Kiteworks

GUIDE

Guide de Kiteworks sur PCI DSS 4.0

Sécuriser les données des détenteurs de carte et simplifier la conformité : Comment les fonctionnalités robustes de Kiteworks s'alignent sur les exigences de la norme PCI DSS v4.0

Introduction

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un ensemble de mesures de sécurité conçu pour protéger les informations des cartes de crédit. Développée par les principales compagnies de cartes de crédit, elle s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, y compris les commerçants, les processeurs, les acquéreurs, les émetteurs et les prestataires de services. Le PCI DSS est structuré autour de six objectifs majeurs, comprenant douze exigences principales. Ces dernières couvrent la construction et le maintien de réseaux sécurisés, la protection des données des titulaires de carte, la gestion des vulnérabilités, la mise en œuvre de contrôles d'accès rigoureux, la surveillance et le test des réseaux, et le maintien des politiques de sécurité de l'information. La norme évolue pour répondre aux menaces émergentes et aux changements dans l'industrie.

La version 4.0 de PCI DSS propose une nouvelle approche personnalisée pour répondre aux exigences, offre une plus grande flexibilité pour les méthodes d'authentification et de chiffrement, et souligne la sécurité comme un processus continu. La version 4.0 reste compatible avec la version 3.2.1 jusqu'au 31 mars 2025, donnant ainsi aux organisations le temps de faire la transition.

La conformité avec le PCI DSS est cruciale pour plusieurs raisons. Elle protège les données sensibles des titulaires de carte contre les violations et le vol, prévenant ainsi la fraude et le vol d'identité. Le non-respect peut entraîner de lourdes pénalités financières de la part des marques de cartes de paiement et des acquéreurs, allant de milliers à des millions de dollars. Les entités non conformes peuvent également faire face à des frais de transaction accrus, des coûts de remplacement de cartes et des audits forensiques obligatoires. Au-delà des répercussions financières, le non-respect peut causer un dommage réputationnel significatif. Les violations de données peuvent éroder la confiance des clients, entraînant une perte d'affaires et des dommages à long terme pour la marque. Dans les cas extrêmes, les entités non conformes peuvent perdre leur capacité à traiter les paiements par carte de crédit.

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.

L'application des normes PCI DSS incombe principalement aux marques de cartes de paiement (telles que Visa, Mastercard, American Express, Discover et JCB) et aux banques acquéreuses. Bien que le PCI DSS ne soit pas une loi en soi, certaines juridictions ont intégré ses exigences dans leur législation, rendant la conformité obligatoire dans ces régions. Le Conseil des normes de sécurité PCI (PCI SSC) gère et fait évoluer le PCI DSS. Il fournit des normes, des outils et des ressources pour aider les organisations à atteindre et à maintenir la conformité, et forme des évaluateurs de sécurité qualifiés et des fournisseurs de scan pour la validation de la conformité.

Maintenir la conformité PCI DSS est un processus continu qui nécessite un effort constant. Les organisations doivent régulièrement évaluer et mettre à jour leurs mesures de sécurité, réaliser des scans de vulnérabilité

et des tests de pénétration, effectuer des audits internes et rester informées des mises à jour des normes et des menaces émergentes. Le PCI DSS est essentiel pour protéger les données des cartes de paiement dans l'industrie. La conformité est cruciale non seulement pour éviter les pénalités et les dommages à la réputation, mais aussi pour garantir la sécurité des informations sensibles des clients. Bien que l'application soit pilotée par les marques de cartes et les banques, la responsabilité ultime de maintenir un environnement sécurisé incombe aux organisations qui traitent les données des titulaires de carte.

Ce guide met en avant comment Kiteworks peut accompagner les organisations internationales souhaitant être conformes à PCI DSS v4.0. Kiteworks est une plateforme conforme à PCI DSS.

La plateforme de partage de fichiers sécurisé et de gouvernance Kiteworks

La plateforme de partage de fichiers et de gouvernance conforme à FedRAMP Moderate et FIPS 140-2 de Kiteworks permet aux entités publiques de partager des informations sensibles rapidement et en toute sécurité tout en conservant une visibilité et un contrôle complets sur leurs activités de partage de fichiers. La plateforme Kiteworks offre :

Protection des données non structurées

Kiteworks est autorisé FedRAMP Moderate et permet aux organisations d'accéder et de partager des données de manière sécurisée, réduisant ainsi les risques de violations de données, d'attaques par malware et de pertes de données.

Gouvernance et conformité

Kiteworks réduit les risques et les coûts de conformité en consolidant des fonctions avancées de gouvernance de contenu dans une seule plateforme. Que les employés envoient et reçoivent du contenu par e-mail, partage de fichiers, transfert automatique de fichiers, API ou formulaires Web, tout est pris en charge.

Simplicité et facilité d'utilisation

Kiteworks permet le partage sécurisé de fichiers et la collaboration entre les entités publiques, les individus et les organisations tierces.

*La plateforme d'entreprise Kiteworks est proposée en option avec un chiffrement certifié FIPS 140-2, et a réussi la rigoureuse validation NIST du gouvernement américain.

