Kiteworks

LEITFADEN

Kiteworks-Leitfaden zu PCI DSS 4.0

Sichere Karteninhaberdaten und vereinfachte Compliance: Wie die leistungsstarken Funktionen von Kiteworks mit den Anforderungen von PCI DSS v4.0 übereinstimmen

Einführung

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein umfassender Katalog von Sicherheitsanforderungen, der zum Schutz von Kreditkarteninformationen entwickelt wurde. Erarbeitet von führenden Kreditkartenunternehmen, gilt er für alle Beteiligten im Zahlungskartenprozess, einschließlich Händler, Verarbeiter, Acquirer, Herausgeber und Dienstleister. Der PCI DSS ist um sechs Hauptziele strukturiert, die zwölf grundlegende Anforderungen umfassen. Diese decken den Aufbau und die Wartung sicherer Netzwerke, den Schutz von Karteninhaberdaten, das Management von Schwachstellen, die Implementierung starker Zugangskontrollen, die Überwachung und das Testen von Netzwerken sowie die Aufrechterhaltung von Richtlinien zur Informationssicherheit ab. Der Standard entwickelt sich weiter, um auf aufkommende Bedrohungen und Branchenveränderungen zu reagieren.

PCI DSS v4.0 bietet einen neuen, individuellen Ansatz zur Erfüllung der Anforderungen, ermöglicht eine erhöhte Flexibilität bei Authentifizierungs- und Verschlüsselungsmethoden und betont Sicherheit als kontinuierlichen Prozess. Version 4.0 bleibt bis zum 31. März 2025 rückwärtskompatibel mit Version 3.2.1 und gibt Organisationen Zeit für den Übergang.

Die Einhaltung der PCI DSS ist aus mehreren Gründen entscheidend. Sie schützt sensible Karteninhaberdaten vor Verstößen und Diebstahl, verhindert Betrug und Identitätsdiebstahl. Nichteinhaltung kann zu schwerwiegenden finanziellen Strafen von Zahlungskartenmarken und Acquirern führen, die von Tausenden bis zu Millionen Dollar reichen. Nicht konforme Einheiten können auch mit erhöhten Transaktionsgebühren, Kartenersatzkosten und obligatorischen forensischen Audits konfrontiert werden. Über finanzielle Folgen hinaus kann Nichteinhaltung erheblichen Reputationsschaden verursachen. Datenpannen können das Kundenvertrauen untergraben, was zu Geschäftsverlusten und langfristigen Markenschäden führt. In extremen Fällen können nicht konforme Einheiten ihre Fähigkeit zur Verarbeitung von Kreditkartenzahlungen verlieren.

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.

Die Durchsetzung von PCI DSS obliegt hauptsächlich den Kreditkartenunternehmen (wie Visa, Mastercard, American Express, Discover und JCB) und den erwerbenden Banken. Obwohl PCI DSS selbst kein Gesetz ist, haben einige Rechtsordnungen seine Anforderungen in die Gesetzgebung aufgenommen, was die Einhaltung in diesen Gebieten zu einer rechtlichen Verpflichtung macht. Der PCI Security Standards Council (PCI SSC) verwaltet und entwickelt den PCI DSS weiter. Er stellt Standards, Tools und Ressourcen zur Verfügung, um Organisationen dabei zu helfen, die Compliance zu erreichen und aufrechtzuerhalten, und bildet qualifizierte Sicherheitsbewerter und Scan-Anbieter für die Compliance-Validierung aus.

Die Einhaltung der PCI DSS-Norm ist ein fortlaufender Prozess, der kontinuierliche Anstrengungen erfordert. Organisationen müssen regelmäßig ihre Sicherheitsmaßnahmen bewerten und aktualisieren, Schwachstellenscans und Penetrationstests durchführen, interne Audits ausführen und sich über Standardaktualisierungen und neu auftretende Bedrohungen informieren. PCI DSS ist von entscheidender Bedeutung für den Schutz von Zahlungskartendaten in der Branche. Die Einhaltung ist nicht nur wichtig, um Strafen und Reputationsschäden zu vermeiden, sondern auch, um die Sicherheit der sensiblen Informationen der Kunden zu gewährleisten. Obwohl die Durchsetzung von den Kartenmarken und Banken vorangetrieben wird, liegt die letztendliche Verantwortung für die Aufrechterhaltung einer sicheren Umgebung bei den Organisationen, die Kartendaten verarbeiten.

Diese Anleitung zeigt, wie Kiteworks globale Unternehmen dabei unterstützen kann, die Anforderungen der PCI DSS v4.0 zu erfüllen. Kiteworks ist eine PCI DSS-konforme Plattform.

Die Kiteworks-Plattform für sicheres Filesharing und Governance

Die Kiteworks-Plattform für sicheres Filesharing und Governance, die FedRAMP Moderate und FIPS 140-2 entspricht, ermöglicht es öffentlichen Einrichtungen, sensible Informationen schnell und sicher zu teilen, während sie volle Transparenz und Kontrolle über ihre Filesharing-Aktivitäten behalten.* Die Kiteworks-Plattform bietet:

Schutz unstrukturierter Daten

Kiteworks ist FedRAMP Moderate autorisiert und ermöglicht es Unternehmen, Daten sicher zu zugreifen und zu teilen, wodurch das Risiko von Datenschutzverstößen, Malware-Angriffen und Datenverlust reduziert wird.

Governance und Compliance

Kiteworks reduziert Compliance-Risiken und -Kosten, indem fortgeschrittene Funktionen zur Inhalts-Governance auf einer einzigen Plattform konsolidiert werden. Ob Mitarbeiter Inhalte via E-Mail, Filesharing, automatisiertem Dateiaustausch, APIs oder Web-Formularen senden und empfangen, alles ist abgedeckt.

Einfachheit und Benutzerfreundlichkeit

Kiteworks ermöglicht sicheres Filesharing und Zusammenarbeit zwischen öffentlichen Einrichtungen, Einzelpersonen und Drittorganisationen.

