Kiteworks

GUIDE

Kiteworks' Guide to PCI DSS 4.0

Secure Cardholder Data and Streamline Compliance: How Kiteworks' Robust Features Align With PCI DSS v4.0 Requirements

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security requirements designed to protect credit card information. Developed by major credit card companies, it applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. PCI DSS is structured around six major objectives, encompassing twelve principal requirements. These cover building and maintaining secure networks, protecting cardholder data, managing vulnerabilities, implementing strong access controls, monitoring and testing networks, and maintaining information security policies. The standard evolves to address emerging threats and industry changes.

PCI DSS v4.0 offers a new, customized approach for meeting requirements, provides enhanced flexibility for authentication and encryption methods, and emphasizes security as a continuous process. Version 4.0 maintains backwards compatibility with version 3.2.1 until March 31, 2025, allowing organizations time to transition.

Compliance with PCI DSS is crucial for several reasons. It protects sensitive cardholder data from breaches and theft, preventing fraud and identity theft. Noncompliance can result in severe financial penalties from payment card brands and acquirers, ranging from thousands to millions of dollars. Noncompliant entities may also face increased transaction fees, card replacement costs, and mandatory forensic audits. Beyond financial repercussions, noncompliance can cause significant reputational damage. Data breaches can erode customer trust, leading to lost business and long-term brand damage. In extreme cases, noncompliant entities may lose their ability to process credit card payments.

Enforcement of PCI DSS primarily falls to payment card brands (like Visa, Mastercard, American Express, Discover, and JCB) and acquiring banks.

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

This document, the Payment Card Industry Data Security Standard Requirements and Testing Procedures, consists of the 12 PCI DSS principal requirements, detailed security requirements, corresponding testing procedures, and other information pertinent to each requirement.

While PCI DSS itself is not law, some jurisdictions have incorporated its requirements into legislation, making compliance a legal obligation in those areas. The PCI Security Standards Council (PCI SSC) manages and evolves the PCI DSS. It provides standards, tools, and resources to help organizations achieve and maintain compliance, and trains qualified security assessors and scanning vendors for compliance validation.

Maintaining PCI DSS compliance is an ongoing process requiring continuous effort. Organizations must regularly assess and update their security measures, conduct vulnerability scans and penetration tests, perform internal audits, and stay informed about standard updates and emerging threats. PCI DSS is vital for protecting payment card data across the industry. Compliance is essential not only to avoid penalties and reputational damage but also to ensure the security of customers' sensitive information. While enforcement is driven by card brands and banks, the ultimate responsibility for maintaining a secure environment lies with the organizations handling cardholder data.

This guide showcases how Kiteworks can support global organizations looking to be compliant with PCI DSS v4.0. Kiteworks is a PCI DSS compliant platform.

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP Moderate 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:

Protection of 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 Enterprise platform is optionally offered with FIPS 140-2 certified encryption, and has passed the rigorous U.S. Government NIST Validation.