La plateforme Kiteworks et PCI DSS v4.0

Construire et maintenir un réseau et des systèmes sécurisés

Exigence 1 : Installer et maintenir les contrôles de sécurité du réseau

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 1 de la norme PCI DSS se concentre sur l'installation et la maintenance des contrôles de sécurité du réseau (NSC) afin de protéger les environnements de données des titulaires de cartes (CDE). Elle met l'accent sur des processus bien définis, une configuration adéquate et une maintenance continue des NSC pour une sécurité réseau efficace. L'exigence est divisée en cinq sections. La sous-catégorie 1.1 impose des processus clairs pour la mise en œuvre et la maintenance des NSC en veillant à ce que toutes les parties comprennent leur rôle. La sous-catégorie 1.2 couvre la configuration et la maintenance du NSC, nécessitant des normes définies, la gestion des changements, des révisions régulières et des diagrammes de réseau précis. La sous-catégorie 1.3 traite de la restriction de l'accès au réseau depuis et vers le CDE, en limitant le trafic aux communications nécessaires et en contrôlant l'accès au réseau sans fil. La sous-catégorie 1.4 se concentre sur le contrôle des connexions entre les réseaux fiables et non fiables, la mise en œuvre de NSC, la restriction du trafic entrant et l'utilisation de mesures anti-spoofing. La sous-catégorie 1.5 aborde les risques liés aux dispositifs se connectant à la fois aux réseaux non fiables et au CDE, en imposant des contrôles de sécurité avec des configurations spécifiques et des limitations sur les possibilités de modification par l'utilisateur. Tout au long du texte, l'exigence met l'accent sur la documentation, les mises à jour régulières et la compréhension de toutes les mesures de sécurité par les parties concernées. L'objectif est de créer une infrastructure de sécurité réseau robuste et bien gérée qui protège les données des titulaires de carte contre l'accès non autorisé et les menaces potentielles.	Kiteworks propose des fonctions complètes qui contribuent à la conformité avec la Norme PCI DSS Exigence 1 et ses cinq sous-exigences. Pour la sous-catégorie 1.1, Kiteworks offre des processus bien définis pour l'installation et la maintenance des contrôles de sécurité réseau, incluant des politiques documentées et des attributions de rôles claires. L'appliance virtuelle durcie de la plateforme, avec ses pare-feu réseau et d'application web (WAFs) intégrés, répond à la sous-catégorie 1.2 en garantissant une configuration et une maintenance appropriées des contrôles de sécurité réseau. Ces pare-feu sont mis à jour automatiquement pour faire face aux nouvelles menaces sans intervention de l'IT. La sous-catégorie 1.3, qui se concentre sur la restriction de l'accès réseau vers et depuis l'environnement de données de carte (CDE), est satisfaite grâce aux contrôles d'accès robustes de Kiteworks, au blocage des adresses IP et aux fonctionnalités de géorepérage. L'architecture de confiance zéro de la plateforme, avec son positionnement en couches des composants et le sandboxing de bibliothèque open-source, contrôle efficacement les connexions réseau entre les réseaux de confiance et non fiables, répondant ainsi à la sous-catégorie 1.4. Pour la sous-catégorie 1.5, qui aborde les risques provenant des dispositifs se connectant à la fois aux réseaux non fiables et au CDE, Kiteworks met en œuvre des contrôles de sécurité stricts sur les dispositifs informatiques. Cela inclut des paramètres de configuration spécifiques, des mesures de sécurité actives et des limitations sur la modifiabilité par les utilisateurs. La conception à locataire unique de la plateforme atténue en outre les risques associés aux environnements multi-locataires. La journalisation détaillée de Kiteworks, les contrôles d'accès basés sur les rôles (RBAC), les politiques de risque basées sur le contenu et le double chiffrement pour les fichiers au repos offrent des couches supplémentaires de sécurité. Ces fonctionnalités, combinées à diverses méthodes d'authentification et à la possibilité de restreindre l'accès en fonction du type de client et de l'emplacement, garantissent une posture de sécurité robuste qui s'aligne avec tous les aspects de la norme PCI DSS Exigence 1.

Exigence 2 : appliquer des configurations sécurisées à tous les composants du système

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 2 se concentre sur l'application de configurations sécurisées à tous les composants du système au sein de l'environnement des données du titulaire de carte. La sous-catégorie 2.1 impose des processus bien définis pour la mise en œuvre de configurations sécurisées, exigeant des politiques de sécurité documentées et actualisées ainsi que des procédures opérationnelles connues de toutes les parties concernées. Elle met également l'accent sur la clarté de l'attribution des rôles et des responsabilités. La sous-catégorie 2.2 traite de la configuration et de la gestion sécurisées des composants du système. Il s'agit notamment d'élaborer des normes de configuration complètes qui s'attaquent aux vulnérabilités connues et s'alignent sur les pratiques de renforcement acceptées par l'industrie. Elle exige une gestion appropriée des comptes par défaut des fournisseurs, l'isolation des fonctions ayant des niveaux de sécurité différents et l'activation des seuls services et protocoles nécessaires. En outre, elle stipule la configuration sécurisée des paramètres de sécurité du système et le chiffrement de l'accès administratif non-console. La sous-catégorie 2.3 vise spécifiquement les environnements sans fil connectés au CDE ou transmettant des données de compte. Elle exige de modifier tous les paramètres par défaut des fournisseurs de systèmes sans fil lors de l'installation ou de confirmer leur sécurité. Cette sous-catégorie exige également la mise à jour des clés de chiffrement sans fil lorsque le personnel possédant les connaissances clés quitte l'entreprise ou lorsque les clés sont potentiellement compromises. Ces sous-catégories visent collectivement à minimiser la surface d'attaque en garantissant que tous les composants du système, y compris les environnements sans fil, sont configurés et gérés de manière sécurisée dans l'ensemble de l'environnement des données du titulaire de carte.	Pour la sous-catégorie 2.1, Kiteworks maintient une documentation détaillée et attribue clairement les rôles pour les politiques de sécurité et les procédures opérationnelles. Cela est évident dans leur environnement hébergé, qui respecte la norme SOC 2 et d'autres certifications, garantissant des processus bien définis pour des configurations sécurisées. Concernant la sous-catégorie 2.2, Kiteworks excelle dans la configuration et la gestion sécurisées des composants système. La plateforme est construite sur une appliance virtuelle durcie, incluant uniquement les services nécessaires. Elle emploie une architecture de confiance zéro avec un positionnement des composants par niveaux, limitant le mouvement latéral potentiel par les attaquants. Kiteworks met en œuvre des mesures de chiffrement robustes, y compris un double chiffrement pour les fichiers au repos et le support de TLS 1.3 pour les données en transit. Kiteworks aborde les préoccupations de sécurité par défaut des fournisseurs en n'utilisant pas de mots de passe par défaut et en permettant aux administrateurs de définir des politiques de mot de passe fortes ou même d'abolir l'utilisation de mot de passe au profit de SSO ou de certificats clients. La console d'administration alerte les administrateurs sur les paramètres potentiellement risqués, nécessitant une validation pour les changements, qui sont ensuite documentés dans les journaux d'audit. Kiteworks est hors de portée pour la sous-catégorie 2.3 en raison de l'absence de réseaux sans fil dans son environnement de service. Les fonctionnalités de reporting de conformité de la plateforme, incluant un journal d'activité consolidé et un cadre de politique de risque, soutiennent également l'adhésion à l'exigence 2. Ces fonctionnalités permettent un suivi et un reporting complets des activités du système, garantissant une conformité et une sécurité continues.