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

Die Kiteworks-Plattform und PCI DSS v4.0

Errichten und Warten eines sicheren Netzwerks und Systems

Anforderung 1: Installation und Wartung von Netzwerksicherheitskontrollen

Definierte Anforderungen an den Ansatz	Kiteworks Solution
PCI DSS-Anforderung 1 konzentriert sich auf die Installation und Wartung von Netzwerksicherheitskontrollen (NSCs), um Karteninhaberdatenumgebungen (CDEs) zu schützen. Sie betont gut definierte Prozesse, eine angemessene Konfiguration und die kontinuierliche Wartung von NSCs für eine effektive Netzwerksicherheit. Die Anforderung ist in fünf Abschnitte unterteilt. Unterkategorie 1.1 fordert klare Prozesse für die Implementierung und Wartung von NSCs, um sicherzustellen, dass alle Parteien ihre Rollen verstehen. Unterkategorie 1.2 befasst sich mit der Konfiguration und Wartung von NSCs und erfordert definierte Standards, Änderungsmanagement, regelmäßige Überprüfungen und genaue Netzwerkdiagramme. Unterkategorie 1.3 behandelt die Einschränkung des Netzwerkzugriffs auf und von der CDE, begrenzt den Verkehr auf notwendige Kommunikationen und kontrolliert den Zugriff auf drahtlose Netzwerke. Unterkategorie 1.4 konzentriert sich auf die Kontrolle von Verbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken, implementiert NSCs, beschränkt eingehenden Verkehr und verwendet Anti-Spoofing-Maßnahmen. Unterkategorie 1.5 befasst sich mit Risiken von Geräten, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit der CDE verbunden sind, und fordert Sicherheitskontrollen mit spezifischen Konfigurationen und Einschränkungen der Benutzeranpassbarkeit. 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.

Anforderung 2: Sichere Konfigurationen für alle Systemkomponenten anwenden

Defined Approach Requirements	Kiteworks Lösung
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. Diese Unterkategorien zielen gemeinsam darauf ab, die Angriffsfläche zu minimieren, indem sichergestellt wird, dass alle Systemkomponenten, einschließlich drahtloser Umgebungen, sicher konfiguriert und im gesamten Karteninhaberdatenumfeld verwaltet werden.	Für Unterkategorie 2.1 hält Kiteworks umfassende Dokumentationen und klare Rollenzuweisungen für Sicherheitsrichtlinien und Betriebsverfahren bereit. Dies zeigt sich in ihrer gehosteten Umgebung, die den SOC 2 und anderen Zertifizierungen entspricht und gut definierte Prozesse für sichere Konfigurationen gewährleistet. In Bezug auf Unterkategorie 2.2 zeichnet sich Kiteworks durch die sichere Konfiguration und Verwaltung von Systemkomponenten aus. Die Plattform basiert auf einer gehärteten virtuellen Appliance und beinhaltet nur notwendige Dienste. Sie verwendet eine Zero-Trust-Architektur mit abgestuften Komponentenpositionierungen, um potenzielle seitliche Bewegungen von Angreifern zu begrenzen. Kiteworks implementiert starke Verschlüsselungsmaßnahmen, einschließlich doppelter Verschlüsselung für Dateien im ruhenden Zustand und Unterstützung für TLS 1.3 für Daten während der Übertragung. Kiteworks begegnet Sicherheitsbedenken bezüglich Standardkonfigurationen von Anbietern, indem es keine Standardpasswörter verwendet und Administratoren ermöglicht, starke Passwortrichtlinien festzulegen oder sogar die Passwortnutzung zugunsten von SSO oder Client-Zertifikaten abzuschaffen. Die Administrationskonsole warnt Administratoren vor potenziell riskanten Einstellungen und verlangt eine Genehmigung für Änderungen, die dann in Prüfprotokollen dokumentiert wird. Kiteworks ist für Unterkategorie 2.3 außerhalb des Anwendungsbereichs, aufgrund der Abwesenheit von drahtlosen Netzwerken in seiner Serviceumgebung. Die Compliance-Berichtsfunktionen der Plattform, einschließlich eines konsolidierten Aktivitätsprotokolls und eines Risikopolitikrahmens, unterstützen weiterhin die Einhaltung von Anforderung 2. Diese Funktionen ermöglichen eine umfassende Überwachung und Berichterstattung von Systemaktivitäten, um fortlaufende Compliance und Sicherheit zu gewährleisten.