The Kiteworks Platform and PCI DSS v4.0

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Defined Approach Requirements	Kiteworks Solution
PCI DSS Requirement 1 focuses on installing and maintaining network security controls (NSCs) to protect cardholder data environments (CDEs). It emphasizes well-defined processes, proper configuration, and ongoing maintenance of NSCs for effective network security. The requirement is divided into five sections. Subcategory 1.1 mandates clear processes for implementing and maintaining NSCs, ensuring all parties understand their roles. Subcategory 1.2 covers NSC configuration and maintenance, requiring defined standards, change management, regular reviews, and accurate network diagrams. Subcategory 1.3 addresses restricting network access to and from the CDE, limiting traffic to necessary communications and controlling wireless network access. Subcategory 1.4 focuses on controlling connections between trusted and untrusted networks, implementing NSCs, restricting inbound traffic, and employing anti-spoofing measures. Subcategory 1.5 addresses risks from devices connecting to both untrusted networks and the CDE, mandating security controls with specific configurations and limitations on user alterability. Throughout, the requirement emphasizes documentation, regular updates, and ensuring all security measures are understood by affected parties. The goal is to create a robust, well-managed network security infrastructure that protects cardholder data from unauthorized access and potential threats.	Kiteworks provides comprehensive features that support compliance with PCI DSS Requirement 1 and its five sub-requirements. For subcategory 1.1, Kiteworks offers well-defined processes for installing and maintaining network security controls, including documented policies and clear role assignments. The platform's hardened virtual appliance, with its embedded network and web application firewalls (WAFs), addresses subcategory 1.2 by ensuring proper configuration and maintenance of network security controls. These firewalls are automatically updated to address new threats without IT intervention. Subcategory 1.3, which focuses on restricting network access to and from the CDE, is met through Kiteworks' robust access controls, IP address blocking, and geofencing features. The platform's zero-trust architecture, with its tiered component positioning and open-source library sandboxing, effectively controls network connections between trusted and untrusted networks, satisfying subcategory 1.4. For subcategory 1.5, which addresses risks from devices connecting to both untrusted networks and the CDE, Kiteworks implements strict security controls on computing devices. These include specific configuration settings, active security measures, and limitations on user alterability. The platform's single-tenant design further mitigates risks associated with multi-tenant environments. Kiteworks' comprehensive logging, role-based access controls (RBAC), content-based risk policies, and double encryption for files at rest provide additional layers of security. These features, combined with various authentication methods and the ability to restrict access based on client type and location, ensure a robust security posture that aligns with all aspects of PCI DSS Requirement 1.

Requirement 2: Apply Secure Configurations to All System Components

Defined Approach Requirements	Kiteworks Solution
Requirement 2 focuses on applying secure configurations to all system components within the cardholder data environment. Subcategory 2.1 mandates well-defined processes for implementing secure configurations, requiring documented, up-to-date security policies and operational procedures known to all affected parties. It also emphasizes clear role assignments and responsibilities. Subcategory 2.2 addresses the secure configuration and management of system components. This includes developing comprehensive configuration standards that tackle known vulnerabilities and align with industry-accepted hardening practices. It requires proper management of vendor default accounts, isolation of functions with differing security levels, and enabling only necessary services and protocols. Additionally, it stipulates secure configuration of system security parameters and encryption of non-console administrative access. Subcategory 2.3 specifically targets wireless environments connected to the CDE or transmitting account data. It requires changing all wireless vendor defaults at installation or confirming their security. This subcategory also mandates updating wireless encryption keys when personnel with key knowledge leave or when keys are potentially compromised. Collectively, these subcategories aim to minimize the attack surface by ensuring all system components, including wireless environments, are securely configured and managed throughout the cardholder data environment.	For subcategory 2.1, Kiteworks maintains comprehensive documentation and clear role assignments for security policies and operational procedures. This is evident in their hosted environment, which adheres to SOC 2 and other certifications, ensuring well-defined processes for secure configurations. Regarding subcategory 2.2, Kiteworks excels in securely configuring and managing system components. The platform is built on a hardened virtual appliance, including only necessary services. It employs a zero-trust architecture with tiered component positioning, limiting potential lateral movement by attackers. Kiteworks implements strong encryption measures, including double encryption for files at rest and support for TLS 1.3 for data in transit. Kiteworks addresses vendor default security concerns by not using default passwords and allowing administrators to set strong password policies or even abolish password usage in favor of SSO or client certificates. The admin console alerts administrators to potentially risky settings, requiring sign-off for changes, which is then documented in audit logs. Kiteworks is out of scope for subcategory 2.3 due to the absence of wireless networks in its service environment. The platform's compliance reporting features, including a consolidated activity log and risk policy framework, further support adherence to Requirement 2. These features allow for comprehensive monitoring and reporting of system activities, ensuring ongoing compliance and security.