Protéger les données du compte

Exigence 3 : Protéger les données stockées sur les comptes

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 3 se concentre sur la protection des données de compte stockées et comprend six sous-catégories essentielles. La sous-catégorie 3.2 exige de minimiser le stockage des données de compte en mettant en œuvre des politiques de conservation et d'élimination des données. La sous-catégorie 3.3 interdit le stockage des données d'authentification sensibles après autorisation, avec des règles spécifiques pour les données de suivi, les codes de vérification de carte et les PIN. La sous-catégorie 3.4 traite de l'affichage et de la copie des numéros de compte principaux (PAN), exigeant qu'ils soient masqués lors de l'affichage et mettant en place des contrôles techniques pour empêcher la copie non autorisée lors de l'accès à distance. La sous-catégorie 3.5 se concentre sur la sécurisation des PANs stockés, exigeant qu'ils soient rendus illisibles en utilisant des méthodes telles que les hachages unidirectionnels, la troncature ou la cryptographie forte. La sous-catégorie 3.6 met l'accent sur la sécurité des clés cryptographiques utilisées pour protéger les données de compte stockées. Elle exige de limiter l'accès aux clés, de s'assurer que les clés de chiffrement des clés sont au moins aussi robustes que les clés de chiffrement des données, et de stocker les clés de manière sécurisée dans le moins d'emplacements possible. Enfin, la sous-catégorie 3.7 impose des processus de gestion des clés couvrant l'intégralité du cycle de vie des clés. Cela inclut la génération, la distribution, le stockage, les modifications, la mise hors service et la destruction des clés. Elle exige également la prévention de la substitution non autorisée des clés et une reconnaissance formelle des responsabilités des gardiens de clés. Dans l'ensemble, l'exigence 3 vise à garantir que les données de compte stockées restent protégées contre l'accès et l'utilisation non autorisés, en adoptant une approche multifacette de la sécurité des données.	Kiteworks offre des fonctionnalités robustes pour soutenir la conformité avec la norme PCI DSS Exigence 3 et ses sous-catégories. Pour la sous-catégorie 3.2, Kiteworks met en œuvre des politiques de rétention et d'élimination des données, incluant la suppression automatique des fichiers et les contrôles d'expiration. La plateforme permet la suppression sécurisée des données, garantissant que les informations sont définitivement retirées lorsque plus nécessaires. Concernant la sous-catégorie 3.3, bien que Kiteworks ne soit pas une plateforme de transactions PCI, elle peut être utilisée comme une plateforme de stockage et de collaboration pour les données téléchargées par les clients. Les clients doivent s'assurer que les données d'authentification sensibles ne sont pas stockées plus longtemps que nécessaire et Kiteworks supporte cela à travers des journaux d'audit complets, des fonctionnalités de suppression sécurisée, des clés appartenant aux clients, un double chiffrement, et des contrôles d'accès granulaires ; ces outils permettent aux clients de surveiller, gérer, et supprimer de manière sécurisée les données comme requis. Pour la sous-catégorie 3.4, la plateforme implémente des contrôles d'accès et des autorisations stricts, incluant l'accès basé sur le rôle et les principes du moindre privilège, pour restreindre l'accès aux PAN complets. La sous-catégorie 3.5 est abordée grâce à la méthode de double chiffrement de Kiteworks. Les fichiers sont chiffrés à la fois au niveau du système d'exploitation et de l'application, garantissant ainsi que les PANs sont sécurisés où qu'ils soient stockés. Cette approche multicouche offre une protection solide même si un attaquant accède au système d'exploitation. Pour la sous-catégorie 3.6, Kiteworks sécurise les clés cryptographiques en permettant aux clients de posséder et de contrôler leurs clés de chiffrement. Cela garantit que même le personnel de Kiteworks ou des acteurs externes ne peuvent pas déchiffrer les données des clients sans autorisation. Pour la sous-catégorie 3.7, la plateforme prend en charge la gestion du cycle de vie des clés en fournissant aux clients les informations et la documentation nécessaires sur leurs clés et leurs responsabilités. Tout au long de ces processus, Kiteworks conserve des journaux d'audit détaillés, suivant toutes les activités et modifications pertinentes, ce qui contribue aux efforts de conformité et assure la transparence dans la gestion des données.

