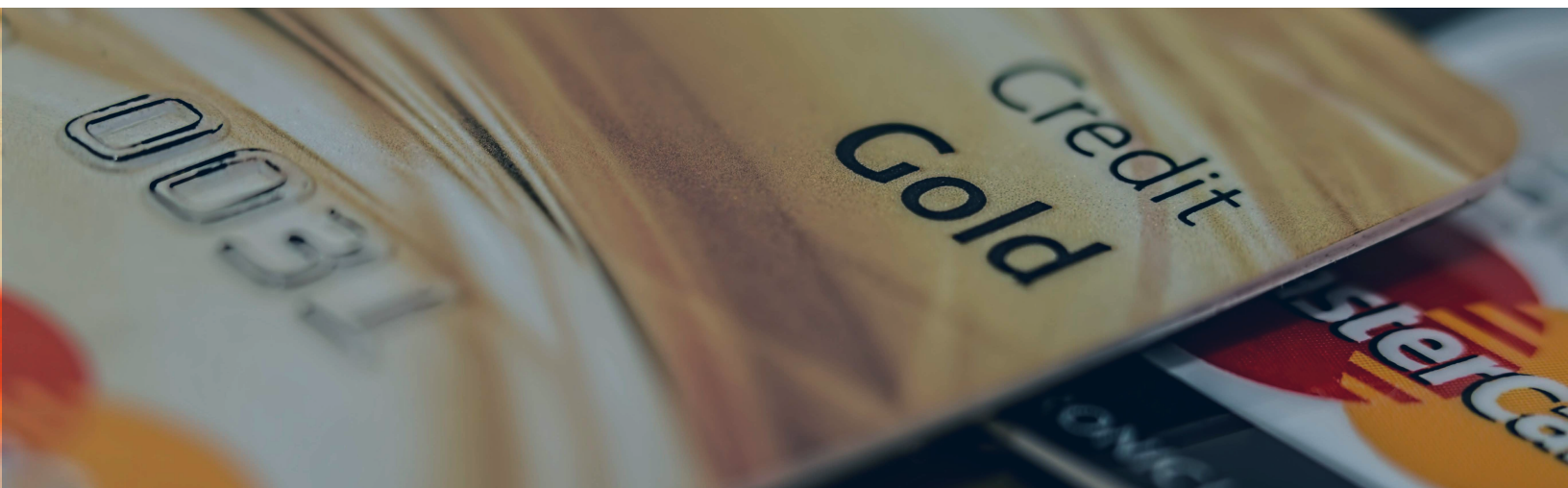


## GUIDE DE CONFORMITE - FINANCE

# Industrie des cartes de paiement Norme de sécurité des données (PCI DSS)

Établie par cinq grands systèmes de cartes de crédit - Visa, MasterCard, American Express, Discover et JCB, la norme de sécurité des données de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard) est une norme pour sécuriser les transactions par carte de paiement, qui protège les transactions contre le vol de données et la fraude.

Pour se conformer à la norme, les entreprises qui traitent des transactions par carte doivent contrôler strictement l'accès aux informations personnelles et financières des titulaires de carte, et surveiller les accès non autorisés au réseau de l'entreprise.



Réduisez les risques avec les solutions **ASC Technologies** d'enregistrement et d'analyse IA

Pour en savoir plus, regardez [cette courte vidéo](#).



## Industrie des cartes de paiement - Norme de sécurité des données

### Objectif principal

Régi par le Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI SSC), le système de conformité vise à sécuriser les transactions par carte de crédit et de débit contre le vol de données et la fraude.

### Qui doit s'y conformer?

Toutes les entreprises qui traitent ou gèrent des données de cartes de crédit, quel que soit leur rôle ou leur secteur d'activité, doivent se conformer aux exigences de la norme PCI DSS.

## PCI DSS Version 4.0

La norme PCI DSS 4.0 est conçue pour mieux sécuriser les données des titulaires de cartes en aidant les organisations à adopter une vision plus globale des mesures de sécurité et des contrôles d'accès. En outre, elle répond aux nouvelles menaces engendrées par les progrès technologiques.