Schützen Sie Kontodaten

Anforderung 3: Gespeicherte Kontodaten schützen

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 3 konzentriert sich auf den Schutz gespeicherter Kontodaten und umfasst sechs wesentliche Unterkategorien. Unterkategorie 3.2 fordert die Minimierung der Speicherung von Kontodaten durch die Implementierung von Datenhaltungs- und Entsorgungsrichtlinien. Unterkategorie 3.3 verbietet die Speicherung sensibler Authentifizierungsdaten nach der Autorisierung, mit spezifischen Regeln für Tracking-Daten, Kartenprüfnummern und PINs. Unterkategorie 3.4 befasst sich mit der Anzeige und dem Kopieren von Primärkontonummern (PANs) und fordert eine Maskierung bei der Anzeige sowie technische Kontrollen, um unbefugtes Kopieren während des Fernzugriffs zu verhindern. Unterkategorie 3.5 konzentriert sich auf die Sicherung gespeicherter PANs und schreibt vor, dass sie unlesbar gemacht werden müssen, unter Verwendung von Methoden wie Einweg-Hashes, Trunkierung oder starker Kryptografie. Unterkategorie 3.6 betont die Sicherheit von kryptografischen Schlüsseln, die zum Schutz gespeicherter Kontodaten verwendet werden. Sie fordert eine Einschränkung des Schlüsselzugriffs, stellt sicher, dass Schlüsselverschlüsselungsschlüssel mindestens so stark sind wie Datenverschlüsselungsschlüssel, und verlangt, dass Schlüssel sicher an möglichst wenigen Orten aufbewahrt werden. Zuletzt verlangt Unterkategorie 3.7 umfassende Schlüsselverwaltungsprozesse, die den gesamten Lebenszyklus des Schlüssels abdecken. Dies umfasst die Schlüsselgenerierung, -verteilung, -speicherung, -änderungen, -außerbetriebnahme und -zerstörung. Es erfordert auch die Verhinderung unautorisierten Schlüsselaustauschs und eine formelle Anerkennung der Verantwortlichkeiten des Schlüsselverwahrers. Insgesamt zielt Anforderung 3 darauf ab, sicherzustellen, dass gespeicherte Kontodaten vor unbefugtem Zugriff und Gebrauch geschützt bleiben, indem ein mehrschichtiger Ansatz für die Datensicherheit angewendet wird.	Kiteworks bietet robuste Funktionen zur Unterstützung der Einhaltung von PCI DSS-Anforderung 3 und deren Unterkategorien. Für Unterkategorie 3.2 implementiert Kiteworks Datenhaltungs- und Entsorgungsrichtlinien, einschließlich automatischer Dateilöschung und Ablaufsteuerungen. Die Plattform ermöglicht eine sichere Löschung von Daten und stellt sicher, dass Informationen dauerhaft entfernt werden, wenn sie nicht mehr benötigt werden. Bezüglich Unterkategorie 3.3, obwohl Kiteworks keine PCI-Transaktionsplattform ist, kann es als Speicher- und Kollaborationsplattform für von Kunden hochgeladene Daten verwendet werden. Kunden müssen sicherstellen, dass sensible Authentifizierungsdaten nicht länger als nötig gespeichert werden, und Kiteworks unterstützt dies durch umfassende Prüfprotokolle, sichere Löschfunktionen, kundeneigene Schlüssel, doppelte Verschlüsselung und granulare Zugriffskontrollen; diese Tools ermöglichen es Kunden, Datenüberwachung, -verwaltung und -sicherung nach Bedarf durchzuführen. Für Unterkategorie 3.4 implementiert die Plattform strenge Zugriffskontrollen und Berechtigungen, einschließlich rollenbasierter Zugriffe und Prinzipien der geringsten Berechtigungen, um den Zugriff auf vollständige PANs zu beschränken. Unterkategorie 3.5 wird durch die doppelte Verschlüsselungsmethode von Kiteworks adressiert. Dateien werden sowohl auf Betriebssystemebene als auch auf Anwendungsebene verschlüsselt, um sicherzustellen, dass PANs überall dort, wo sie gespeichert sind, gesichert sind. Dieser mehrschichtige Ansatz bietet starken Schutz, selbst wenn ein Angreifer Zugang zum Betriebssystem erlangt. Für Unterkategorie 3.6 sichert Kiteworks kryptografische Schlüssel, indem Kunden ermöglicht wird, ihre Verschlüsselungsschlüssel zu besitzen und zu kontrollieren. Dies stellt sicher, dass selbst Kiteworks-Mitarbeiter oder externe Akteure Kundendaten ohne Autorisierung nicht entschlüsseln können. Für Unterkategorie 3.7 unterstützt die Plattform das Schlüssellebenszyklusmanagement, indem Kunden mit notwendigen Informationen und Dokumentationen über ihre Schlüssel und Verantwortlichkeiten versorgt werden. Im Rahmen dieser Prozesse erstellt Kiteworks umfassende Audit-Protokolle, die alle relevanten Aktivitäten und Änderungen verfolgen, was die Compliance-Bemühungen unterstützt und Transparenz im Umgang mit Daten bietet.

Anforderung 4: Schutz von Karteninhaberdaten mit starker Kryptographie bei der Übertragung über offene, öffentliche Netzwerke

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 4 konzentriert sich auf den Schutz von Kartendaten während der Übertragung über offene, öffentliche Netzwerke mittels starker Kryptografie. Unterkategorie 4.2 befasst sich speziell mit dem Schutz von Primärkontonummern (PANs). Sie fordert die Implementierung starker Kryptografie und Sicherheitsprotokolle für die Übertragung von PANs, die Verwendung von ausschließlich vertrauenswürdigen Schlüsseln und gültigen Zertifikaten und die Unterstützung von nur sicheren Versionen von Protokollen. Organisationen müssen ein Inventar von vertrauenswürdigen Schlüsseln und Zertifikaten pflegen und branchenübliche Best Practices für drahtlose Netzwerke, die PANs übertragen, implementieren. Die Anforderung erstreckt sich auf die Sicherung von PANs mit starker Kryptografie in Endbenutzer-Nachrichtentechnologien. Sie behandelt auch Szenarien, in denen Kartendaten unaufgefordert über unsichere Kanäle empfangen werden, und ermöglicht Organisationen, entweder den Kanal zu sichern oder dessen Nutzung für Kartendaten zu verhindern. Anforderung 4 betont die entscheidende Rolle robuster Verschlüsselung beim Schutz sensibler Kartendaten während der Übertragung über verschiedene Netzwerktypen und Kommunikationskanäle.	Kiteworks unterstützt Anforderung 4, die sich auf den Schutz von Karteninhaberdaten während der Übertragung konzentriert. Die Plattform bietet starken kryptografischen Schutz, indem TLS 1.3 und 1.2 unterstützt werden, was den Kunden die Flexibilität gibt, nur TLS 1.3, nur 1.2 oder beides zu aktivieren, je nach ihren Sicherheitsbedürfnissen. Alle durch Kiteworks übertragenen Daten werden mit TLS 1.2 oder höher verschlüsselt, was ein hohes Maß an Sicherheit für sensible Informationen während der Übertragung gewährleistet. Kiteworks stellt die Infrastruktur für die sichere Übertragung bereit und die Verantwortung für das Schlüsselmanagement liegt beim Kunden, was eine größere Kontrolle und Anpassung der Sicherheitsmaßnahmen ermöglicht.

