audit reduction and report generation**	The Supplier shall provide and implement an appropriate audit record reduction and report generation capability that: i) supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and ii) does not alter the original content or time ordering of audit records.	Kiteworks provides comprehensive audit reduction and reporting through Admin event export to CSV, exporting admin activities and user event logs asynchronously as CSV for compliance review. Log export feeds enable viewing logs natively in Kiteworks and exporting automatically through supported connectors via syslog for use by any SIEM or SOAR product, or via Splunk Universal Forwarder to Splunk Enterprise or Splunk Cloud. Admin reporting provides system-level reports available as default built-in or custom reports, supporting ad hoc or scheduled generation with CSV export capability. These capabilities support on-demand review by allowing instant access to filtered audit data, enable analysis through export to specialized tools, meet reporting requirements with customizable reports, and facilitate after-the-fact investigations. The system preserves original content and time ordering of audit records, with exports containing unmodified audit data maintaining chronological integrity for forensic validity.

Control	Requirement	Kiteworks Solution
3109 Integration of records with incident management	The Supplier shall integrate audit record review, triage, analysis, and reporting processes with organisational governance and incident management structure.	Kiteworks integrates audit records with incident management through Real-time SIEM Feed delivering comprehensive audit logs in real time to external SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk via syslog. Splunk Universal Forwarder log export installs/enables Splunk forwarder, configures TLS with server cert verification, and forwards audit logs to Splunk Cloud or Enterprise. Consolidation, unification, and standardization appends all activities to a single log with consistent formatting and terminology, bringing together multiple activity streams into a single stream for quick interpretation. This integration ensures audit records flow directly into organizational incident management platforms where they support automated triage, enable correlation with other security data, facilitate analysis within existing workflows, and generate reports aligned with governance requirements. The standardized format and real-time delivery enable immediate incorporation into incident response processes.
3110 Monitor alerts/ advisories and take action	The Supplier shall monitor system security alerts and advisories and take action in response.	Kiteworks monitors security alerts through comprehensive Activity and audit event logging recording all important user, data, and system activities in a single internal audit log with multiple views based on interface type and user role. HIDS intrusion detection events from the host-based intrusion detection system log into the audit trail for security monitoring. Alerting and service monitoring registers monitored services with mute toggles for admin alert management, enabling focused attention on critical alerts. Admin dashboard alert cards provide admin console cards for DB, host, EPG, email migration, and security scanning alerts, surfacing important security advisories requiring action. The platform monitors these various alert sources continuously, presents them through dashboards for admin review, logs all alerts for audit purposes, and enables administrators to take appropriate actions including investigation, remediation, or escalation based on alert severity and type.
3200 Proactive security event discovery	The Supplier shall detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of business Functions and protection of Data even when the activity evades standard signature-based security prevent/ detect solutions (or when standard solutions are not deployable).	Kiteworks proactively discovers security events through AI-based Intrusion and Anomaly Detection maintaining an evolving library of patterns detecting suspicious activities using artificial intelligence and other technologies beyond traditional signatures. Embedded Managed Detection and Response provides product-focused MDR with built-in threat detection and telemetry connecting to Kiteworks 24×7 headquarters security staff. Security Analytics visualizes suspicious traffic patterns including anomalies in download locations, traffic levels, user activities, and individual file activities across all data exchange channels. HIDS (OSSEC/Wazuh) host intrusion detection controls the service, parses alerts, whitelists events, emails alerts, and logs failed SSH/SFTP logins. These capabilities detect malicious activity through behavioral analysis, machine learning patterns, and anomaly detection that identify threats evading signature-based solutions. The multi-layered approach ensures comprehensive coverage even when standard security solutions cannot be deployed in certain areas of the infrastructure.
3201 System abnormalities for attack detection	The Supplier shall define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify. The Supplier shall take appropriate action upon identifying this behaviour.	Kiteworks defines and detects abnormal system behavior through AI-based Intrusion and Anomaly Detection maintaining an evolving library of patterns for suspicious activities using artificial intelligence. Security Analytics visualizes suspicious traffic patterns showing anomalies in download locations, traffic levels, user activities, and individual file activities. AI-powered alerts notify administrators of suspicious activities, enabling investigation before they become breaches. ABL activity baseline/user behavior analytics captures abl_active_ users (internal/external) and abl_obj_ownership snapshots with abl_stats aggregation for UBA dashboards establishing normal baselines. The platform defines abnormal behaviors including unusual geographic access patterns, atypical data volume transfers, irregular access times, abnormal user activity levels, and unexpected system resource usage. When these abnormalities are detected, the system takes action by generating alerts, logging detailed forensic data, notifying security teams, and enabling rapid investigation and response to potential threats.