Exigence 4 : Protéger les données des titulaires de cartes par une cryptographie forte lors de leur transmission sur des réseaux ouverts et publics

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 4 met l'accent sur la protection des données des titulaires de carte lors de la transmission sur des réseaux ouverts et publics en utilisant une cryptographie forte. La sous-catégorie 4.2 traite spécifiquement de la protection des numéros de compte principaux (PAN). Elle exige l'implémentation d'une cryptographie forte et de protocoles de sécurité pour la transmission des PAN, en utilisant uniquement des clés de confiance et des certificats valides, et en supportant uniquement des versions sécurisées de protocoles. Les organisations doivent maintenir un inventaire des clés et certificats de confiance et mettre en œuvre les meilleures pratiques industrielles pour les réseaux sans fil transmettant des PAN. Ce point s'étend à la sécurisation des PAN avec une cryptographie forte dans les technologies de messagerie pour les utilisateurs finaux. Il aborde également les scénarios où les données des titulaires de carte sont reçues de manière non sollicitée via des canaux non sécurisés, permettant aux organisations de sécuriser le canal ou d'en empêcher l'utilisation pour les données des titulaires de carte. Le point 4 souligne le rôle crucial d'une encryption robuste dans la protection des données sensibles des titulaires de carte lors de la transmission à travers différents types de réseaux et canaux de communication.	Kiteworks offre un support pour l'exigence 4, qui se concentre sur la protection des données des titulaires de carte lors de la transmission. La plateforme propose une protection cryptographique renforcée en supportant TLS 1.3 et 1.2, donnant aux clients la flexibilité d'activer seulement TLS 1.3, seulement 1.2, ou les deux, en fonction de leurs besoins de sécurité. Toutes les données transmises via Kiteworks sont chiffrées en utilisant TLS 1.2 ou supérieur, assurant un haut niveau de sécurité pour les informations sensibles en transit. Kiteworks fournit l'infrastructure pour une transmission sécurisée et les responsabilités de gestion des clés reposent sur le client, permettant un plus grand contrôle et une personnalisation des mesures de sécurité.

Maintenir un programme de gestion de la vulnérabilité

Exigence 5 : protéger tous les systèmes et réseaux contre les logiciels malveillants

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 5 se concentre sur la protection de tous les systèmes et réseaux contre les logiciels malveillants et exige une protection antimalware complète sur tous les systèmes et réseaux, y compris contre les menaces émergentes telles que les attaques de phishing. Les sous-catégories 5.2 à 5.4 abordent des aspects spécifiques de cette protection. La sous-catégorie 5.2 impose la prévention, la détection et la gestion des malwares en déployant des solutions antimalware sur tous les composants du système, à l'exception des systèmes à faible risque. Ces solutions doivent détecter, supprimer, bloquer ou contenir tous les types de malwares connus, et des évaluations régulières des systèmes jugés non à risque sont requises. La sous-catégorie 5.3 assure que les mécanismes antimalware sont actifs, maintenus et surveillés. Cela inclut la mise à jour automatique des solutions, l'exécution de scans périodiques ou en temps réel ou l'analyse comportementale continue, la gestion des supports électroniques amovibles, la conservation des journaux d'audit et la prévention de la désactivation ou de la modification non autorisée des mécanismes antimalware. La sous-catégorie 5.4 introduit la protection anti-phishing, nécessitant la mise en œuvre de processus et de mécanismes automatisés pour détecter et protéger contre les attaques de phishing.	Kiteworks propose plusieurs fonctionnalités qui contribuent à la conformité avec l'Exigence 5 et ses sous-catégories. Pour la sous-catégorie 5.2, Kiteworks offre un service antivirus WithSecure(R) intégré en tant que service additionnel. Cette solution antivirus analyse les fichiers à la recherche de logiciels malveillants lors des processus de téléchargement et de téléversement, gérant des fichiers de toute taille, y compris ceux transitant par les sources Enterprise Connect ou la passerelle de protection des e-mails (EPG). Conformément à la sous-catégorie 5.3, Kiteworks impose l'analyse antivirus sur tous ses systèmes comme condition de renouvellement du service. La plateforme conserve des journaux détaillés des activités du système, y compris les résultats des analyses antivirus et les échecs, améliorant ainsi la visibilité sur les opérations de sécurité. Les administrateurs peuvent configurer le système pour mettre en quarantaine les fichiers infectés ou pour enregistrer et alerter lors d'une détection, garantissant ainsi un suivi et une maintenance continus. Abordant la sous-catégorie 5.4, Kiteworks prend en charge les protocoles DKIM, SPF et DMARC pour les e-mails des clients. Ces protocoles aident à prévenir l'usurpation d'e-mails et d'autres attaques basées sur les e-mails, protégeant ainsi les utilisateurs contre les tentatives de phishing. Kiteworks propose également des rôles d'administrateur robustes, y compris un rôle d'Administrateur Système capable de configurer et de maintenir tous les aspects du produit, garantissant ainsi une gestion adéquate des fonctionnalités de sécurité dans toutes les sous-catégories. Ensemble, ces fonctionnalités illustrent l'approche de Kiteworks pour la prévention, la détection et l'atténuation des logiciels malveillants, aidant les organisations dans leurs efforts pour être conforme à l'exigence 5 et ses sous-catégories.