Ein Vulnerability-Management-Programm pflegen

Anforderung 5: Schutz aller Systeme und Netzwerke vor Schadsoftware

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 5 konzentriert sich auf den Schutz aller Systeme und Netzwerke vor bösartiger Software und fordert einen umfassenden Malware-Schutz über alle Systeme und Netzwerke hinweg, einschließlich aufkommender Bedrohungen wie Phishing-Angriffe. Die Unterkategorien 5.2-5.4 behandeln spezifische Aspekte dieses Schutzes. Unterkategorie 5.2 verlangt die Prävention, Erkennung und Behebung von Malware durch den Einsatz von Anti-Malware-Lösungen auf allen Systemkomponenten, mit Ausnahmen für Systeme mit geringem Risiko. Diese Lösungen müssen alle bekannten Malware-Typen erkennen, entfernen, blockieren oder eindämmen, und regelmäßige Bewertungen von Systemen, die als nicht gefährdet gelten, sind erforderlich. Unterkategorie 5.3 stellt sicher, dass Anti-Malware-Mechanismen aktiv, gewartet und überwacht werden. Dies umfasst das Aktuellhalten der Lösungen durch automatische Updates, das Durchführen periodischer oder Echtzeit-Scans oder kontinuierliche Verhaltensanalysen, das Ansprechen von wechselbaren elektronischen Medien, das Beibehalten von Audit-Protokollen und das Verhindern einer unbefugten Deaktivierung oder Änderung von Anti-Malware-Mechanismen. Unterkategorie 5.4 führt den Schutz vor Phishing ein, der die Implementierung von Prozessen und automatisierten Mechanismen zur Erkennung und zum Schutz vor Phishing-Angriffen erfordert.	Kiteworks bietet mehrere Funktionen, die die Einhaltung von Anforderung 5 und deren Unterkategorien unterstützen. Für Unterkategorie 5.2 bietet Kiteworks einen integrierten WithSecure(R) Anti-Virus (AV)-Dienst als Zusatzservice an. Diese AV-Lösung scannt Dateien auf Malware während des Hoch- und Herunterladeprozesses und verarbeitet Dateien jeder Größe, einschließlich derer, die über Enterprise Connect-Quellen oder das Email Protection Gateway (EPG) übertragen werden. Im Einklang mit Unterkategorie 5.3 setzt Kiteworks die Durchführung von Antivirus-Scans auf allen seinen Systemen als Bedingung für die Verlängerung des Dienstes durch. Die Plattform hält detaillierte Protokolle der Systemaktivitäten fest, einschließlich der Abschlüsse und Fehlschläge von Virenscans, was die Transparenz in den Sicherheitsoperationen erhöht. Administratoren können das System so konfigurieren, dass infizierte Dateien entweder in Quarantäne verschoben oder bei Erkennung protokolliert und alarmiert werden, was eine kontinuierliche Überwachung und Wartung gewährleistet. Im Rahmen der Unterkategorie 5.4 unterstützt Kiteworks die Protokolle DKIM, SPF und DMARC für Kunden-E-Mails. Diese Protokolle helfen dabei, E-Mail-Spoofing und andere auf E-Mails basierende Angriffe zu verhindern und schützen die Nutzer vor Phishing-Versuchen. Kiteworks bietet ebenfalls robuste Admin-Rollen an, einschließlich einer Rolle als Systemadministrator, der alle Aspekte des Produkts konfigurieren und warten kann, um eine angemessene Verwaltung der Sicherheitsfunktionen über alle Unterkategorien hinweg sicherzustellen. Gemeinsam demonstrieren diese Funktionen den umfassenden Ansatz von Kiteworks zur Malware-Prävention, -Erkennung und -Minderung und unterstützen Organisationen in ihren Bemühungen, die Anforderung 5 und ihre Unterkategorien einzuhalten.

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Software

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 6 konzentriert sich auf die Entwicklung und Wartung sicherer Systeme und Software und betont die Bedeutung proaktiver Sicherheitsmaßnahmen während des gesamten Softwareentwicklungslebenszyklus und des Systemwartungsprozesses. Unterkategorie 6.2 befasst sich mit der sicheren Entwicklung von maßgeschneiderter und individueller Software, fordert branchenübliche Praktiken, regelmäßige Schulungen für Entwicklerpersonal und gründliche Code-Überprüfungen vor der Produktionsfreigabe. Es erfordert auch die Implementierung von Techniken zur Verhinderung gängiger Softwareangriffe. Unterkategorie 6.3 betont die Identifizierung und Verwaltung von Sicherheitsanfälligkeiten. Dies umfasst die Nutzung branchenanerkannter Quellen für Anfälligkeitsinformationen, die Zuweisung von Risikostufen, die Aufrechterhaltung eines Inventars von Softwarekomponenten und die umgehende Installation von Sicherheitspatches. Unterkategorie 6.4 konzentriert sich auf den Schutz öffentlich zugänglicher Webanwendungen vor Angriffen. Sie erfordert regelmäßige Schwachstellenbewertungen, die Korrektur identifizierter Schwachstellen und den Einsatz automatisierter technischer Lösungen zur Erkennung und Verhinderung webbasierter Angriffe. Unterkategorie 6.5 befasst sich mit sicherem Änderungsmanagement für alle Systemkomponenten. Sie schreibt festgelegte Verfahren für die Implementierung von Änderungen vor, einschließlich der Dokumentation des Grundes und der Sicherheitsauswirkungen, der Einholung von Genehmigungen, Tests und der Bestätigung der PCI DSS-Anforderungen nach signifikanten Änderungen. Sie erfordert auch die Trennung von Vorproduktions- und Produktionsumgebungen sowie die Entfernung von Testdaten vor der Produktionsbereitstellung.	Kiteworks setzt einen umfassenden sicheren Softwareentwicklungslebenszyklus ein, der regelmäßige Schulungen für Entwickler, sichere Codierungspraktiken und Designüberprüfungen mit Schwerpunkt auf Sicherheit umfasst, was die Unterstützung der Unterkategorie 6.2 unterstützt. Das Unternehmen nutzt Best Practices wie OWASP und implementiert einen “Shift-Left”-Ansatz zur Sicherheit. Im Hinblick auf die Unterkategorie 6.3 unterhält Kiteworks einen kontinuierlichen Zyklus von Sicherheitstests, einschließlich interner und externer Schwachstellenbewertungen. Das Unternehmen aktualisiert seine Software regelmäßig, um bekannte Schwachstellen anzugehen, veröffentlicht CVEs und zielt darauf ab, eine CVE-Nummernbehörde zu werden. Für Unterkategorie 6.4 implementiert Kiteworks eine gehärtete virtuelle Appliance mit mehreren Schutzschichten, einschließlich einer eingebetteten Web Application Firewall (WAF), die Web- und REST-API-Angriffe erkennt und blockiert. Dies entspricht der Anforderung, öffentlich zugängliche Webanwendungen zu schützen. Bezüglich Unterkategorie 6.5 unterstützt Kiteworks sicheres Änderungsmanagement durch sein Ein-Klick-Update-System, das die kryptografische Überprüfung von Updates ermöglicht. Das Unternehmen unterhält separate Produktions- und Entwicklungs-Umgebungen, implementiert rollenbasierte Zugriffskontrollen (RBAC) und gewährleistet die Entfernung von Testkonten vor dem Einsatz. Kiteworks verfolgt einen umfassenden Ansatz zur sicheren Softwareentwicklung und -wartung, einschließlich regelmäßiger Schulungen, Best Practices wie OWASP, kontinuierlicher Sicherheitstests, gehärteter virtueller Appliances mit mehreren Schutzschichten, sicherem Änderungsmanagement und strengen Zugriffskontrollen, die alle mit den PCI DSS-Anforderungen für die Entwicklung und Wartung sicherer Systeme und Software übereinstimmen.