Control	Requirement	Kiteworks Solution
3202 Proactive attack discovery	The Supplier shall implement reasonable and proportionate measures to detect malicious activity affecting, or with the potential to affect, the operation of Functions and protection of Data.	Kiteworks implements comprehensive measures for proactive attack discovery through Multi-engine antivirus scanning with quarantine providing AV/ATP scan counters, file quarantine/unquarantine, external scanner lock management, and pending scan handling. Advanced Threat Prevention Integration connects with commercially available ATP solutions via ICAP protocol, supporting Trellix threat detection and response products and Check Point Harmony Endpoint using native APIs. Data Loss Prevention Integration enables content monitoring and analysis, filtering data files based on corporate policy, IP protection, and compliance requirements to detect potential data exfiltration attempts. Real-time SIEM Feed delivers comprehensive audit logs to external SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk for correlation and advanced threat detection. These layered measures provide multiple detection mechanisms for malicious activity, from malware and advanced persistent threats to insider threats and data loss attempts, ensuring comprehensive coverage of potential attacks affecting business functions and data protection.
3203 Use indicators of compromise from alerts	The Supplier shall monitor system security alerts and advisories and take action in response using agreed and managed indicators of compromise.	Kiteworks monitors and responds to indicators of compromise through Embedded Managed Detection and Response where detected vulnerabilities via telemetry or threat intelligence enable development engineers to create WAF rules or code patches. Participating systems worldwide update themselves automatically like antivirus signature updates. Threat Intelligence Notifications alert administrators in real time via banners at the top of admin console pages when the Kiteworks security team identifies threats impacting systems. Trellix Helix Connect (formerly FireEye Helix) integration submits files to Trellix Malware Analysis (formerly FireEye AX) and Trellix Intelligent Virtual Execution (IVX) for on-demand detonation, tracking submission and analysis status with configurable priority and mode for IOC detection. Check Point Threat Prevention integration uploads and queries file verdicts via API with cookie-based session reuse identifying compromised files. These systems use agreed IOCs from threat intelligence sources, automated detection rules, and vendor-provided indicators to monitor for compromise, taking action through automatic updates, administrator notifications, and file quarantine when threats are identified.
3204 Presence of unauthorised system components	The Supplier shall implement proportionate measures to: i) Detect the presence of unauthorised hardware, software, and firmware components within the system using tooling ii) Take the following actions when unauthorised components are detected: disable network access by such components; isolate the components; notify systems administrators and/or security operations teams.	Kiteworks detects unauthorized system components through File Integrity Monitoring (FIM), enabling admins to inspect file integrity monitoring results for tamper detection on the host system. HIDS (OSSEC/Wazuh) host intrusion detection controls the service, parses alerts, whitelists events, emails alerts, and logs security events including unauthorized component detection. Zero Trust Mode blocks all IP addresses by default except those explicitly allowed, preventing unauthorized components from network access. IP Address Blocking Fail2Ban blocks access to ports based on IP blocks and geographic locations, reactively banning IPs with suspicious behavior. When unauthorized components are detected, the system takes action by alerting administrators through email and dashboard notifications, blocking network access through firewall rules, isolating threats through zero-trust enforcement, and logging all detection events for security operations team review. These measures ensure rapid detection and containment of unauthorized hardware, software, or firmware components.