Exigence 6 : développer et maintenir des systèmes et des logiciels sécurisés

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 6 se concentre sur le développement et le maintien de systèmes et de logiciels sécurisés et souligne l'importance de mesures de sécurité proactives tout au long du cycle de vie du développement logiciel et du processus de maintenance du système. La sous-catégorie 6.2 aborde le développement sécurisé de logiciels sur mesure et personnalisés, exigeant des pratiques standard de l'industrie, une formation régulière pour le personnel de développement et des revues de code approfondies avant la mise en production. Elle requiert également la mise en œuvre de techniques pour prévenir les attaques logicielles courantes. La sous-catégorie 6.3 met l'accent sur l'identification et la gestion des vulnérabilités de sécurité. Cela inclut l'utilisation de sources reconnues par l'industrie pour les informations sur les vulnérabilités, l'attribution de classements de risque, le maintien d'un inventaire des composants logiciels et l'installation rapide de correctifs de sécurité. La sous-catégorie 6.4 se concentre sur la protection des applications web accessibles au public contre les attaques. Elle exige des évaluations régulières de vulnérabilité, la correction des vulnérabilités identifiées et le déploiement de solutions techniques automatisées pour détecter et prévenir les attaques basées sur le web. La sous-catégorie 6.5 traite de la gestion sécurisée des changements pour tous les composants du système. Elle impose des procédures établies pour la mise en œuvre des changements, y compris la documentation de la raison et de l'impact sur la sécurité, l'obtention d'une approbation, les tests et la confirmation des exigences PCI DSS après des changements significatifs. Elle exige également la séparation des environnements de pré-production et de production et la suppression des données de test avant le déploiement en production.	Kiteworks met en œuvre un cycle de vie du développement logiciel sécurisé, incluant des formations régulières pour les développeurs, des pratiques de codage sécurisé et des revues de conception mettant l'accent sur la sécurité, soutenant ainsi la sous-catégorie 6.2. L'entreprise utilise les meilleures pratiques telles que OWASP et adopte une approche de sécurité "shift left". En adressant la sous-catégorie 6.3, Kiteworks maintient un cycle continu de tests de sécurité, comprenant des évaluations de vulnérabilité internes et externes. L'entreprise met régulièrement à jour son logiciel pour corriger les vulnérabilités connues, publie des CVE et vise à devenir une Autorité de Numérotation CVE. Pour la sous-catégorie 6.4, Kiteworks met en œuvre une appliance virtuelle durcie avec plusieurs niveaux de protection, incluant un pare-feu d'application web (WAF) intégré qui détecte et bloque les attaques web et REST API. Cela correspond à l'exigence de protection des applications web accessibles au public. Concernant la sous-catégorie 6.5, Kiteworks prend en charge la gestion sécurisée des changements grâce à son système de mise à jour en un clic, qui permet la vérification cryptographique des mises à jour. L'entreprise maintient des environnements de production et de développement séparés, met en œuvre des contrôles d'accès basés sur les rôles (RBAC) et assure la suppression des comptes de test avant le déploiement. Kiteworks adopte une approche globale pour le développement et la maintenance de logiciels sécurisés, incluant des formations régulières, les meilleures pratiques telles que OWASP, des tests de sécurité continus, des appliances virtuelles durcies avec plusieurs niveaux de protection, une gestion sécurisée des changements et des contrôles d'accès stricts, le tout en conformité avec les exigences PCI DSS pour le développement et la maintenance de systèmes et logiciels sécurisés.

Mettre en place des mesures de contrôle d'accès strictes

Exigence 7 : Restreindre l'accès aux composants du système et aux données des titulaires de cartes en fonction du besoin d'en connaître

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 7 se concentre sur la restriction de l'accès aux composants du système et aux données des titulaires de carte en fonction des besoins professionnels à connaître. Elle comprend deux principales sous-catégories : 7.2 et 7.3. Ces deux sous-catégories soulignent l'importance des révisions régulières, de l'attribution d'accès appropriée et du principe du moindre privilège pour maintenir un environnement sécurisé pour les données des titulaires de carte et les composants du système. La sous-catégorie 7.2 exige une définition et une attribution appropriées des accès aux composants du système et aux données. Elle nécessite un modèle de contrôle d'accès défini qui accorde l'accès en fonction des besoins commerciaux, des classifications de poste et du principe du moindre privilège. L'accès des utilisateurs, y compris les utilisateurs privilégiés et les comptes tiers, doit être régulièrement examiné et approuvé. Les comptes d'application et de système doivent être gérés avec les privilèges nécessaires minimaux et périodiquement révisés. La sous-catégorie 7.3 traite de la gestion de l'accès logique via les systèmes de contrôle d'accès. Ces systèmes doivent restreindre l'accès en fonction du besoin de savoir de l'utilisateur, couvrir tous les composants du système et appliquer les privilèges attribués. Il est important que le système de contrôle d'accès soit configuré sur "tout refuser" par défaut, garantissant que l'accès est accordé uniquement lorsqu'il est explicitement autorisé.	Pour la sous-catégorie 7.2, Kiteworks met en œuvre un système de contrôle d'accès basé sur les rôles (RBAC). Ce système comprend des rôles prédéfinis tels que Propriétaire, Gestionnaire, Collaborateur, Téléchargeur, Visionneur et Chargeur, chacun avec des autorisations spécifiques alignées sur les fonctions de travail et le principe du moindre privilège. Kiteworks est conçu pour attribuer automatiquement aux utilisateurs les autorisations les moins élevées nécessaires, nécessitant une action explicite de l'administrateur pour les privilèges élevés. Abordant la sous-catégorie 7.3, Kiteworks utilise un système de contrôle d'accès sophistiqué qui restreint l'accès en fonction des besoins en connaissance de l'utilisateur. La plateforme prend en charge diverses méthodes d'authentification, y compris l'authentification multifactorielle (MFA) et la connexion unique (SSO), et met en œuvre une architecture de confiance zéro où chaque service traite les communications provenant d'autres services comme non fiables. Kiteworks prend également en charge le contrôle d'accès basé sur les attributs (ABAC), permettant des politiques de risque dynamiques basées sur les attributs du contenu, les attributs de l'utilisateur et les actions spécifiques. De plus, Kiteworks conserve des journaux d'audit détaillés de toutes les activités liées à l'accès, y compris les modifications des autorisations, la gestion des utilisateurs et les modifications de configuration. Ce système de journalisation soutient les examens réguliers des accès utilisateurs, une exigence clé des deux sous-catégories. Le principe de la plateforme « refuser par défaut, autoriser par exception » s'aligne parfaitement avec l'exigence du PCI DSS selon laquelle les systèmes de contrôle d'accès doivent être configurés pour « tout refuser » par défaut.