Implementieren Sie starke Zugriffskontrollmaßnahmen

Anforderung 7: Beschränken Sie den Zugriff auf Systemkomponenten und Karteninhaberdaten nach dem geschäftlichen Erfordernis zu wissen

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 7 konzentriert sich auf die Einschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten basierend auf dem geschäftlichen Bedarf zu wissen. Sie umfasst zwei Hauptunterkategorien: 7.2 und 7.3. Beide Unterkategorien betonen die Bedeutung regelmäßiger Überprüfungen, angemessener Zugriffsvergabe und des Prinzips der geringsten Rechte, um eine sichere Umgebung für Karteninhaberdaten und Systemkomponenten zu gewährleisten. Unterkategorie 7.2 fordert eine angemessene Definition und Zuweisung von Zugriff auf Systemkomponenten und Daten. Sie verlangt ein definiertes Zugriffskontrollmodell, das Zugriff basierend auf geschäftlichen Anforderungen, Stellenklassifizierungen und dem Prinzip der geringsten Rechte gewährt. Der Zugriff von Benutzern, einschließlich privilegierter Benutzer und Konten Dritter, muss regelmäßig überprüft und genehmigt werden. Anwendungs- und Systemkonten sollten mit minimal notwendigen Rechten verwaltet und periodisch überprüft werden. Unterkategorie 7.3 befasst sich mit der Verwaltung des logischen Zugriffs durch Zugangskontrollsysteme. Diese Systeme sollten den Zugang basierend auf dem Informationsbedarf des Benutzers einschränken, alle Systemkomponenten abdecken und die zugewiesenen Privilegien durchsetzen. Wichtig ist, dass das Zugangskontrollsystem standardmäßig auf „Alles verweigern“ gesetzt ist, um sicherzustellen, dass der Zugang nur gewährt wird, wenn er ausdrücklich autorisiert ist.	Für Unterkategorie 7.2 implementiert Kiteworks ein umfassendes rollenbasiertes Zugriffskontrollsystem (RBAC). Dieses System umfasst vordefinierte Rollen wie Eigentümer, Manager, Mitarbeiter, Downloader, Betrachter und Uploader, jeweils mit spezifischen Berechtigungen, die auf die Arbeitsfunktionen und das Prinzip der geringsten Rechte abgestimmt sind. Kiteworks ist so konzipiert, dass Benutzern automatisch die geringsten notwendigen Berechtigungen zugewiesen werden, wobei eine explizite Admin-Aktion für erweiterte Privilegien erforderlich ist. Im Hinblick auf Unterkategorie 7.3 setzt Kiteworks ein ausgeklügeltes Zugriffskontrollsystem ein, das den Zugang basierend auf dem Bedarf des Benutzers einschränkt. Die Plattform unterstützt verschiedene Authentifizierungsmethoden, einschließlich Zwei-Faktor-Authentifizierung (2FA) und Single Sign-On (SSO), und implementiert eine zero-trust-Architektur, bei der jeder Dienst die Kommunikation von anderen Diensten als nicht vertrauenswürdig behandelt. Kiteworks unterstützt auch eine attributbasierte Zugriffskontrolle (ABAC), die dynamische Risikopolitiken basierend auf Inhaltsattributen, Benutzerattributen und spezifischen Aktionen ermöglicht. Zusätzlich führt Kiteworks umfassende Audit-Logs aller zugriffsbezogenen Aktivitäten, einschließlich Berechtigungsänderungen, Benutzerverwaltung und Konfigurationsmodifikationen. Dieses Protokollierungssystem unterstützt regelmäßige Überprüfungen des Benutzerzugriffs, eine Schlüsselanforderung beider Unterkategorien. Das Prinzip „standardmäßig verweigern, ausnahmsweise erlauben“ von Kiteworks passt perfekt zur PCI DSS-Anforderung, dass Zugriffskontrollsysteme standardmäßig auf „alles verweigern“ eingestellt sein müssen.