Control	Requirement	Kiteworks Solution
4100 Response and recovery planning	The Supplier shall implement well-defined and tested incident management processes that aim to ensure continuity of business Functions and protection of Data in the event of system or service failure. Mitigation activities are designed and where possible automated to contain or limit the impact of a compromise.	Kiteworks implements comprehensive response and recovery capabilities through high-availability cluster administration reporting cluster state, performing rolling reboots and OS upgrades with per-node prechecks/postchecks and migration. Cluster high availability and recovery enables admins to trigger and monitor cluster recovery, reboot clusters, and check OS upgrade HA prechecks, ensuring service continuity. Database backup and EPGDB import/export allow admins to run database backups, export EPGDB archives, download them, and import EPGDB data for recovery scenarios. High-availability configuration for the entire Kiteworks cluster including MFT Servers provides redundancy without single points of failure. These well-defined processes ensure business continuity through automated failover, rapid recovery procedures, and comprehensive backup/restore capabilities. Mitigation activities are automated where possible, including automatic cluster recovery, health monitoring, and failover to healthy nodes, containing and limiting the impact of any system compromise or failure.
4104 Incident handling capability	The Supplier shall establish an operational incident handling capability for organisational information systems that is consistently applied across the organisation and includes: i) Adequate preparation, detection, forensic analysis, containment, recovery, and user response activities ii) Tracking, documenting, and reporting incidents to appropriate organisational officials and/or authorities iii) Sufficient rigour, intensity and scope.	Kiteworks establishes operational incident handling through a Persistent audit event log with per-event enrichment persisting events with entity resolution for files, folders, users, mail, attachments, and comments providing forensic analysis capabilities. Admin diagnostic log generation and upload generates encrypted/unencrypted diagnostic logs per host and uploads them to support for incident investigation. HIDS alert processing and quarantine ingests host-IDS alerts via ZMQ consumer, runs quarantine actions, and logs remaining alerts for containment and review. eDiscovery search and CISO asset data generate CISO asset statistics and fills eDiscovery data for investigations and compliance searches supporting forensic analysis. These capabilities provide preparation through continuous monitoring, detection via multiple security layers, forensic analysis through detailed logging, containment through quarantine and access controls, recovery through backup/restore procedures, and comprehensive tracking/documentation for reporting to officials. The system maintains sufficient rigor for enterprise incident-handling requirements.
4105 Exfiltration tests	The Supplier shall conduct data exfiltration tests at the network boundaries at least every 12 months. These tests must be conducted against both authorised and covert channels.	Kiteworks supports data exfiltration testing through Data Loss Prevention Integration connecting with commercially available DLP solutions via ICAP protocol. The Kiteworks DLP module monitors and analyzes content, filtering data files based on corporate policy, IP protection, and compliance requirements to detect exfiltration attempts. Audit log and threat reporting exports provide scheduled and on-demand export of audit logs, threat reports, and activity listings to CSV emailed to recipients for analysis of potential exfiltration patterns. Insider/outsider threat reporting covers threat report categories for insider/outsider communications with view/generate/export/delete workflows identifying potential covert channels. CISO activity dashboard with geolocation visualizes file activity as nodes/routes on maps, top senders/recipients/downloaders, and per-domain file access with manual IP/host-to-geolocation mapping revealing unusual data movements. These capabilities enable organizations to conduct exfiltration tests by monitoring both authorized channels (legitimate file transfers) and potential covert channels (unusual access patterns, geographic anomalies) at network boundaries.

Control	Requirement	Kiteworks Solution
4106 Attempted unauthorised connections from staff	The Supplier shall audit the identity of internal users associated with denied communications.	Kiteworks comprehensively audits internal user identities associated with denied communications through Failed login detection and account lockout tracking failed login attempts, locking/unlocking user accounts, and supporting admin unlock with full user identity logging. IP Address Blocking Fail2Ban shuts down failed login attempts when thresholds are reached, logging the identity of users triggering blocks. Geofencing and IP-based access restrictions with route filters reject requests outside allowed geographic regions or IP ranges, with violations logged as events including user identity information. End-user login notifications and blocked-access tracking logs user login, logout, blocked access, blocked IP, and login unlock events maintaining complete auditability of denied communications. All denied access attempts are recorded with timestamps, user identities, source IPs, attempted resources, and denial reasons, providing comprehensive audit trails for security review and compliance reporting of internal users whose communications were denied by security controls.
4202 Operation resilience for equipment	The Supplier shall assess the requirement for redundant networking and telecommunication systems to protect Functions and Data. Where required, the Supplier shall implement and protect these systems.	Kiteworks implements operational resilience through high-availability cluster administration reporting cluster state, performing rolling reboots and OS upgrades with per-node prechecks/postchecks and migration ensuring continuous service. Clustered high availability with replication config allows admins to configure cross-site replication targets, cluster settings, add/move/expand storage, run NFS mounts, and track health across hosts and services. Cross-region replication with consistency checks implements replication rules with thresholds/alerting, locked locations, replication statistics, and ACFS consistency checks with scheduled runner for data redundancy. Geo-distributed storage locations with failover use Location/Locations entities and Upload failover-to-healthy-location plus nearest-location selection modeling geo-distributed storage. These capabilities provide redundant networking through multi-node clusters, redundant telecommunications through cross-site replication, and protection of redundant systems through health monitoring and automatic failover, ensuring business functions and data remain available even during equipment failures or site outages.

[1] [sic] — this punctuation error is reproduced verbatim from the official MOD source document (Def Stan 05-138 Issue 4, Control 2210). The intended meaning is "…credentials to authorised users and processes."
[2] Product ownership has changed since these integrations were established: QRadar SaaS is now owned by Palo Alto Networks (acquisition completed August 2024); LogRhythm merged with Exabeam (completed July 2024); Splunk was acquired by Cisco (completed March 2024); ArcSight is owned by OpenText. All product names remain current and the Kiteworks integrations remain valid.

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.