Exigence 8 : Identifier les utilisateurs et authentifier l'accès aux composants du système

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 8 souligne l'importance de pratiques robustes d'identification et d'authentification des utilisateurs pour garantir la responsabilité et protéger contre l'accès non autorisé aux données sensibles et aux systèmes. Cela se concentre sur l'identification des utilisateurs et l'authentification de l'accès aux composants du système. La sous-catégorie 8.2 impose une gestion stricte des identifiants et des comptes utilisateurs tout au long de leur cycle de vie, incluant des identifiants uniques pour tous les utilisateurs, l'utilisation contrôlée de comptes partagés et la révocation rapide de l'accès pour les utilisateurs résiliés. La sous-catégorie 8.3 établit des pratiques d'authentification fortes, incluant l'authentification multifactorielle (MFA), les exigences de complexité des mots de passe et le stockage sécurisé des facteurs d'authentification. La sous-catégorie 8.4 exige la mise en œuvre de la MFA pour tout accès administratif non-console à l'environnement de données du titulaire de carte (CDE) et pour tout accès réseau à distance. La sous-catégorie 8.5 se concentre sur la configuration des systèmes MFA pour prévenir les abus, en s'assurant qu'ils ne sont pas susceptibles aux attaques de replay et ne peuvent pas être contournés sans autorisation appropriée. Enfin, la sous-catégorie 8.6 traite de la gestion des comptes d'application et de système, incluant la limitation de l'utilisation interactive, la protection des mots de passe contre l'écriture en dur dans le code et la mise en œuvre de changements périodiques de mots de passe basés sur une analyse des risques.	Kiteworks facilite l'identification des utilisateurs et l'authentification de l'accès aux composants du système. Pour la sous-catégorie 8.2, Kiteworks assure une gestion stricte des identifiants utilisateurs, incluant des ID uniques pour tous les utilisateurs et l'utilisation contrôlée des comptes partagés. La plateforme prend en charge diverses méthodes d'authentification (sous-catégorie 8.3), y compris basées sur les identifiants, sur certificat et l'authentification multifactorielle (MFA), avec des options pour SAML 2.0 SSO, Kerberos SSO et OAuth. En abordant les sous-catégories 8.4 et 8.5, Kiteworks met en œuvre la MFA par plusieurs méthodes telles que le protocole RADIUS, les cartes PIV/CAC et les OTP basés sur le temps. La plateforme permet aux administrateurs de configurer et de contrôler les politiques d'authentification, garantissant que les systèmes MFA sont correctement mis en place et sécurisés contre les abus. Pour la sous-catégorie 8.6, Kiteworks permet aux administrateurs de définir des politiques de mot de passe strictes, incluant une longueur minimale, des exigences de complexité et un historique de mot de passe. La plateforme prend également en charge l'expiration des mots de passe et impose le changement de mot de passe lors de la première connexion. Tout au long de ces processus, Kiteworks conserve des journaux d'audit détaillés de toutes les activités liées à l'accès, y compris les changements de permissions et la gestion des utilisateurs. Le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC) de la plateforme renforcent davantage la sécurité en appliquant le principe du moindre privilège.

Exigence 9 : Restreindre l'accès physique aux données des titulaires de cartes

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 9 souligne l'importance de mesures de sécurité physique approfondies pour protéger les données des titulaires de carte contre l'accès ou le retrait non autorisés. La sous-catégorie 9.2 impose des contrôles d'accès physique pour gérer l'entrée dans les installations et les systèmes contenant des données de titulaires de carte. Cela inclut des contrôles d'entrée appropriés dans les installations, la surveillance des zones sensibles et des restrictions sur les prises réseau accessibles au public et les points d'accès sans fil. La sous-catégorie 9.3 traite de l'autorisation et de la gestion de l'accès physique pour le personnel et les visiteurs. Elle exige des procédures pour identifier le personnel, gérer les changements d'accès et révoquer l'accès lors de la résiliation. Pour les visiteurs, elle impose une autorisation, un accompagnement et la tenue de registres de visiteurs. La sous-catégorie 9.4 se concentre sur le stockage sécurisé, l'accès, la distribution et la destruction des supports contenant des données de titulaires de carte. Cela inclut la sécurité physique des supports, la classification basée sur la sensibilité des données, le transport sécurisé et les méthodes de destruction appropriées pour les supports papier et électroniques. La sous-catégorie 9.5 concerne la protection des dispositifs de point d'interaction (POI) contre le sabotage et le remplacement non autorisé. Elle exige de maintenir une liste des dispositifs POI, des inspections périodiques et de former le personnel à reconnaître et à signaler les comportements suspects.	Bien que les contrôles d'accès physiques et les dispositifs POI soient hors de portée, Kiteworks est conforme à la sous-catégorie 9.4. Kiteworks propose des capacités de journalisation d'audit détaillées, enregistrant toutes les activités des utilisateurs liées à l'accès, à la modification et à la suppression des données. Cela fournit un enregistrement détaillé de toutes les interactions avec les données sensibles, ce qui peut être crucial pour la surveillance de la sécurité et la réponse aux incidents. La suppression sécurisée de la plateforme aide à maintenir la confidentialité et la sécurité des données des utilisateurs, en accord avec les exigences du PCI DSS pour une destruction appropriée des données.