Protect Account Data

Requirement 3: Protect Stored Account Data

Defined Approach Requirements	Kiteworks Solution
Requirement 3 focuses on protecting stored account data and comprises six essential subcategories. Subcategory 3.2 mandates minimizing account data storage through implementation of data retention and disposal policies. Subcategory 3.3 prohibits storing sensitive authentication data after authorization, with specific rules for tracking data, card verification codes, and PINs. Subcategory 3.4 addresses the display and copying of primary account numbers (PANs), requiring masking when displayed and implementing technical controls to prevent unauthorized copying during remote access. Subcategory 3.5 focuses on securing stored PANs, mandating they be rendered unreadable using methods such as one-way hashes, truncation, or strong cryptography. Subcategory 3.6 emphasizes the security of cryptographic keys used to protect stored account data. It requires restricting key access, ensuring key-encrypting keys are at least as strong as data-encrypting keys, and storing keys securely in the fewest possible locations. Lastly, subcategory 3.7 mandates comprehensive key management processes covering the entire key life cycle. This includes key generation, distribution, storage, changes, retirement, and destruction. It also requires prevention of unauthorized key substitution and formal acknowledgment of key-custodian responsibilities. Overall, Requirement 3 aims to ensure that stored account data remains protected from unauthorized access and use, employing a multi-faceted approach to data security.	Kiteworks provides robust features to support compliance with PCI DSS Requirement 3 and its subcategories. For subcategory 3.2, Kiteworks implements data retention and disposal policies, including automatic file deletion and expiration controls. The platform allows for secure deletion of data, ensuring that information is permanently removed when no longer needed. Regarding subcategory 3.3, while Kiteworks is not a PCI transaction platform, it can be used as a storage and collaborative platform for customer-uploaded data. Customers must ensure that sensitive authentication data is not stored longer than needed and Kiteworks supports this through comprehensive audit logs, secure deletion features, customer-owned keys, double encryption, and granular access controls; these tools allow customers to monitor, manage, and securely remove data as required. For subcategory 3.4, the platform implements strict access controls and permissions, including role-based access and least-privilege principles, to restrict access to full PANs. Subcategory 3.5 is addressed through Kiteworks' double encryption method. Files are encrypted at both the operating system level and the application level, ensuring that PANs are secured wherever stored. This multi-layered approach provides strong protection even if an attacker gains access to the operating system. For subcategory 3.6, Kiteworks secures cryptographic keys by allowing customers to own and control their encryption keys. This ensures that even Kiteworks staff or external actors cannot decrypt customer data without authorization. For subcategory 3.7, the platform supports key life-cycle management by providing customers with necessary information and documentation about their keys and responsibilities. Throughout these processes, Kiteworks maintains comprehensive audit logs, tracking all relevant activities and changes, which supports compliance efforts and provides transparency in data handling.

Requirement 4: Protect Cardholder Data With Strong Cryptography During Transmission Over Open, Public Networks

Defined Approach Requirements	Kiteworks Solution
Requirement 4 focuses on protecting cardholder data during transmission over open, public networks using strong cryptography. Subcategory 4.2 specifically addresses the protection of primary account numbers (PANs). It mandates implementing strong cryptography and security protocols for PAN transmission, using only trusted keys and valid certificates, and supporting only secure versions of protocols. Organizations must maintain an inventory of trusted keys and certificates and implement industry best practices for wireless networks transmitting PANs. The requirement extends to securing PANs with strong cryptography in end-user messaging technologies. It also addresses scenarios where cardholder data is received unsolicited through insecure channels, allowing organizations to either secure the channel or prevent its use for cardholder data. Requirement 4 emphasizes the crucial role of robust encryption in protecting sensitive cardholder data during transmission across various network types and communication channels.	Kiteworks provides support for Requirement 4, which focuses on protecting cardholder data during transmission. The platform offers strong cryptographic protection by supporting TLS 1.3 and 1.2, giving customers the flexibility to enable TLS 1.3 only, 1.2 only, or both, depending on their security needs. All data transmitted through Kiteworks is encrypted using TLS 1.2 or higher, ensuring a high level of security for sensitive information in transit. Kiteworks provides the infrastructure for secure transmission and key management responsibilities lie with the customer, allowing for greater control and customization of security measures.