Anforderung 8: Benutzer identifizieren und Zugriff auf Systemkomponenten authentifizieren

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 8 betont die Bedeutung robuster Praktiken zur Identifizierung und Authentifizierung von Benutzern, um Verantwortlichkeit zu gewährleisten und den Schutz vor unbefugtem Zugriff auf sensible Daten und Systeme zu sichern. Dies konzentriert sich auf die Identifizierung von Benutzern und die Authentifizierung des Zugriffs auf Systemkomponenten. Unterkategorie 8.2 fordert eine strenge Verwaltung von Benutzer-IDs und -Konten während ihres gesamten Lebenszyklus, einschließlich eindeutiger IDs für alle Benutzer, kontrollierter Verwendung von gemeinsam genutzten Konten und sofortiger Zugriffsentzug für ausgeschiedene Benutzer. Unterkategorie 8.3 etabliert starke Authentifizierungspraktiken, einschließlich Zwei-Faktor-Authentifizierung (2FA), Anforderungen an die Passwortkomplexität und sichere Speicherung von Authentifizierungsfaktoren. Unterkategorie 8.4 verlangt die Implementierung von 2FA für alle nicht-konsolenbasierten administrativen Zugriffe auf die Umgebung mit Karteninhaberdaten (CDE) und für allen Fernnetzzugriff. Unterkategorie 8.5 konzentriert sich auf die Konfiguration von 2FA-Systemen, um Missbrauch zu verhindern, und stellt sicher, dass sie nicht anfällig für Replay-Angriffe sind und nicht ohne angemessene Autorisierung umgangen werden können. Zuletzt behandelt Unterkategorie 8.6 das Management von Anwendungs- und Systemkonten, einschließlich der Einschränkung interaktiver Nutzung, dem Schutz von Passwörtern vor hartkodierter Speicherung und der Implementierung periodischer Passwortänderungen basierend auf Risikoanalysen.	Kiteworks unterstützt die Identifizierung von Benutzern und die Authentifizierung des Zugriffs auf Systemkomponenten. Für Unterkategorie 8.2 bietet Kiteworks ein strenges Benutzer-ID-Management, einschließlich eindeutiger IDs für alle Benutzer und kontrollierter Nutzung von gemeinsam genutzten Konten. Die Plattform unterstützt verschiedene Authentifizierungsmethoden (Unterkategorie 8.3), einschließlich kennwortbasierter, zertifikatbasierter und Multi-Faktor-Authentifizierung (MFA), mit Optionen für SAML 2.0 SSO, Kerberos SSO und OAuth. Kiteworks setzt MFA durch verschiedene Methoden wie das RADIUS-Protokoll, PIV/CAC-Karten und zeitbasierte OTPs um. Die Plattform ermöglicht es Administratoren, Authentifizierungsrichtlinien zu konfigurieren und zu steuern, um sicherzustellen, dass MFA-Systeme ordnungsgemäß implementiert und gegen Missbrauch gesichert sind. Für die Unterkategorie 8.6 ermöglicht Kiteworks Administratoren, starke Passwortrichtlinien festzulegen, einschließlich Mindestlänge, Komplexitätsanforderungen und Passwortverlauf. Die Plattform unterstützt auch das Ablaufen von Passwörtern und erzwingt Passwortänderungen beim ersten Login. Im Rahmen dieser Prozesse führt Kiteworks umfassende Prüfprotokolle aller zugriffsbezogenen Aktivitäten, einschließlich Änderungen der Berechtigungen und Benutzerverwaltung, durch. Die rollenbasierte Zugriffskontrolle (RBAC) und attributbasierte Zugriffskontrolle (ABAC) der Plattform verbessern die Sicherheit weiter, indem sie das Prinzip der geringsten Rechte durchsetzen.

Anforderung 9: Beschränken Sie den physischen Zugang zu Karteninhaberdaten

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 9 betont die Bedeutung umfassender physischer Sicherheitsmaßnahmen zum Schutz von Karteninhaberdaten vor unbefugtem Zugriff oder Entfernung. Unterkategorie 9.2 fordert physische Zugangskontrollen, um den Zutritt zu Einrichtungen und Systemen, die Karteninhaberdaten enthalten, zu verwalten. Dies umfasst angemessene Eintrittskontrollen für Einrichtungen, Überwachung sensibler Bereiche und Einschränkungen für öffentlich zugängliche Netzwerkdosen und drahtlose Zugangspunkte. Unterkategorie 9.3 befasst sich mit der Autorisierung und Verwaltung des physischen Zugangs für Personal und Besucher. Sie verlangt Verfahren zur Identifizierung des Personals, zur Verwaltung von Zugangsänderungen und zur Aufhebung des Zugangs bei Beendigung des Arbeitsverhältnisses. Für Besucher werden Autorisierung, Begleitung und das Führen von Besucherprotokollen vorgeschrieben. Unterkategorie 9.4 konzentriert sich auf die sichere Aufbewahrung, den Zugriff, die Verteilung und die Vernichtung von Medien, die Kartendaten enthalten. Dies umfasst die physische Sicherheit der Medien, die Klassifizierung basierend auf der Datensensibilität, den sicheren Transport und die ordnungsgemäßen Vernichtungsmethoden für sowohl in Papierform als auch elektronische Medien. Unterkategorie 9.5 befasst sich mit dem Schutz von Point-of-Interaction (POI)-Geräten vor Manipulation und unbefugtem Austausch. Sie erfordert die Führung einer Liste der POI-Geräte, regelmäßige Inspektionen und die Schulung des Personals, um verdächtiges Verhalten zu erkennen und zu melden.	Während physische Zugangskontrollen und POI-Geräte nicht im Fokus stehen, unterstützt Kiteworks die Einhaltung der Unterkategorie 9.4. Kiteworks bietet umfassende Fähigkeiten für Audit-Protokolle, die alle Benutzeraktivitäten im Zusammenhang mit Datenzugriff, -änderung und -löschung verfolgen. Dies stellt eine detaillierte Aufzeichnung aller Interaktionen mit sensiblen Daten bereit, die für die Sicherheitsüberwachung und Reaktion auf Vorfälle entscheidend sein kann. Die sichere Löschfunktion der Plattform hilft, die Privatsphäre und Sicherheit der Benutzerdaten zu wahren und entspricht den PCI DSS-Anforderungen für eine ordnungsgemäße Datenvernichtung.