Contrôler et tester régulièrement les réseaux

Exigence 10 : Enregistrer et contrôler tous les accès aux composants du système et aux données des titulaires de cartes

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 10 œuvre pour aider les organisations à maintenir un environnement sécurisé, en prévenant l'accès non autorisé et en garantissant la conformité aux normes PCI DSS. L'exigence 10 du PCI DSS se concentre sur le besoin critique de consigner et surveiller tous les accès aux composants systèmes et aux données des titulaires de carte, assurant une posture de sécurité robuste contre les violations de données. Les journaux d'audit, cruciaux pour détecter les anomalies et les activités suspectes, doivent être activés sur tous les composants systèmes et les environnements de données des titulaires de carte conformément à la sous-catégorie 10.2. Ces journaux doivent capturer des détails complets des activités des utilisateurs, y compris les actions administratives et les tentatives d'accès. La sous-catégorie 10.3 se concentre sur le maintien de l'intégrité de ces journaux. Ils doivent être protégés contre la destruction et les modifications non autorisées, avec un accès strictement contrôlé. La sous-catégorie 10.4 exige des révisions régulières de ces journaux pour identifier et adresser toute anomalie, et la sous-catégorie 10.5 requiert qu'un historique minimum de 12 mois de journaux soit conservé. Selon la sous-catégorie 10.6, une synchronisation temporelle cohérente à travers tous les systèmes est vitale pour assurer une consignation précise. Enfin, au sein de la sous-catégorie 10.7, la détection rapide, le signalement et la réponse aux défaillances dans les systèmes de contrôle de sécurité critiques sont essentiels pour prévenir les lacunes de sécurité.	Pour la sous-catégorie 10.2, Kiteworks garantit que les journaux d'audit sont activés et capturent toutes les activités pertinentes, telles que les tentatives d'authentification des utilisateurs, les téléchargements et téléversements de fichiers, les changements systèmes et les actions administratives, le tout au sein d'un journal d'activité consolidé. Cette tenue de journaux répond aux exigences de détection des anomalies et de soutien à l'analyse forensique. Pour la sous-catégorie 10.3, Kiteworks protège les journaux d'audit contre la destruction et les modifications non autorisées, assurant que les journaux sont protégés et uniquement accessibles à ceux ayant un besoin professionnel. Conformément à la sous-catégorie 10.4, ces journaux peuvent être régulièrement examinés pour identifier et traiter rapidement toute activité suspecte. Kiteworks aborde également la sous-catégorie 10.5 en permettant aux organisations de personnaliser les périodes de rétention, garantissant que l'historique des journaux d'audit est conservé et accessible pendant au moins 12 mois. En ce qui concerne la sous-catégorie 10.6, Kiteworks s'intègre aux serveurs du Protocole de Temps Réseau (NTP) pour maintenir une synchronisation temporelle cohérente à travers tous les systèmes, crucial pour une tenue de journaux précise. Enfin, sous la sous-catégorie 10.7, l'intégration en temps réel des journaux de Kiteworks avec les outils SIEM permet une détection, un rapport et une réponse immédiats à toute défaillance des systèmes de contrôle de sécurité critiques.