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks From Malicious Software

Defined Approach Requirements	Kiteworks Solution
Requirement 5 focuses on protecting all systems and networks from malicious software and demands comprehensive malware protection across all systems and networks, including emerging threats like phishing attacks. Subcategories 5.2-5.4 address specific aspects of this protection. Subcategory 5.2 mandates the prevention, detection, and addressing of malware by deploying anti-malware solutions on all system components, with exceptions for low-risk systems. These solutions must detect, remove, block, or contain all known malware types, and regular evaluations of systems deemed not at risk are required. Subcategory 5.3 ensures anti-malware mechanisms are active, maintained, and monitored. This includes keeping solutions current via automatic updates, performing periodic or real-time scans or continuous behavioral analysis, addressing removable electronic media, retaining audit logs, and preventing unauthorized disabling or alteration of anti-malware mechanisms. Subcategory 5.4 introduces anti-phishing protection, requiring the implementation of processes and automated mechanisms to detect and protect against phishing attacks.	Kiteworks offers several features that support compliance with Requirement 5 and its subcategories. For subcategory 5.2, Kiteworks provides a built-in WithSecure(R) Anti-virus (AV) service as an add-on service. This AV solution scans files for malware during both upload and download processes, handling files of any size, including those passing through Enterprise Connect sources or the Email Protection Gateway (EPG). Aligning with subcategory 5.3, Kiteworks enforces anti-virus scanning on all its systems as a condition of service renewal. The platform maintains detailed logs of system activities, including virus scanning completions and failures, enhancing visibility into security operations. Administrators can configure the system to either quarantine infected files or log and alert upon detection, ensuring ongoing monitoring and maintenance. Addressing subcategory 5.4, Kiteworks supports DKIM, SPF, and DMARC protocols for customer emails. These protocols help prevent email spoofing and other email-based attacks, protecting users against phishing attempts. Kiteworks also provides robust admin roles, including a System Administrator role that can configure and maintain all aspects of the product, ensuring proper management of security features across all subcategories. Together, these features demonstrate Kiteworks' comprehensive approach to malware prevention, detection, and mitigation, supporting organizations in their efforts to comply with Requirement 5 and its subcategories.

Requirement 6: Develop and Maintain Secure Systems and Software

Defined Approach Requirements	Kiteworks Solution
Requirement 6 focuses on developing and maintaining secure systems and software and emphasizes the importance of proactive security measures throughout the software development life cycle and system maintenance process. Subcategory 6.2 addresses the secure development of bespoke and custom software, mandating industry-standard practices, regular training for development personnel, and thorough code reviews before production release. It also requires the implementation of techniques to prevent common software attacks. Subcategory 6.3 emphasizes the identification and management of security vulnerabilities. This includes using industry-recognized sources for vulnerability information, assigning risk rankings, maintaining an inventory of software components, and promptly installing security patches. Subcategory 6.4 focuses on protecting public-facing web applications against attacks. It requires regular vulnerability assessments, correction of identified vulnerabilities, and the deployment of automated technical solutions to detect and prevent web-based attacks. Subcategory 6.5 deals with secure change management for all system components. It mandates established procedures for implementing changes, including documenting the reason and security impact, obtaining approval, testing, and confirming PCI DSS requirements after significant changes. It also requires the separation of pre-production and production environments and the removal of test data before production deployment.	Kiteworks employs a comprehensive secure software development life cycle, including regular training for developers, secure coding practices, and design reviews emphasizing security, supporting subcategory 6.2. The company utilizes best practices like OWASP and implements a “shift left” approach to security. Addressing subcategory 6.3, Kiteworks maintains a continuous cycle of security testing, including internal and external vulnerability assessments. The company regularly updates its software to address known vulnerabilities, publishes CVEs, and aims to become a CVE Numbering Authority. For subcategory 6.4, Kiteworks implements a hardened virtual appliance with multiple layers of protection, including an embedded web application firewall (WAF) that detects and blocks web and REST API attacks. This aligns with the requirement to protect public-facing web applications. Regarding subcategory 6.5, Kiteworks supports secure change management through its one-click update system, which allows for cryptographic verification of updates. The company maintains separate production and development environments, implements role-based access controls (RBAC), and ensures the removal of test accounts before deployment. Kiteworks employs a comprehensive approach to secure software development and maintenance, including regular training, best practices like OWASP, continuous security testing, hardened virtual appliances with multiple layers of protection, secure change management, and strict access controls, all of which align with PCI DSS requirements for developing and maintaining secure systems and software.

