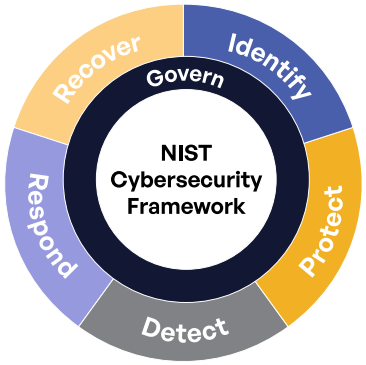
Kiteworks

GUIDE

Kiteworks' Guide to NIST CSF 2.0

Aligning the Kiteworks Secure File Sharing and Governance Platform With NIST Cybersecurity Framework (CSF) 2.0 for Enhanced Data Protection and Risk Management

Introduction



The NIST Cybersecurity Framework (CSF) 2.0 is a comprehensive set of guidelines and best practices designed to help organizations across various industries strengthen their cybersecurity posture and protect their critical assets. By adhering to these standards, organizations can effectively manage and mitigate cyber risks, safeguard sensitive data, and maintain the trust of their customers and stakeholders. The importance of following the NIST CSF 2.0 cannot be overstated. Cybersecurity incidents can have devastating consequences for organizations, resulting in financial losses, reputational damage, and legal liabilities. By adopting and implementing the framework, organizations can significantly reduce the likelihood and impact of such incidents. The NIST CSF 2.0 provides a structured approach to identifying, assessing, and managing cybersecurity risks, enabling organizations to prioritize their efforts and allocate resources effectively.

Organizations that adhere to these guidelines can improve their overall cybersecurity resilience, ensuring the confidentiality, integrity, and availability of their critical assets and data. Compliance also demonstrates a commitment to industry best practices, which enhance an organization's reputation and competitive advantage. Furthermore, by aligning with the NIST CSF 2.0, organizations can meet regulatory requirements and avoid costly penalties associated with noncompliance. The NIST CSF 2.0 is relevant to a wide range of industries, including healthcare, finance, energy, telecommunications, and government. These sectors often handle sensitive data and are subject to strict regulations, making compliance with the framework essential. The consequences of noncompliance can be severe, ranging from financial penalties and legal liabilities to reputational damage and loss of customer trust. In some cases, noncompliance can even lead to the suspension or revocation of operating licenses, severely impacting an organization's ability to conduct business.

The NIST CSF 2.0 covers a comprehensive set of cybersecurity domains and functions. It provides a holistic approach to managing cybersecurity risks, focusing on five core functions: Identify, Protect, Detect, Respond, and Recover. Additionally, the framework introduces a sixth function, Govern, which addresses the establishment of cybersecurity strategy, roles, responsibilities, and oversight. This function is crucial for integrating cybersecurity into an organization's overall risk management strategy and ensuring effective governance and accountability. Within each function, the NIST CSF 2.0 outlines specific categories and subcategories that address key areas of cybersecurity. These include asset management, access control, data security, incident response, and recovery planning. By implementing the controls and processes outlined in the framework, organizations can establish a robust cybersecurity program that addresses the full spectrum of cybersecurity risks. The NIST CSF 2.0 also emphasizes the importance of continuous improvement and adaptability. The framework provides guidance on monitoring, measuring, and improving cybersecurity performance, enabling organizations to stay ahead of emerging threats and maintain a strong security posture over time.

This guide showcases how Kiteworks can support organizations looking to be compliant with the NIST CSF 2.0 standards.

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP and FIPS-140-2 compliant file sharing and governance platform enables public entities to share sensitive information quickly and securely while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

Secure File Sharing

Kiteworks was built using secure software development best practices that align with CISA's "Principles and Approaches for Security-by-Design and Default." Kiteworks enforces least-privilege access, defense in-depth, Secure-by-Default settings, input/output validation, versioning, and industry standards like OWASP and CIS benchmarks.

Protect Unstructured Data

Kiteworks is FedRAMP Moderate Authorized and enables organizations to access and share data securely, reducing the risk of data breaches, malware attacks, and data loss.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced content governance capabilities into a single platform. Whether employees send and receive content via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks enables secure file sharing and collaboration among public entities, individuals, and third-party organizations.

The Kiteworks Platform and the NIST Cybersecurity Framework (CSF) 2.0

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
GV.OC, GV.RM, GV.RR, GV.PO, GV.OV, and GV.SC	Organizational Context: The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements —surrounding the organization's cybersecurity risk management decisions are understood Risk Management Strategy: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions Roles, Responsibilities, and Authorities: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated Policy: Organizational cybersecurity policy is established, communicated, and enforced Oversight: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy Cybersecurity Supply Chain Risk Management: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	Kiteworks supports the Govern function by providing features that help organizations manage their cybersecurity risks in the context of their mission. The platform's comprehensive security features enable organizations to safeguard sensitive data and demonstrate their commitment to cybersecurity best practices. Kiteworks offers granular user profile settings, integration with external repositories, and collaboration roles that respect access controls, ensuring stakeholders' needs for secure file sharing and access control are met. Kiteworks supports the Govern function's decisions as they are applied to the other five functions of the NIST CSF 2.0. For the Identify function, Kiteworks offers asset management capabilities, classifying content based on various conditions and managing supply chain risks. In terms of the Protect function, the platform supports authentication, access controls, least-privilege principles, data loss prevention, encryption, and audit logging. Regarding the Detect function, Kiteworks provides comprehensive logging, SIEM integration, automated notifications, and forensic data to detect anomalies and potential threats. For the Respond function, the platform's detailed logging and monitoring features enable organizations to establish and communicate appropriate risk response options. Finally, for the Recover function, Kiteworks supports high availability and disaster recovery configurations, ensuring that critical resources are available when needed. By aligning with the framework and providing features that support the Govern function across the other five functions, Kiteworks helps organizations establish, communicate, and enforce their cybersecurity risk management strategy, expectations, and policy.