Regelmäßige Überwachung und Prüfung von Netzwerken

Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 10 hilft Organisationen dabei, eine sichere Umgebung aufrechtzuerhalten, um unbefugten Zugriff zu verhindern und die Einhaltung der PCI-DSS-Standards zu gewährleisten. Anforderung 10 des PCI DSS konzentriert sich auf die kritische Notwendigkeit, alle Zugriffe auf Systemkomponenten und Karteninhaberdaten zu protokollieren und zu überwachen, um eine robuste Sicherheitsposition gegen Datenpannen zu gewährleisten. Audit-Protokolle, die für die Erkennung von Anomalien und verdächtigen Aktivitäten entscheidend sind, müssen gemäß Unterkategorie 10.2 in allen Systemkomponenten und Umgebungen mit Karteninhaberdaten aktiviert werden. Diese Protokolle müssen umfassende Details der Benutzeraktivitäten erfassen, einschließlich administrativer Aktionen und Zugriffsversuche. Unterkategorie 10.3 konzentriert sich darauf, die Integrität dieser Protokolle zu wahren. Sie müssen vor Zerstörung und unbefugten Änderungen geschützt werden, wobei der Zugriff streng kontrolliert wird. Unterkategorie 10.4 erfordert regelmäßige Überprüfungen dieser Protokolle, um Anomalien zu identifizieren und anzugehen, und Unterkategorie 10.5 verlangt, dass mindestens 12 Monate der Protokollhistorie aufbewahrt werden müssen. Gemäß Unterkategorie 10.6 ist eine konsistente Zeitsynchronisation über alle Systeme hinweg entscheidend, um eine genaue Protokollierung zu gewährleisten. Zuletzt ist innerhalb der Unterkategorie 10.7 die schnelle Erkennung, Meldung und Reaktion auf Ausfälle in kritischen Sicherheitskontrollsystemen wesentlich, um Sicherheitslücken zu verhindern.	Für Unterkategorie 10.2 stellt Kiteworks sicher, dass Prüfprotokolle aktiviert sind und alle relevanten Aktivitäten erfassen, wie Benutzerauthentifizierungsversuche, Dateiuploads, -downloads, Systemänderungen und Admin-Aktionen, alles innerhalb eines einzigen, konsolidierten Aktivitätsprotokolls. Diese umfassende Protokollierung erfüllt die Anforderungen zur Erkennung von Anomalien und unterstützt die forensische Analyse. Für Unterkategorie 10.3 schützt Kiteworks Prüfprotokolle vor Zerstörung und unbefugten Änderungen, um sicherzustellen, dass die Protokolle geschützt sind und nur Personen mit einem geschäftlichen Bedarf zugänglich sind. Im Einklang mit Unterkategorie 10.4 können diese Protokolle regelmäßig überprüft werden, um verdächtige Aktivitäten umgehend zu identifizieren und anzugehen. Kiteworks adressiert auch Unterkategorie 10.5, indem Organisationen die Möglichkeit gegeben wird, die Aufbewahrungszeiträume anzupassen, um sicherzustellen, dass die Historie der Prüfprotokolle für mindestens 12 Monate aufbewahrt und zugänglich ist. Im Hinblick auf Unterkategorie 10.6 integriert Kiteworks mit Network Time Protocol (NTP)-Servern, um eine konsistente Zeitsynchronisation über alle Systeme hinweg zu gewährleisten, was für eine genaue Protokollierung entscheidend ist. Abschließend ermöglicht unter Unterkategorie 10.7 die Echtzeit-Log-Integration von Kiteworks mit SIEM-Tools die sofortige Erkennung, Berichterstattung und Reaktion auf jegliche Ausfälle kritischer Sicherheitskontrollsysteme.

Anforderung 11: Regelmäßige Sicherheitsprüfungen von Systemen und Netzwerken

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
Anforderung 11 konzentriert sich auf die regelmäßige Überprüfung der Sicherheit von Systemen und Netzwerken, um sicherzustellen, dass die Sicherheitskontrollen effektiv gegen sich entwickelnde Bedrohungen bleiben. Unterkategorie 11.2 fordert die Identifizierung und Überwachung von drahtlosen Zugangspunkten, um sicherzustellen, dass nicht autorisierte Zugangspunkte umgehend behandelt werden. Regelmäßige interne und externe Schwachstellenscans sind unter Unterkategorie 11.3 erforderlich, mit einem Fokus auf die Identifizierung, Priorisierung und Behebung von Schwachstellen. Zusätzlich müssen regelmäßig externe und interne Penetrationstests durchgeführt werden, um ausnutzbare Schwachstellen und Sicherheitslücken aufzudecken und zu korrigieren, wie in Unterkategorie 11.4 spezifiziert. Unterkategorie 11.5 erfordert den Einsatz von Intrusion-Detection- oder -Prevention-Techniken, um sicherzustellen, dass Netzwerkeindringungen und unerwartete Dateiänderungen schnell erkannt und darauf reagiert wird. Schließlich fordert Unterkategorie 11.6 den Einsatz von Änderungs- und Manipulationserkennungsmechanismen, um das Personal über unautorisierte Modifikationen auf Zahlungsseiten zu informieren und so vor potenziellen Kompromittierungen zu schützen. Insgesamt stellen diese Anforderungen sicher, dass die Sicherheitslage einer Organisation kontinuierlich bewertet und gestärkt wird, wodurch das Risiko von Datenpannen verringert und die Einhaltung der PCI DSS gewährleistet wird.	Kiteworks unterstützt Unternehmen dabei, regelmäßig interne und externe Schwachstellen durch seine umfassenden Protokollierungs- und Überwachungsfunktionen zu identifizieren und zu beheben, die die Unterkategorie 11.3 unterstützen. Diese Fähigkeiten stellen sicher, dass alle Sicherheitsschwächen innerhalb der Kiteworks-Umgebung umgehend identifiziert und behoben werden, um die Integrität der innerhalb der Plattform verwalteten Daten zu wahren. Zur Unterstützung der Einhaltung der Unterkategorie 11.5 setzt Kiteworks fortschrittliche Techniken zur Erkennung und Prävention von Eindringlingen ein, indem sämtlicher Netzwerkverkehr an kritischen Punkten innerhalb des Systems überwacht wird. Dies umfasst die Erkennung von unautorisierten Zugriffsversuchen, die Überwachung auf unerwartete Dateiänderungen und die Sicherstellung, dass das Personal über potenzielle Kompromisse informiert wird. Zusätzlich gewährleisten die integrierten Tools zur Überwachung der Dateiintegrität von Kiteworks, dass jegliche unautorisierte Modifikationen an kritischen Dateien umgehend erkannt und behoben werden. Während die Unterkategorien 11.2, 11.4 und 11.6 aufgrund des Schwerpunkts und der Architektur der Plattform außerhalb des Geltungsbereichs von Kiteworks liegen, bietet Kiteworks weiterhin einen Mehrwert, indem es die Daten und Aktivitäten innerhalb seiner Umgebung sichert. Dies unterstützt die Bemühungen eines Unternehmens um die Einhaltung der PCI DSS-Anforderungen insgesamt, indem es wichtige Sicherheitsanforderungen in seinem Bereich adressiert.