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need-to-Know

Defined Approach Requirements	Kiteworks Solution
Requirement 7 focuses on restricting access to system components and cardholder data based on business need-to-know. It comprises two main subcategories: 7.2 and 7.3. Both subcategories emphasize the importance of regular reviews, appropriate access assignment, and the principle of least privilege to maintain a secure environment for cardholder data and system components. Subcategory 7.2 mandates appropriate definition and assignment of access to system components and data. It requires a defined access control model that grants access based on business needs, job classifications, and the principle of least privilege. User access, including privileged users and third-party accounts, must be regularly reviewed and approved. Application and system accounts should be managed with minimal necessary privileges and periodically reviewed. Subcategory 7.3 addresses the management of logical access through access control systems. These systems should restrict access based on a user's need-to-know, cover all system components, and enforce assigned privileges. Importantly, the access control system must be set to "deny all" by default, ensuring that access is only granted when explicitly authorized.	For subcategory 7.2, Kiteworks implements a comprehensive role-based access control (RBAC) system. This system includes predefined roles such as Owner, Manager, Collaborator, Downloader, Viewer, and Uploader, each with specific permissions aligned with job functions and the principle of least privilege. Kiteworks is designed to automatically assign users the least permissions necessary, requiring explicit admin action for elevated privileges. Addressing subcategory 7.3, Kiteworks employs a sophisticated access control system that restricts access based on user need-to-know. The platform supports various authentication methods, including multi-factor authentication (MFA) and single sign-on (SSO), and implements a zero-trust architecture where each service treats communications from other services as untrusted. Kiteworks also supports attribute-based access control (ABAC), allowing for dynamic risk policies based on content attributes, user attributes, and specific actions. Additionally, Kiteworks maintains comprehensive audit logs of all access-related activities, including permission changes, user management, and configuration modifications. This logging system supports regular reviews of user access, a key requirement of both subcategories. The platform's "deny by default, allow by exception" principle aligns perfectly with the PCI DSS requirement for access control systems to be set to "deny all" by default.

Requirement 8: Identify Users and Authenticate Access to System Components

Defined Approach Requirements	Kiteworks Solution
Requirement 8 emphasizes the importance of robust user identification and authentication practices to ensure accountability and protect against unauthorized access to sensitive data and systems. This focuses on identifying users and authenticating access to system components. Subcategory 8.2 mandates strict management of user IDs and accounts throughout their life cycle, including unique IDs for all users, controlled use of shared accounts, and prompt revocation of access for terminated users. Subcategory 8.3 establishes strong authentication practices, including multi-factor authentication (MFA), password complexity requirements, and secure storage of authentication factors. Subcategory 8.4 requires the implementation of MFA for all non-console administrative access to the cardholder data environment (CDE) and for all remote network access. Subcategory 8.5 focuses on configuring MFA systems to prevent misuse, ensuring they're not susceptible to replay attacks and can't be bypassed without proper authorization. Lastly, subcategory 8.6 addresses the management of application and system accounts, including limiting interactive use, protecting passwords from being hard-coded, and implementing periodic password changes based on risk analysis.	Kiteworks supports identifying users and authenticating access to system components. For subcategory 8.2, Kiteworks provides strict user ID management, including unique IDs for all users and controlled use of shared accounts. The platform supports various authentication methods (subcategory 8.3), including credential-based, certificate-based, and multi-factor authentication (MFA), with options for SAML 2.0 SSO, Kerberos SSO, and OAuth. Addressing subcategories 8.4 and 8.5, Kiteworks implements MFA through multiple methods such as RADIUS protocol, PIV/CAC cards, and time-based OTP. The platform allows administrators to configure and control authentication policies, ensuring MFA systems are properly implemented and secured against misuse. For subcategory 8.6, Kiteworks enables administrators to set strong password policies, including minimum length, complexity requirements, and password history. The platform also supports password expiration and enforces password changes upon first login. Throughout these processes, Kiteworks maintains comprehensive audit logs of all access-related activities, including permission changes and user management. The platform's role-based access control (RBAC) and attribute-based access control (ABAC) further enhance security by enforcing the principle of least privilege.