IDENTIFY (ID): The organization's current cybersecurity risks are understood

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy		
ID.AM-01	Inventories of hardware managed by the organization are maintained	Kiteworks supports maintaining inventories of hardware managed by the organization through its integration with hardware security modules (HSMs) and its comprehensive logging capabilities. The platform offers integrations with Gemalto and AWS Key Management Service (AWS KMS) for secure handling and management of cryptographic keys. When hosting services on AWS cloud infrastructure, Kiteworks inherits the compliance controls from AWS's continuous audits and assessments of its underlying infrastructure, including physical and environmental security of its hardware and data centers. Additionally, Kiteworks provides a single, consolidated activity log that tracks various activities, such as logins, uploads, downloads, and administrative actions. These tracking features are complete, detailed, timely, consolidated, and standardized, enabling organizations to prove compliance to auditors, hunt for threats, mitigate attacks, and perform forensic investigations.
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	Kiteworks supports maintaining inventories of software, services, and systems managed by the organization through its secure software development life cycle (SDLC) process and comprehensive logging capabilities. The platform's SDLC process incorporates both offensive and defensive techniques, as well as best practices from OWASP, SANS Institute, CWE, and CVSS, ensuring that vulnerabilities in third-party software are tracked and addressed with timely, tested fixes. Kiteworks logs various activities related to the management of software, services, and systems, such as the addition or update of servers, external data sources, application settings, and system software updates. These logs provide a detailed inventory of the organization's managed assets, enabling effective monitoring and control.
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	The platform's layers of protection ensure that content and metadata are safeguarded from the outside world as they travel through or rest in the Private Content Network. This includes an embedded network firewall that limits entry points to defined interfaces only, an embedded web application firewall (WAF) that detects and blocks web and REST API attacks, and IP address blocking through Fail2Ban. Additionally, Kiteworks employs a zero-trust architecture with open-source library sandboxing, tiered component positioning, customer-owned keys, and file and disk double encryption. These features, combined with an intrusion detection system (IDS) and comprehensive, normalized audit logs that feed into the organization's SIEM, enable effective monitoring and control of authorized network communication and data flows.
ID.AM-04	Inventories of services provided by suppliers are maintained	The platform employs a least-privilege approach, where users are automatically assigned the minimum permissions necessary to perform their tasks, and administrators must explicitly enable elevated permissions. This ensures that access to features and resources, including those provided by suppliers, is strictly controlled and monitored. Kiteworks offers four default admin roles (System, Application, Helpdesk, and DLI) and allows for the creation of custom roles by copying and modifying existing roles. The hierarchy of admin roles enables granular control over permissions, with each permission set to no access, view only, or full access.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	The platform provides asset management for content assets by classifying them in the context of a content-based risk policy when a user requests an action on that content. The classification process takes into account various conditions, such as the folder path, specified MIP or custom sensitivity labels, file type, and creator. Organizations can assign appropriate priorities to their assets based on their sensitivity, criticality, and potential impact on the mission.
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	The platform provides asset management for content assets by classifying them based on conditions such as folder path, specified MIP or custom sensitivity labels, file type, and creator, in the context of a content-based risk policy. This classification process ensures that data and metadata inventories are accurate and up to date. Kiteworks' single, consolidated activity log captures all necessary data for compliance and audits, including date, user, activity, IP address, and additional metadata related to specific activities. The log can be searched, filtered, and sorted, allowing for granular analysis of data and metadata inventories. The platform also employs a zero-trust architecture with features such as open-source library sandboxing, tiered component positioning, customer-owned keys, file and disk double encryption, and an intrusion detection system (IDS). These features, combined with access control policies and the principle of least privilege, ensure that data and metadata inventories are protected from unauthorized access and potential breaches.
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	Offensive security measures, such as penetration testing, vulnerability scanning, and bounty hunting, proactively identify and address potential vulnerabilities before they can be exploited. Defensive security measures, including firewalls, access controls, encryption, and timely patching of software vulnerabilities, provide ongoing protection and maintain the security posture of the platform. By employing a comprehensive SDLC process that combines offensive and defensive techniques, Kiteworks enables organizations to effectively manage their systems, hardware, software, services, and data throughout their entire life cycles.
Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization		
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	The platform's development process includes ongoing automated and periodic manual penetration testing, conducted for web, server, Enterprise Connect, mobile, and desktop clients. These tests, which conform to OWASP requirements, involve sophisticated attempts to gain unauthorized access to the Kiteworks virtual appliance. Kiteworks also employs white box and black box bounty hunters, tasked with finding and reporting vulnerabilities before malicious actors can exploit them. The platform also maintains an evolving library of patterns that detect suspicious activities on the network and within the application code, including network traffic, known attack signatures, exfiltration attempts, and unauthorized code changes. When vulnerabilities are discovered, they are reported and confirmed through a strict process, and the Kiteworks development team scores them for threat level, prioritizes them against other threats, and addresses them with patches as necessary. The platform's one-click update feature allows system administrators to easily apply these patches, updating the entire solution in a single step.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	Kiteworks' security team actively participates in information-sharing forums and sources to gather the latest cyber threat intelligence, which is then used to continuously update and refine the platform's web application firewall (WAF) rules. These expert-tuned WAF rules are automatically applied to customer systems, ensuring robust protection against even the most sophisticated web and REST API attacks without requiring any maintenance on the customer's part.