Pflegen Sie eine Richtlinie zur Informationssicherheit

Anforderung 12: Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme

Festgelegte Anforderungen an den Ansatz	Kiteworks Lösung
PCI DSS-Anforderung 12 konzentriert sich auf die Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme. Sie stellt sicher, dass Organisationen umfassende, aktuelle Richtlinien und Verfahren haben, um eine starke Sicherheitsposition aufrechtzuerhalten und die PCI DSS-Compliance effektiv zu verwalten. Unterkategorie 12.1 fordert eine umfassende Informationssicherheitsrichtlinie, die bekannt, aktuell und regelmäßig überprüft wird. Unterkategorie 12.2 verlangt definierte und implementierte Richtlinien für die akzeptable Nutzung von Endbenutzertechnologien. Unterkategorie 12.3 konzentriert sich auf die formelle Identifizierung, Bewertung und Steuerung von Risiken für die Umgebung der Karteninhaberdaten. Die Unterkategorien 12.4 und 12.5 befassen sich mit dem Management der PCI DSS-Compliance und der Dokumentation des Geltungsbereichs. Unterkategorie 12.6 betont die fortlaufende Sensibilisierung aller Mitarbeiter für Sicherheitsbewusstsein. Unterkategorie 12.7 erfordert ein Screening des Personals, um Risiken durch Insider-Bedrohungen zu reduzieren. Die Unterkategorien 12.8 und 12.9 befassen sich mit dem Management von Risiken, die mit Beziehungen zu Dienstleistern von Drittparteien verbunden sind, und stellen sicher, dass diese Anbieter die PCI DSS-Compliance der Kunden unterstützen. Schließlich erfordert die Unterkategorie 12.10 eine sofortige Reaktion auf vermutete und bestätigte Sicherheitsvorfälle, die die Umgebung der Karteninhaberdaten beeinträchtigen könnten. Dies umfasst die Aufrechterhaltung eines Vorfallsreaktionsplans, regelmäßige Tests und Aktualisierungen sowie benanntes Personal für die 24/7-Vorfallsreaktion.	Die Advanced-Governance-Lizenz der Plattform ermöglicht es Compliance-Administratoren, dynamische Risikorichtlinien basierend auf Inhaltsressourcen, Benutzerattributen und spezifischen Aktionen zu definieren und durchzusetzen, in Übereinstimmung mit den Unterkategorien 12.3 und 12.5. Kiteworks ist gemäß branchenüblichen Best Practices und Standards konzipiert, wie dem NIST Cybersecurity Framework, und unterstützt die Funktionen Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Dieser umfassende Ansatz hilft dabei, eine starke Sicherheitsposition in mehreren Aspekten des Betriebs aufrechtzuerhalten, wie es die Unterkategorie 12.1 fordert. Die Steuerungseinstellungen der Plattform ermöglichen eine granulare Verwaltung von Zugriffskontrollen und Datenschutzmaßnahmen, indem das Prinzip der geringsten Rechte umgesetzt wird. Dies unterstützt die Unterkategorie 12.4 bei der Verwaltung der PCI DSS-Compliance. Kiteworks bietet auch umfassende Möglichkeiten für Audit-Logging und Konfigurationsmanagement, die für die Planung der Incident Response, wie in Unterkategorie 12.10 dargelegt, entscheidend sind. Die Single-Tenant-Architektur von Kiteworks und die vom Kunden besessenen Verschlüsselungsschlüssel gewährleisten Datenschutz und Sicherheit und unterstützen die allgemeinen Compliance-Bemühungen. Die Fähigkeiten der Plattform zur Erkennung von Eindringlingen und Anomalien, zusammen mit regelmäßigen Überprüfungen der kryptografischen Module und Cipher, verstärken die Sicherheitsmaßnahmen weiter. Während bestimmte Aspekte der Anforderung 12 außerhalb des Geltungsbereichs von Kiteworks liegen (Unterkategorien 12.2, 12.6, 12.7, 12.8 und 12.9), tragen die Funktionen der Plattform dazu bei, dass eine Organisation in der Lage ist, Informations-Sicherheitsrichtlinien in Übereinstimmung mit den PCI DSS-Anforderungen zu pflegen und durchzusetzen.

Die auf dieser Seite bereitgestellten Informationen stellen keine Rechtsberatung dar und sind auch nicht als solche gedacht. Alle Informationen, Inhalte und Materialien auf dieser Seite dienen ausschließlich allgemeinen Informationszwecken. Informationen auf dieser Website stellen möglicherweise nicht die aktuellsten rechtlichen oder anderen Informationen dar. Zusatzoptionen sind in diesem Leitfaden enthalten und werden benötigt, um die Compliance zu unterstützen.

Kiteworks

Copyright © 2024 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.