Requirement 9: Restrict Physical Access to Cardholder Data

Defined Approach Requirements	Kiteworks Solution
Requirement 9 emphasizes the importance of comprehensive physical security measures to protect cardholder data from unauthorized access or removal. Subcategory 9.2 mandates physical access controls to manage entry into facilities and systems containing cardholder data. This includes appropriate facility entry controls, monitoring of sensitive areas, and restrictions on publicly accessible network jacks and wireless access points. Subcategory 9.3 addresses the authorization and management of physical access for personnel and visitors. It requires procedures for identifying personnel, managing access changes, and revoking access upon termination. For visitors, it mandates authorization, escorting, and maintaining visitor logs. Subcategory 9.4 focuses on the secure storage, access, distribution, and destruction of media containing cardholder data. This includes physical security of media, classification based on data sensitivity, secure transportation, and proper destruction methods for both hard-copy and electronic media. Subcategory 9.5 deals with protecting point-of-interaction (POI) devices from tampering and unauthorized substitution. It requires maintaining a list of POI devices, periodic inspections, and training personnel to recognize and report suspicious behavior.	While physical access controls and POI devices are out of scope, Kiteworks supports compliance with subcategory 9.4. Kiteworks offers comprehensive audit logging capabilities, tracking all user activities related to data access, modification, and deletion. This provides a detailed record of all interactions with sensitive data, which can be crucial for security monitoring and incident response. The platform's secure deletion helps maintain the privacy and security of user data, aligning with PCI DSS requirements for proper data destruction.

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Defined Approach Requirements	Kiteworks Solution
Requirement 10 works to help organizations maintain a secure environment, preventing unauthorized access and ensuring compliance with PCI DSS standards. Requirement 10 of the PCI DSS focuses on the critical need to log and monitor all access to system components and cardholder data, ensuring a robust security posture against data breaches. Audit logs, which are crucial for detecting anomalies and suspicious activity, must be enabled across all system components and cardholder data environments per subcategory 10.2. These logs need to capture comprehensive details of user activities, including administrative actions and access attempts. Subcategory 10.3 focuses on maintaining the integrity of these logs. They must be protected from destruction and unauthorized modifications, with access strictly controlled. Subcategory 10.4 requires regular reviews of these logs are necessary to identify and address any anomalies, and subcategory 10.5 requires a minimum of 12 months of log history must be retained. Per subcategory 10.6, consistent time synchronization across all systems is vital to ensure accurate logging. Lastly, within subcategory 10.7, the prompt detection, reporting, and response to failures in critical security control systems are essential to prevent security lapses.	For subcategory 10.2, Kiteworks ensures that audit logs are enabled and capture all relevant activities, such as user authentication attempts, file uploads, downloads, system changes, and admin actions, all within a single, consolidated activity log. This comprehensive logging meets the requirements of detecting anomalies and supporting forensic analysis. For subcategory 10.3, Kiteworks safeguards audit logs from destruction and unauthorized modifications, ensuring that logs are protected and only accessible by those with a business need. In line with subcategory 10.4, these logs can be reviewed regularly to identify and address any suspicious activities promptly. Kiteworks also addresses subcategory 10.5 by allowing organizations to customize retention periods, ensuring audit log history is retained and accessible for at least 12 months. With regard to subcategory 10.6, Kiteworks integrates with Network Time Protocol (NTP) servers to maintain consistent time synchronization across all systems, crucial for accurate logging. Finally, under subcategory 10.7, Kiteworks' real-time log integration with SIEM tools enables immediate detection, reporting, and response to any failures of critical security control systems.