ID.RA-03	Internal and external threats to the organization are identified and recorded	The platform provides a single, consolidated activity log that captures all necessary data for compliance and audits, including date, user, activity, IP address, and additional metadata related to specific activities. This log can be searched, filtered, and sorted, allowing for granular analysis of potential threats. Kiteworks also maintains an evolving library of patterns that detect suspicious activities on the network and within the application code, including network traffic, known attack signatures, exfiltration attempts, and unauthorized code changes. Kiteworks also integrates seamlessly with security information and event management (SIEM) systems, providing a clean, normalized, and standardized stream of log data that can be easily incorporated into an organization's existing security dashboards. The platform feeds log data to SIEMs in real time through standard syslogs and supports multiple syslogs and the Splunk Universal Forwarder, ensuring that organizations can effectively identify and respond to threats.
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Unlike competitors that throttle or drop logs during surges, Kiteworks captures all log data in full detail without loss. Its consolidated, searchable activity log provides a single auditable source across the system, users, files, and forms. Kiteworks automatically cleans, normalizes, and aggregates logs into a standardized stream for seamless SIEM integration and real-time threat detection. It maintains an evolving library of patterns to detect suspicious network activities, attack signatures, exfiltration attempts, and unauthorized code changes within its secure virtual appliance.
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Out of Scope
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	Comprehensive logging capabilities capture all activity data without throttling or dropping messages, ensuring a complete audit log. The consolidated, searchable activity log provides visibility across the system, users, files, and forms, streamlining risk assessment and response planning. By automatically aggregating normalized log data into a standardized stream, Kiteworks seamlessly integrates with existing SIEM tools for real-time threat monitoring and analysis. This centralized view of risk indicators empowers SecOps teams to prioritize and coordinate appropriate risk responses based on aggregated intelligence from multiple sources. Kiteworks' robust logging and SIEM integration capabilities facilitate informed decision-making and effective communication of risk mitigation strategies across the organization.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Kiteworks' consolidated activity log captures all data changes, user management actions, and configuration updates without throttling or data loss. This complete audit log allows organizations to evaluate the risk impact of any modifications across the system, users, files, folders, and forms. This centralized visibility into access control policies, permission changes, and other critical events empowers organizations to promptly identify, assess, and mitigate risks associated with system alterations.
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Kiteworks' comprehensive DevSecOps practices, including automated and manual penetration testing, as well as white and black box bounty programs, ensure vulnerabilities are identified and addressed proactively. The minimized attack surface, zero-trust architecture, and layered security controls mitigate the impact of potential vulnerabilities. Kiteworks' one-click update process streamlines the deployment of security patches and updates across the entire solution. Additionally, the intrusion detection system and comprehensive logging capabilities facilitate prompt analysis and response to disclosed vulnerabilities in coordination with customers' SIEM tools.
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Kiteworks' secure development life cycle adheres to industry frameworks like NIST CSF, incorporating supply chain risk management by documenting all open-source components and CVEs. The hardened virtual appliance is designed for deployment on customer-provided hardware or cloud infrastructure, undergoing comprehensive testing and verification processes. Kiteworks maintains ISO 27001, 27017, and 27018 certifications, and is pursuing FIPS 140-3 validation, ensuring its solutions meet stringent security standards. By thoroughly vetting hardware and software components through industry-recognized practices, Kiteworks delivers authenticated, integrity-assured solutions that enhance customers' overall risk management posture.
ID.RA-10	Critical suppliers are assessed prior to acquisition	Out of Scope
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF functions		
ID.IM-01	Improvements are identified from evaluations	Detailed audit logs provide complete visibility across all system components and communication channels, enabling thorough analysis and feedback. The consolidated, normalized log data can be seamlessly integrated with SIEM tools, empowering organizations to detect areas for enhancement based on aggregated intelligence. Kiteworks' configurable access controls, risk policies, and integrations allow organizations to implement identified improvements by tailoring the solution to their evolving needs, enabling continuous improvement cycles driven by regular evaluations and actionable insights from operational data.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Kiteworks' comprehensive design reviews, code analysis, automated testing, and penetration testing by external vendors help uncover potential vulnerabilities prior to release. Through bug bounty programs, Kiteworks engages white hat hackers to simulate advanced threat actors, further validating its security posture. All open-source components and identified CVEs are thoroughly documented for transparency. By closely collaborating with security researchers and suppliers throughout this rigorous testing process, Kiteworks gains valuable insights to drive continuous improvements to its hardened virtual appliance and layered security controls.
ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	Detailed, consolidated audit logs provide complete visibility into all system events, communication channels, and user activities. This operational data can be seamlessly integrated with existing SIEM tools for in-depth analysis and monitoring, enabling organizations to pinpoint areas for optimization based on insights gleaned from real-world usage patterns and security events. Additionally, Kiteworks' configurable access controls, risk policies, and integrations empower organizations to implement identified improvements by tailoring the solution to align with evolving operational requirements.
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Comprehensive logging features capture detailed forensic data across all system components and communication channels, providing invaluable insights for incident analysis and response planning improvement. This can be seamlessly integrated with SIEM tools through real-time syslog and Splunk feeds, enabling coordinated monitoring and alerting mechanisms. Kiteworks' automated notification and quarantine functions facilitate swift containment actions during security events.