### Objectifs de la mise à jour

#### Continuer à répondre aux besoins de sécurité du secteur des paiements

- Extension des exigences en matière d'authentification multifactorielle.
- Mise à jour des exigences en matière de mot de passe.
- Nouvelles exigences en matière de commerce électronique et de phishing pour faire face aux menaces actuelles.

#### Promouvoir la sécurité comme un processus continu

- Rôles et responsabilités clairement attribués pour chaque exigence.
- Des conseils ont été ajoutés pour aider les utilisateurs à mieux comprendre comment mettre en oeuvre et maintenir la sécurité.

#### Flexibilité accrue pour les différentes méthodologies

- Possibilité de créer des comptes de groupe, des comptes partagés et des comptes génériques.
- Les analyses de risque ciblées permettent aux organisations d'établir des fréquences, patterns (ex : carte de crédit), pour l'exécution de certaines activités.
- L'approche personnalisée, une nouvelle méthode de mise en oeuvre et de validation des exigences de la norme PCI DSS, offre une autre option aux organisations qui utilisent des méthodes innovantes pour atteindre leurs objectifs de sécurité.

#### Améliorer les méthodes de validation

- Meilleure harmonisation des informations communiquées dans un rapport de conformité ou une auto-évaluation.
- Questionnaire et informations résumés dans une attestation de conformité.





## Avantages de la conformité

- **Une sécurité renforcée:** La conformité à la norme PCI DSS aide les entreprises à mettre en place et à maintenir des mesures de sécurité solides pour protéger les informations sensibles relatives aux cartes de paiement. En adhérant aux exigences de la norme, les entreprises peuvent réduire le risque de violation des données, de fraude et d'accès non autorisé.
- **Confiance des clients:** La démonstration de la conformité à la norme PCI DSS peut renforcer la confiance de vos clients qui sont plus enclins à faire confiance aux entreprises qui accordent la priorité à la sécurité de leurs données de cartes de paiement. Cela se traduit par une satisfaction et une fidélité accrues de la clientèle.
- **Conformité juridique et réglementaire:** La conformité à la norme PCI DSS aide les entreprises à répondre aux exigences légales et réglementaires liées à la protection des données des cartes de paiement. Le nonrespect de la norme PCI DSS peut entraîner des amendes, des pénalités et des responsabilités juridiques, c'est pourquoi il est essentiel de s'y conformer.

## Comment ASC peut vous aider à garantir la conformité?

Outre les règles de conformité établies par le Dodd-Frank Act, la MiFID II et le PCI DSS, les entreprises doivent également se conformer aux réglementations de sécurité des données telles que le RGPD. Les solutions d'ASC s'assurent que les entreprises respectent les exigences réglementaires. Conçues pour les environnements de communication modernes d'aujourd'hui, les solutions ASC permettent de se conformer facilement et en toute sécurité aux normes les plus strictes en matière des autres solutions.

- L'IA aide à détecter instantanément les violations potentielles de conformité
- Règles d'enregistrement configurables, droits d'accès
- Options de stockage sécurisé et d'archivage sélectionnables
- Chiffrement des données dédié / bring your own key
- Processus d'approbation pour l'accès et la relecture
- Durée de conservation personnalisable et processus de suppression sécurisé
- Rapports d'audit

### À propos d'ASC Technologies

ASC est l'un des principaux fournisseurs mondiaux de logiciels et de solutions cloud dans le domaine de l'enregistrement omni-canal, de la gestion de la qualité et de l'analyse. Nous offrons des solutions pour l'enregistrement ainsi que pour l'analyse et l'évaluation de toutes les communications basées sur l'IA - avec une flexibilité totale en tant que service cloud, sur site ou en tant que solution hybride. Basé en Allemagne, avec des filiales dans 14 pays et des partenariats d'intégration de systèmes expérimentés dans plus de 60 pays, ASC est le premier acteur européen de son secteur.



SUIVEZ-NOUS SUR