Requirement 11: Test Security of Systems and Networks Regularly

Defined Approach Requirements	Kiteworks Solution
Requirement 11 focuses on regularly testing the security of systems and networks to ensure that security controls remain effective against evolving threats. Subcategory 11.2 mandates the identification and monitoring of wireless access points, ensuring that unauthorized access points are promptly addressed. Regular internal and external vulnerability scans are required under subcategory 11.3, with a focus on identifying, prioritizing, and addressing vulnerabilities. Additionally, external and internal penetration testing must be conducted regularly to uncover and correct exploitable vulnerabilities and security weaknesses, as specified in subcategory 11.4. Subcategory 11.5 requires the deployment of intrusion detection or prevention techniques, ensuring that network intrusions and unexpected file changes are detected and responded to promptly. Finally, subcategory 11.6 mandates the use of change- and tamper-detection mechanisms to alert personnel to unauthorized modifications on payment pages, safeguarding against potential compromises. Collectively, these requirements ensure that an organization's security posture is continually assessed and strengthened, reducing the risk of data breaches and maintaining PCI DSS compliance.	Kiteworks helps organizations regularly identify and address internal and external vulnerabilities through its comprehensive logging and monitoring features supporting subcategory 11.3. These capabilities ensure that any security weaknesses within the Kiteworks environment are promptly identified and remediated, maintaining the integrity of data managed within the platform. Supporting compliance with subcategory 11.5, Kiteworks employs advanced intrusion detection and prevention techniques, monitoring all network traffic at critical points within the system. This includes detecting unauthorized access attempts, monitoring for unexpected file changes, and ensuring that personnel are alerted to potential compromises. Additionally, Kiteworks' built-in file integrity monitoring tools ensure that any unauthorized modifications to critical files are detected and addressed promptly. While subcategories 11.2, 11.4, and 11.6 are outside of Kiteworks' scope due to the platform's focus and architecture, Kiteworks continues to provide value by securing the data and activities within its environment. This supports an organization's overall PCI DSS compliance efforts by addressing key security requirements in its domain.

Maintain an Information Security Policy

Requirement 12: Support Information Security With Organizational Policies and Programs

Defined Approach Requirements	Kiteworks Solution
PCI DSS Requirement 12 focuses on supporting information security with organizational policies and programs. It ensures that organizations have comprehensive, up-to-date policies and procedures in place to maintain a strong security posture and effectively manage PCI DSS compliance. Subcategory 12.1 mandates a comprehensive information security policy that is known, current, and regularly reviewed. Subcategory 12.2 requires defined and implemented acceptable use policies for end-user technologies. Subcategory 12.3 focuses on formally identifying, evaluating, and managing risks to the cardholder data environment. Subcategories 12.4 and 12.5 address PCI DSS compliance management and scope documentation. Subcategory 12.6 emphasizes ongoing security awareness education for all personnel. Subcategory 12.7 requires personnel screening to reduce insider threat risks. Subcategories 12.8 and 12.9 deal with managing risks associated with third-party service provider relationships and ensuring these providers support customers' PCI DSS compliance. Finally, Subcategory 12.10 requires an immediate response to suspected and confirmed security incidents that could impact the cardholder data environment. This includes maintaining an incident response plan, regular testing and updates, and designated personnel for 24/7 incident response.	The platform's Advanced Governance license enables compliance administrators to define and enforce dynamic risk policies based on content assets, user attributes, and specific actions, aligning with subcategories 12.3 and 12.5. Kiteworks is designed according to industry best practices and standards, such as the NIST Cybersecurity Framework, supporting the Identify, Protect, Detect, Respond, and Recover functions. This comprehensive approach aids in maintaining a strong security posture across multiple aspects of operations, as required by subcategory 12.1. The platform's control settings allow for granular management of access controls and data protection measures, implementing the principle of least privilege. This supports subcategory 12.4 on managing PCI DSS compliance. Kiteworks also provides comprehensive audit logging and configuration management capabilities, which are crucial for incident response planning as outlined in subcategory 12.10. Kiteworks' single-tenant architecture and customer-owned encryption keys ensure data privacy and security, supporting overall compliance efforts. The platform's intrusion and anomaly detection capabilities, along with regular reviews of cryptographic modules and ciphers, further enhance security measures. While certain aspects of Requirement 12 are out of Kiteworks' scope (subcategories 12.2, 12.6, 12.7, 12.8, and 12.9), the platform's features contribute to an organization's ability to maintain and enforce information security policies in compliance with PCI DSS requirements.