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access		
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	Kiteworks provides robust identity and credential management capabilities that enable organizations to control and secure access for authorized users, services, and hardware with built-in authentication options as well as seamless integration with existing identity providers like LDAP, Active Directory, Azure AD, and SSO solutions. Kiteworks supports various authentication methods including credentials, certificates, multi-factor authentication, and federated identity standards. Through its granular role-based access controls and principle of least privilege, Kiteworks ensures users only have the minimum necessary permissions. Dedicated admin roles further segregate privileged access.
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	For internally managed users and credentials, Kiteworks maintains a secure repository where trusted administrators can provision new external users with restricted, least-privilege access roles. This controlled onboarding process, coupled with self-service registration for external parties, allows Kiteworks to validate identities and appropriately associate them with the necessary credentials and permissions tailored to the specific collaboration context.
PR.AA-03	Users, services, and hardware are authenticated	Kiteworks supports a wide range of authentication methods including credentials, certificates, multi-factor authentication, SAML/Kerberos SSO, OAuth, and integration with LDAP, Active Directory, and Azure AD identity providers. Kiteworks allows seamless deployment of multiple authentication types within a single instance, catering to diverse requirements. Its role-based access control model, built on the principle of least privilege, assigns granular permissions tailored to each user's authorized actions. Collaboration roles further govern access to specific files and folders based on predefined roles like Owner, Manager, and Collaborator.
PR.AA-04	Identity assertions are protected, conveyed, and verified	The platform supports various authentication methods and integrates with existing identity providers. Kiteworks employs double encryption for customer files, minimizing the attack surface and ensuring data protection even if an attacker breaches outer layers. Following zero-trust principles, internal services treat communications as untrusted, with each service running in a silo and communicating through secure channels. This approach slows down potential attacks and increases detection probability.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	The platform supports a wide range of authentication methods and integrates with existing identity providers, allowing organizations to enforce granular access control policies. Kiteworks' zero-trust architecture ensures that internal services treat communications from other services as untrusted, with each service running in a silo and communicating through secure channels. This approach enforces the principle of least privilege and separation of duties, limiting the potential impact of a compromised service. The platform also logs all changes to permissions, user management, configuration settings, servers, external data sources, and system updates, enabling regular review and auditing of access policies.
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	Kiteworks' FedRAMP systems are deployed in controlled environments with strict and audited procedures in place, including the escorting and monitoring of visitors. The platform maintains comprehensive audit logs of all physical access to FedRAMP systems, enabling organizations to track and review access events.
Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks		
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Kiteworks supports a custom banner message feature on the login page of the web application, which can be used to communicate important cybersecurity awareness and training information to personnel. Additionally, audit logs and protected folders track and store signed training materials. This allows organizations to ensure that their employees possess the necessary knowledge and skills to perform general tasks with cybersecurity risks in mind. Kiteworks follows the SANS Institute best practices to provide its personnel with deep cybersecurity training and certification, all Kiteworks developers receive thorough training on secure coding best practices, and every design and line of code undergoes rigorous automated and manual security testing to identify and remediate potential vulnerabilities.
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Kiteworks supports a custom banner message feature on the login page of the web application, which can be used to communicate important cybersecurity awareness and training information to personnel. Additionally, audit logs and protected folders track and store signed training materials. This allows organizations to ensure that their employees possess the necessary knowledge and skills to perform general tasks with cybersecurity risks in mind. Kiteworks follows the SANS Institute best practices to provide its personnel with deep cybersecurity training and certification, and all Kiteworks developers receive thorough training on secure coding best practices.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information		
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	The platform employs a multi-layered encryption approach, where files are encrypted at the file level and then encrypted again at the disk level using separate keys. Kiteworks secures data at rest via 256-bit AES, to prevent unauthorized access in storage. The combination of file-level and disk-level encryption makes it virtually impossible for unauthorized parties to decrypt and access the data. Customers also retain full control over their encryption keys, ensuring the privacy of their data and supporting compliance with privacy regulations.
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	Kiteworks secures data in transit via Transport Layer Security (TLS) 1.3 to prevent unauthorized access during transmission. TLS 1.3 is the latest version of the TLS protocol that provides enhanced security and performance improvements over its predecessor, TLS 1.2, by streamlining the handshake process, removing outdated and insecure features, and introducing new cryptographic algorithms to protect sensitive data transmitted over the internet.
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	Kiteworks' Next-gen DRM, SafeEDIT, helps organizations comply by providing a secure environment for collaborating on sensitive content. SafeEDIT allows authorized users to edit files natively in their browser, while keeping the content within the Kiteworks secure enclave. The platform streams a video rendition of the application UI to the user, eliminating content leakage risk. Kiteworks offers granular access controls and policies for all content folders, emails, connections, and functions, including location-based restrictions using IP addresses and time-based access controls that become effective after a configured amount of time has elapsed since a specific action. These access controls can be set at the individual user, user profile, or system level, ensuring the confidentiality, integrity, and availability of data-in-use.
PR.DS-11	Backups of data are created, protected, maintained, and tested	The platform allows customers to create snapshots of their storage node VMs, which capture the entire virtual computer, including code, metadata, and data, at a specific point in time. These snapshots can be securely stored and used to restore the system in the event of a disaster or data center failure, ensuring data availability and business continuity. Kiteworks can also be configured for automatic replication between storage nodes located in different data centers, providing a robust disaster recovery solution. This replication feature ensures that the storage contents remain identical across nodes, enabling the system to continue running even if one data center experiences an outage.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability		