Exigence 11 : tester régulièrement la sécurité des systèmes et des réseaux

Exigences de l'approche définie	Solution de Kiteworks
L'exigence 11 se concentre sur le test régulier de la sécurité des systèmes et des réseaux pour garantir que les contrôles de sécurité restent efficaces face aux menaces évolutives. La sous-catégorie 11.2 mandate l'identification et la surveillance des points d'accès sans fil, en s'assurant que les points d'accès non autorisés sont traités rapidement. Des scans de vulnérabilité internes et externes réguliers sont requis sous la sous-catégorie 11.3, avec un accent mis sur l'identification, la priorisation et le traitement des vulnérabilités. De plus, des tests de pénétration externes et internes doivent être effectués régulièrement pour découvrir et corriger les vulnérabilités exploitables et les faiblesses de sécurité, comme spécifié dans la sous-catégorie 11.4. La sous-catégorie 11.5 exige le déploiement de techniques de détection ou de prévention des intrusions, garantissant que les intrusions réseau et les changements de fichiers inattendus sont détectés et traités rapidement. Enfin, la sous-catégorie 11.6 impose l'utilisation de mécanismes de détection de changement et de falsification pour alerter le personnel des modifications non autorisées sur les pages de paiement, se protégeant contre les compromissions potentielles. Collectivement, ces exigences garantissent qu'une posture de sécurité d'organisation est continuellement évaluée et renforcée, réduisant le risque de violations de données et maintenant la conformité avec le PCI DSS.	Kiteworks aide les organisations à identifier et à traiter régulièrement les vulnérabilités internes et externes grâce à ses fonctionnalités complètes de journalisation et de surveillance, soutenant la sous-catégorie 11.3. Ces fonctions garantissent que toute faiblesse de sécurité au sein de l'environnement Kiteworks est rapidement identifiée et corrigée, maintenant l'intégrité des données gérées sur la plateforme. Conformément à la sous-catégorie 11.5, Kiteworks utilise des techniques avancées de détection et de prévention des intrusions, surveillant tout le trafic réseau aux points critiques du système. Cela inclut la détection des tentatives d'accès non autorisées, la surveillance des changements de fichiers inattendus et l'assurance que le personnel est alerté en cas de compromissions potentielles. De plus, les outils intégrés de surveillance de l'intégrité des fichiers de Kiteworks garantissent que toute modification non autorisée des fichiers critiques est détectée et traitée rapidement. Bien que les sous-catégories 11.2, 11.4 et 11.6 soient hors du champ d'application de Kiteworks en raison de l'orientation et de l'architecture de la plateforme, Kiteworks continue d'apporter de la valeur en sécurisant les données et les activités au sein de son environnement. Cela soutient les efforts de conformité globale PCI DSS d'une organisation en abordant les exigences de sécurité clés dans son domaine.

Maintenir une politique de sécurité de l'information

Exigence 12 : Soutenir la sécurité de l'information par des politiques et des programmes organisationnels

Exigences de l'approche définie	Solution de Kiteworks
La norme PCI DSS Exigence 12 se concentre sur le soutien de la sécurité de l'information avec des politiques et des programmes organisationnels. Elle garantit que les organisations disposent de politiques et de procédures à jour et complètes pour maintenir une posture de sécurité forte et gérer efficacement la conformité au PCI DSS. La sous-catégorie 12.1 exige une politique de sécurité de l'information complète, connue, actuelle et régulièrement révisée. La sous-catégorie 12.2 nécessite des politiques d'utilisation acceptable définies et mises en œuvre pour les technologies utilisées par les utilisateurs finaux. La sous-catégorie 12.3 se concentre sur l'identification formelle, l'évaluation et la gestion des risques pour l'environnement des données du titulaire de carte. Les sous-catégories 12.4 et 12.5 traitent de la gestion de la conformité au PCI DSS et de la documentation de portée. La sous-catégorie 12.6 met l'accent sur l'éducation continue à la sensibilisation à la sécurité pour tout le personnel. La sous-catégorie 12.7 exige un filtrage du personnel pour réduire les risques liés aux menaces internes. Les sous-catégories 12.8 et 12.9 traitent de la gestion des risques associés aux relations avec les prestataires de services tiers et garantissent que ces fournisseurs soutiennent la conformité au PCI DSS des clients. Enfin, la sous-catégorie 12.10 exige une réponse immédiate aux incidents de sécurité suspectés et confirmés qui pourraient affecter l'environnement des données du titulaire de carte. Cela inclut le maintien d'un plan de réponse aux incidents, des tests et mises à jour réguliers, et du personnel désigné pour une réponse aux incidents 24/7.	La licence de Gouvernance Avancée de la plateforme permet aux administrateurs de conformité de définir et d'appliquer des politiques de risque dynamiques basées sur les actifs de contenu, les attributs des utilisateurs et les actions spécifiques, en accord avec les sous-catégories 12.3 et 12.5. Kiteworks est conçu selon les meilleures pratiques et normes de l'industrie, telles que le Cadre de Cybersécurité du NIST, soutenant les fonctions Identifier, Protéger, Détecter, Répondre et Récupérer. Cette approche aide à maintenir une posture de sécurité forte à travers plusieurs aspects des opérations, comme requis par la sous-catégorie 12.1. Les paramètres de contrôle de la plateforme permettent une gestion granulaire des contrôles d'accès et des mesures de protection des données, en appliquant le principe du moindre privilège. Cela soutient la sous-catégorie 12.4 sur la gestion de la conformité PCI DSS. Kiteworks fournit également des capacités complètes de journalisation des audits et de gestion de la configuration, qui sont cruciales pour la planification de la réponse aux incidents comme décrit dans la sous-catégorie 12.10. L'architecture à locataire unique de Kiteworks et les clés de chiffrement détenues par le client garantissent la confidentialité et la sécurité des données, soutenant les efforts de conformité globaux. Les capacités de détection d'intrusion et d'anomalies de la plateforme, ainsi que les revues régulières des modules cryptographiques et des chiffrements, renforcent davantage les mesures de sécurité. Bien que certains aspects du Requis 12 soient hors du champ d'application de Kiteworks (sous-catégories 12.2, 12.6, 12.7, 12.8, et 12.9), les fonctionnalités de la plateforme contribuent à la capacité d'une organisation de maintenir et d'appliquer des politiques de sécurité de l'information en conformité avec les exigences PCI DSS.

Maintenir une politique de sécurité de l'information

Exigence 12 : Soutenir la sécurité de l'information par des politiques et des programmes organisationnels

Les informations fournies sur cette page ne constituent pas, et ne sont pas destinées à constituer, un conseil juridique ; au contraire, toutes les informations, contenus et matériaux disponibles sur cette page sont à des fins d'information générale uniquement. Les informations sur ce site Web peuvent ne pas constituer les informations juridiques ou autres les plus récentes. Des options supplémentaires sont incluses dans ce Guide et sont nécessaires pour soutenir la conformité.