PR.PS-01	Configuration management practices are established and applied	The platform logs various system activities, including the addition or update of servers, external data sources, application settings, and system software updates. These logs provide a detailed record of configuration changes, enabling effective monitoring and control. Kiteworks also employs an embedded network firewall and a web application firewall (WAF) that work in tandem to protect the virtual appliance from unauthorized access and intrusion attempts. The network firewall blocks all unused ports, while the WAF acts as a zero-management barrier tuned against suspicious network traffic, known attack signatures, SQL injection, exfiltration, and command and control attempts. Kiteworks issues continuous updates to address new threat patterns, which can be automatically downloaded and applied by default in non-air-gapped systems. These features, combined with the hands-off approach to firewall management, ensure that organizations can effectively establish and apply configuration management practices without adding to their IT department's workload.
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	The platform is deployed as a virtual appliance containing all necessary files and software, running securely within multiple layers of protection that minimize the attack surface. Kiteworks' SDLC process incorporates both offensive and defensive techniques, such as penetration testing, vulnerability scanning, bounty hunting, firewalls, access controls, encryption, and timely patching of software vulnerabilities. The process follows best practices from OWASP, SANS Institute, CWE, and CVSS, ensuring a comprehensive approach to software security. The platform also tracks vulnerabilities in third-party software and distributes timely, tested fixes, maintaining the security of the software stack.
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	Out of Scope
PR.PS-04	Log records are generated and made available for continuous monitoring	Kiteworks generates log records in full, ensuring that no data is lost during surges of activity. Kiteworks provides a single, consolidated activity log that can be searched, filtered, and sorted, with log entries appended immediately and available for real-time monitoring and response to emergencies, such as attacks in progress. The log records include detailed information such as date, user, activity, IP address, and additional metadata related to specific activities. Kiteworks also feeds log entries immediately to external syslogs and Splunk servers, if configured by the admin.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
PR.PS-05	Installation and execution of unauthorized software are prevented	The platform's software bill of materials is visible to administrators with System Admin privileges, ensuring transparency and control over the software components. Kiteworks employs defense-in-depth, secure-by-default settings, input/output validation, and adheres to industry standards like OWASP and CIS benchmarks. Multiple security layers, including role-based access, encryption, security reviews, penetration testing, and automated QA, defend against threats and prevent unauthorized software installation and execution. Additionally, Kiteworks restricts access to the operating system, ensuring that neither Kiteworks employees nor customers can modify the files, software, database, or operating system within the virtual appliance. This "No Admin Access" policy guarantees that the software within the virtual application is always known and vetted by Kiteworks.
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Kiteworks has integrated secure software development practices and monitors their performance throughout the software development life cycle (SDLC). The platform employs a "shift left" approach, moving testing, quality, and performance evaluation as early as possible in the development process to anticipate and address potential security vulnerabilities. Kiteworks' secure SDLC process incorporates both offensive and defensive techniques, such as penetration testing, vulnerability scanning, bounty hunting, firewalls, access controls, encryption, and timely patching of software vulnerabilities. The process follows best practices from OWASP, SANS Institute, CWE, and CVSS, ensuring a comprehensive approach to software security. The platform's development process includes security training for developers, security design reviews, and secure code reviews by security engineers. Automated testing, internal penetration testing, authenticated scanning, and bug bounty programs are conducted to identify and address vulnerabilities before they can affect customers. Ongoing activities, such as yearly external vulnerability assessments, white box analysis, customer penetration testing, tracking and fixing vulnerabilities in third-party software, and continuous development of new security features, ensure that secure software development practices are integrated and monitored throughout the SDLC
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience		
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	Kiteworks protects networks and environments from unauthorized logical access and usage through a combination of embedded network firewall, web application firewall (WAF), and secure architecture. The platform's embedded network firewall blocks all unused ports from outside traffic, while the WAF acts as a zero-management barrier tuned against suspicious network traffic, known attack signatures, SQL injection, exfiltration, and command and control attempts. Kiteworks issues continuous updates to address new threat patterns, which can be automatically downloaded and applied in non-air-gapped systems. The platform also employs strict access controls for sensitive operations, such as SSH access for support engineers, which is fully logged and requires authorization from both the customer admin and Kiteworks. Kiteworks is designed for single tenancy, ensuring that each customer's data is isolated and protected from cross-tenant bugs and attacks. Customers also retain full control over their encryption keys, preventing unauthorized access to their private content.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
PR.IR-02	The organization's technology assets are protected from environmental threats	The platform is deployed as a self-contained virtual appliance, minimizing the attack surface and ensuring that all necessary files and software are running securely within the appliance. Kiteworks' layers of protection include secure build processes, vulnerability management, minimized attack surface, perimeter protection, and a zero-trust assume-breach architecture. These layers work together to safeguard the organization's content and metadata from environmental threats as they travel through or rest in the Private Content Network. Additionally, Kiteworks supports clustering, where a set of hardened virtual appliances can be deployed in a cluster configuration, with nodes communicating using a secure cryptographic channel. This ensures continued protection and availability of technology assets even in the face of environmental disruptions.
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	The platform's multiple layers of protection, including secure build processes, vulnerability management, minimized attack surface, perimeter protection, and zero-trust assume-breach architecture, work together to ensure the resilience of the system and the protection of customer data. In addition, Kiteworks supports clustering, where a set of hardened virtual appliances can be deployed in a cluster configuration, with nodes communicating using a secure cryptographic channel. This clustering mechanism ensures high availability and resilience, allowing the system to continue operating effectively even in adverse situations. The platform also provides one-click updates that automatically update the entire solution, including the operating system, databases, web servers, and application code, in a single step. Furthermore, Kiteworks offers a secure offline update process for air-gapped deployments, ensuring that even isolated systems can maintain their resilience.
PR.IR-04	Adequate resource capacity to ensure availability is maintained	The platform is deployed as a self-contained virtual appliance that contains all the necessary files and software to run securely, minimizing the risk of resource constraints. Kiteworks also supports clustering, where a set of hardened virtual appliances can be deployed in a cluster configuration, with nodes communicating using a secure cryptographic channel. This clustering mechanism allows for scalability and high availability, ensuring that adequate resources are always available to meet the organization's needs. The platform also provides one-click updates that automatically update the entire solution, including the operating system, databases, web servers, and application code, in a single step. This streamlined update process helps maintain the system's availability by reducing the time and effort required for updates and minimizing the risk of compatibility issues.

DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events		
DE.CM-01	Networks and network services are monitored to find potentially adverse events	The platform's development process includes ongoing automated and periodic manual penetration testing, conducted for web, server, Enterprise Connect, mobile, and desktop clients, conforming to OWASP requirements. Kiteworks also employs white box and black box bounty hunters. The platform maintains an evolving library of patterns that detect suspicious activities on the network and within the application code, including network traffic, known attack signatures, exfiltration attempts, and unauthorized code changes. These patterns, along with the platform's multiple layers of security and intrusion detection tripwires, help monitor networks and network services for potentially adverse events.
DE.CM-02	The physical environment is monitored to find potentially adverse events	Kiteworks' FedRAMP systems are deployed in controlled environments with strict and audited procedures in place, including the escorting and monitoring of visitors. The platform maintains comprehensive audit logs of all physical access to FedRAMP systems, enabling organizations to track and review access events.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. Kiteworks ensures that all log entries are captured and fed to SIEM systems in real time through standard syslogs and the Splunk Universal Forwarder. This streamlined approach to log management enables organizations to identify threat patterns and potentially adverse events.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	Kiteworks supports monitoring external service provider activities and services to find potentially adverse events through its evolving library of patterns that detect suspicious activities on the network and within the application code. These patterns, which are proprietary to protect the security of the platform, are continuously updated by the Kiteworks team to proactively protect against attack vectors before they become publicly known.
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	The platform's development process includes security training for developers, security design reviews, secure code reviews, and automated testing to ensure that code changes do not introduce new security flaws. Kiteworks also conducts internal penetration testing, authenticated scanning, and bug bounty programs to identify vulnerabilities deeper in the product and address them before they can affect customers. Ongoing activities include yearly external vulnerability assessments and penetration testing, white box analysis, customer penetration testing, tracking and fixing vulnerabilities in third-party software, and continuous development of new security features. Discovered vulnerabilities are fed back to the Kiteworks development team, where they are scored for threat level, prioritized against other threats, and addressed with patches as necessary. This prioritization process ensures that critical threats are addressed promptly, with immediate updates or patches distributed to customers when warranted.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents		
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	Kiteworks supports analyzing potentially adverse events to better understand associated activities through its evolving library of patterns that detect suspicious activities on the network and within the application code. These proprietary patterns are continuously updated by the Kiteworks team to proactively protect against known and emerging attack vectors. The patterns may match various indicators, such as network traffic, known attack signatures, exfiltration attempts, command and control attempts, and unauthorized code changes. By analyzing these patterns, organizations can gain a deeper understanding of the activities associated with potentially adverse events.
DE.AE-03	Information is correlated from multiple sources	Kiteworks enables organizations to correlate information from multiple sources through its comprehensive logging capabilities and seamless integration with security information and event management (SIEM) systems. The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. This streamlined approach to log management eliminates the need for organizations to consolidate logs from different subsystems and formats before analyzing them in their SIEM tools. Kiteworks ensures that all log entries are captured and fed to SIEM systems in real time through standard syslogs and the Splunk Universal Forwarder, without any delays or throttling due to heavy traffic.
DE.AE-04	The estimated impact and scope of adverse events are understood	The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. By providing a single, standardized stream of log data, Kiteworks enables organizations to easily incorporate this information into their existing security dashboards and SIEM tools. With access to comprehensive and timely log data, organizations can leverage their SIEM tools to analyze the information, identify threat patterns, and gain a better understanding of the estimated impact and scope of adverse events. This insight allows them to make informed decisions and respond effectively to security incidents.
DE.AE-06	Information on adverse events is provided to authorized staff and tools	The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. This streamlined approach ensures that all log entries are captured and fed to SIEM systems in real time through standard syslogs and the Splunk Universal Forwarder, without any delays or throttling due to heavy traffic. Authorized staff can access the Kiteworks CISO Dashboard, which exposes audit logs and visual representations of certain activities. This integration allows authorized personnel to access and analyze information on adverse events without additional data preparation, providing an immediate security benefit.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. By providing a single, standardized stream of log data, Kiteworks allows organizations to easily incorporate this information into their existing security dashboards and SIEM tools. Once integrated, the Kiteworks log data can be combined with cyber threat intelligence and other contextual information within the organization's SIEM tools. This integration enables security teams to perform comprehensive analysis, identify threat patterns, and gain a more complete understanding of the organization's security posture.
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	Kiteworks helps organizations declare incidents when adverse events meet the defined incident criteria through its evolving library of patterns that detect suspicious activities on the network and within the application code. These proprietary patterns are continuously updated by the Kiteworks team to proactively protect against known and emerging attack vectors. The patterns may match various indicators, such as network traffic, known attack signatures, exfiltration attempts, command and control attempts, and unauthorized code changes. When an adverse event triggers one or more of these patterns and meets the organization's defined incident criteria, an incident can be declared.

RESPOND (RS): Actions regarding a detected cybersecurity incident are taken

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed		
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	SafeEDIT allows authorized external users to review and edit potentially compromised files without the sensitive content ever leaving Kiteworks' secure enclave. Comprehensive, consolidated logging captures all user activities, administrative actions, and file/folder events without throttling during surges. Granular access controls enforce least privilege by default. With identity provider integration supporting various authentication methods, including MFA and SSO, Kiteworks ensures only authorized parties can participate in incident response efforts.
RS.MA-02	Incident reports are triaged and validated	Kiteworks enables organizations to triage and validate incident reports through its comprehensive logging capabilities. The platform captures all log messages in full, without throttling the volume of logging messages during surges of activity, ensuring that no critical data is lost. All necessary data for compliance and audits is provided in a single, consolidated activity log that can be searched, filtered, and sorted. The log entries include fields such as date, user, activity, IP address, and additional metadata related to the specific activity tracked. This comprehensive logging allows organizations to quickly and effectively triage and validate incident reports. Kiteworks also appends log entries to the log immediately, enabling real-time monitoring and response to emergencies, such as attacks in progress. The platform also feeds log entries to external syslogs and Splunk servers, if configured by the admin, and appends all activities to a single log with consistent formatting and terminology.
RS.MA-03	Incidents are categorized and prioritized	The platform maintains detailed log data for security and compliance-related activities, automatically cleaning, normalizing, standardizing, and aggregating the data into a single stream. This streamlined approach ensures that all log entries are captured and fed to SIEM systems in real time through standard syslogs and the Splunk Universal Forwarder, without any delays or throttling due to heavy traffic. By providing a single, standardized stream of log data, Kiteworks allows organizations to easily incorporate this information into their existing security dashboards and SIEM tools. Once integrated, the Kiteworks log data can be analyzed within the organization's SIEM tools, enabling security teams to identify threat patterns, categorize incidents based on their severity and potential impact, and prioritize their response efforts accordingly.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
RS.MA-04	Incidents are escalated or elevated as needed	Kiteworks allows organizations to easily incorporate logs into their existing security dashboards and SIEM tools. Once integrated, the Kiteworks log data can be analyzed within the organization's SIEM tools, enabling security teams to identify threat patterns, categorize incidents based on their severity and potential impact, and prioritize their response efforts accordingly.
RS.MA-05	The criteria for initiating incident recovery are applied	Out of Scope
Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities		
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Kiteworks provides robust logging capabilities that facilitate comprehensive analysis during incident response and root cause analysis. The consolidated activity log presents a unified view of all logged activities, including administrative actions, user activities, and file/folder operations, with detailed metadata such as timestamps, IP addresses, and key-value pairs. This centralized log streamlines incident investigation, eliminating the need for additional consolidation and normalization efforts. Additionally, the real-time logging and integration with external monitoring tools enable prompt detection and response to ongoing threats or incidents.
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Kiteworks facilitates comprehensive incident data collection and preservation by maintaining a consolidated activity log that captures all relevant details of actions performed on the platform during an investigation. The log entries include essential metadata such as date, user, activity description, IP address, and additional key-value pairs specific to the logged event. Audit logs are immutable and cannot be altered, providing accurate records of investigation activities.
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	Kiteworks facilitates comprehensive incident data collection and preservation by maintaining a consolidated activity log that captures all relevant details. The log entries include essential metadata such as date, user, activity description, IP address, and additional key-value pairs specific to the logged event. This structured approach ensures the integrity and provenance of the incident data by providing a centralized, searchable, and sortable repository. Administrators can filter the log based on various criteria, including system-wide activities, administrative actions, specific users, files/folders, or forms, enabling targeted analysis and investigation.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
RS.AN-08	An incident's magnitude is estimated and validated	Kiteworks' comprehensive logging capabilities enable accurate estimation and validation of an incident's magnitude. By capturing all log messages without throttling, even during high-volume events, Kiteworks ensures that no critical data is lost, providing a complete picture of the incident. The consolidated activity log presents a unified view of all activities, including administrative actions, user activities, and file/folder operations, with detailed metadata such as timestamps, IP addresses, and key-value pairs. This centralized log, combined with real-time logging and integration with external monitoring tools, allows for prompt detection and analysis of ongoing incidents. Administrators can leverage the filtering and sorting capabilities to isolate relevant log entries, facilitating a thorough assessment of the incident's scope and impact across the system, users, and data assets.
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies		
RS.CO-02	Internal and external stakeholders are notified of incidents	Kiteworks' robust logging capabilities and seamless integration with external monitoring tools facilitate timely notification to internal and external stakeholders during incidents. By capturing all log messages in real time without throttling, Kiteworks ensures that critical incident data is available immediately. Additionally, Kiteworks can be configured to feed log entries directly to external monitoring systems, such as Splunk and syslog servers. This real-time data flow enables prompt detection and analysis of ongoing incidents, allowing organizations to swiftly notify relevant stakeholders, both internal and external, about the incident's nature, scope, and potential impact, supporting compliance with incident notification requirements.
RS.CO-03	Information is shared with designated internal and external stakeholders	Kiteworks facilitates comprehensive information sharing with designated internal and external stakeholders through its robust access control and reporting capabilities. End-users can access tracking information for specific files and folders they have permissions for, enabling visibility into who has accessed or modified the content, including both internal and external parties. Administrators have granular access permissions based on their roles, ensuring separation of duties and adherence to security and compliance policies. Kiteworks provides dashboards and reports tailored for different stakeholder groups, including system-level activity logs, storage and bandwidth consumption reports, user rankings, trend graphs, and compliance-specific summaries for regulations like GDPR and HIPAA. Additionally, administrators can access detailed activity logs for specific users, files, folders, and forms, as well as version logs for individual files, supporting thorough auditing and information sharing as required by compliance standards.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects		
RS.MI-01	Incidents are contained	Kiteworks employs a sandboxing approach to contain potential incidents and mitigate risks associated with open-source software libraries. The Kiteworks virtual appliance incorporates a sandbox environment that isolates certain externally sourced code from the main application code. This isolation prevents the sandboxed code from accessing sensitive data or functions within the primary virtual appliance, effectively containing any potential threats or vulnerabilities within the sandbox. Kiteworks also undergoes a process of removing or disabling unused portions of open-source software before incorporating them, further reducing the attack surface and limiting the potential for incidents to propagate.
RS.MI-02	Incidents are eradicated	Kiteworks implements a comprehensive approach to eradicate incidents through continuous security testing, vulnerability management, and timely patching. The platform undergoes annual external vulnerability assessments and penetration testing by third-party firms, as well as internal white box analyses to identify and address potential weaknesses. Customer-submitted penetration test results are also analyzed and addressed by the Kiteworks security team. Additionally, Kiteworks closely tracks vulnerabilities in third-party software and libraries, distributing tested and timely fixes to customers. New security features are continuously developed to reduce customer risks, and system hardening measures, such as minimizing the attack surface, implementing file integrity monitoring, and enforcing vulnerability management and patching, are employed. Discovered vulnerabilities are prioritized based on threat level, and urgent threats are addressed promptly through the distribution of updates and patches to customers, effectively eradicating the identified incidents.

RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents		
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	Out of Scope
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	Out of Scope

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	Kiteworks supports the verification of backup integrity through its snapshot and replication capabilities. Customers can create snapshots of the storage node virtual machines (VMs), capturing the entire state of the VM, including code, metadata, and data at a specific point in time. These snapshots can be safely stored and deployed on another environment in case of system failure or disaster, ensuring business continuity. Kiteworks also enables automatic replication between storage nodes for disaster recovery purposes. Customers can configure the system to maintain two storage nodes in separate data centers, with the replication feature synchronizing their contents by sending changes between them. In the event of an outage or disaster at one data center, the other storage node will have an identical and verified copy of the data, allowing for seamless failover and system recovery if properly configured for high availability.
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Out of Scope
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	Kiteworks ensures the integrity of restored assets and facilitates the restoration of systems, services, and normal operations through its snapshot and replication capabilities. Customers can create snapshots of the storage node virtual machines (VMs), capturing the complete state of the VM, including code, metadata, and data at a specific point in time. These snapshots can be deployed on a new environment, allowing for a complete and verified restoration of the system in case of disasters or failures. Additionally, Kiteworks supports automatic replication between storage nodes for disaster recovery purposes. By configuring two storage nodes in separate data centers, the replication feature synchronizes their contents, ensuring that one node has an identical copy of the other. In the event of an outage or disaster at one site, the replicated storage node can be brought online, enabling the restoration of systems, services, and data with verified integrity, and facilitating a return to normal operating status if properly configured for high availability.
RC.RP-06	The end of incident recovery is declared based on criteria, and incident related documentation is completed	Kiteworks' comprehensive logging capabilities and seamless integration with security information and event management (SIEM) systems facilitate effective incident recovery declaration and documentation. Kiteworks consolidates security and compliance-related activities into a single, normalized log stream. This streamlined approach eliminates the need for additional log consolidation and normalization efforts within the SIEM, reducing the workload on security teams. Kiteworks logs are fed to SIEM systems in real time, without dropping entries due to traffic throttling. This real-time visibility into log data enables prompt detection, analysis, and response to security incidents. With the ability to integrate Kiteworks logs into existing SIEM tools and security dashboards, organizations can leverage their established incident management processes and criteria to declare the end of incident recovery and complete related documentation seamlessly.

CSF 2.0 Core Function and Category	Control Description	Kiteworks Solution
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties		
RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Kiteworks' seamless integration with security information and event management (SIEM) systems and its real-time, consolidated logging capabilities facilitate effective communication of recovery activities and progress to designated internal and external stakeholders. By feeding comprehensive security and compliance logs into organizations' existing SIEM tools and security dashboards, Kiteworks enables centralized monitoring and reporting of recovery efforts. The single, normalized log stream provided by Kiteworks eliminates the need for additional data preparation, allowing security teams to leverage their established processes and dashboards for incident response communication. Real-time visibility into log data ensures that stakeholders receive timely updates on recovery progress and the restoration of operational capabilities. Furthermore, the ability to integrate Kiteworks logs with multiple SIEM systems within an organization enables organizations to adhere to their communication protocols and stakeholder notification requirements during recovery activities, supporting compliance with relevant standards and regulations.
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	Kiteworks' integration with security information and event management (SIEM) systems and its consolidated, real-time logging capabilities enable organizations to share public updates on incident recovery through approved methods and messaging. By leveraging existing SIEM tools and security dashboards, organizations can monitor and analyze Kiteworks' comprehensive log data alongside other security events and threat patterns. The normalized, single-stream log data provided by Kiteworks eliminates the need for additional data preparation, reducing the workload on security teams. This streamlined approach allows organizations to utilize their established processes, communication protocols, and approved messaging channels for delivering public updates on incident recovery progress. Furthermore, the ability to integrate Kiteworks logs with multiple SIEM systems within an organization ensures that relevant stakeholders have access to consistent and up-to-date information, facilitating timely and accurate public updates on incident recovery efforts.