



L'impact de PCI-DSS sur les différents acteurs du marché

Marchands, PSP, Banques... quel est-il ?



Présentation

Sébastien MAZAS – Verizon Business

QSA

Responsable GRC France

15 ans d'expériences dans la sécurité des systèmes d'information

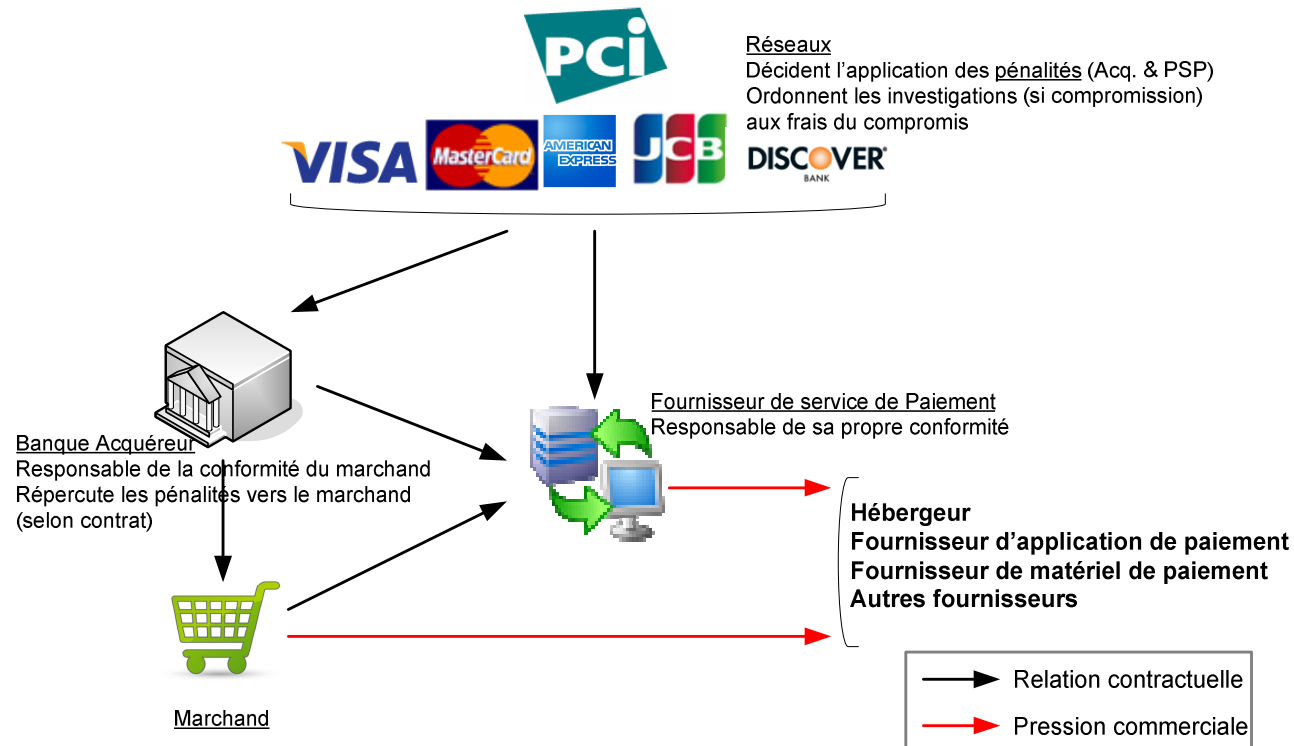
CISSP, CISA, PCI-QSA,

ISO/IEC 27001:2005 Lead Implementer

ISO/IEC 27005:2008 Risk Manager.



Les acteurs autour de PCI-DSS



La certification est un choix stratégique pour lequel l'activité de l'entité est primordiale.

Les marchands – obligations

- La Conformité est une obligation vis-à-vis de son contrat avec sa banque
 - Le niveau de marchand impose la certification
 - L'acquéreur est responsable vis-à-vis des réseaux
- La conformité est une contrainte
 - Coût de la conformité et de la certification
 - Sécurité vs conformité
 - Obligations métier vs réglementation locale
- La conformité est un levier
 - Débloque les budgets
 - Rapproche le métier de l'IT



Les marchands – selon l'activité

- PCI-DSS cible le e-Commerce
 - Activité « carte non présente »
 - Maturité importante sur la sécurité « IT »
- D'autres secteurs sensibles
 - Hôtellerie
 - Les Autoroutes
- Les différentes structures rendent les obligations complexes
 - Franchises, filiales, multi-acquéreurs...
 - Assistance de QSA pour la relation avec les banques



Les PSP – obligations

- L'obligation vient des réseaux
 - Liste des PSP certifiés chez Visa
 - Relation directe sans passer par les acquéreurs

- Contrainte métier forte
 - Interdiction de contractualiser avec un PSP non certifié
 - Marché hautement concurrentiel
 - Point d'attention de tous les acteurs de PCI



Les PSP – les difficultés

- Service vs entité
 - Multiples services et offres indépendantes
 - Programmes de mise en conformité

- Architectures complexes et contraintes de dispo
 - Masse de transactions très importante
 - Bases de données très larges
 - Limites des solutions techniques
 - Compétition sur le temps de réponse



Les banques - obligations

- Obligation « morale »
 - Pas de certification exigée par les réseaux
 - Devoir vis-à-vis des marchands
 - Demande de conformité par la BdF
 - Risque sur l'image

- Prise en compte par les grands groupes
 - Programmes de refonte
 - Analyses d'écart
 - Accompagnement



Les banques - contraintes

- Complexité
 - La donnée est partout
 - Systèmes hétérogènes
 - Criticité de la Disponibilité
- Mais aussi systèmes très anciens
 - Mainframe
 - HP nonstop
 - Cobol
 - ...
- La sécurité est assurée depuis très longtemps



Et les autres ?

- De très nombreux services « indirects »
 - De la supervision à l'archivage
 - Parfois services très limités
- Obligation par ricochet
 - Jamais directement concerné
 - Exigences 12.8.x
 - De plus en plus demandé
- Stratégie de certification
 - Service pas nécessairement adapté (mono client)
 - Mais peut être un argument commercial



L'épreuve de l'audit

- Evaluation de la conformité par rapport au standard
 - 280 exigences, environ 900 points de contrôles
 - 100% de conformité pour la certification

- Le QSA évalue, le réseau certifie
 - Lien entre réalité du métier et attentes des réseaux
 - Etablit un constat et non un jugement de valeur
 - Le meilleur avocat pour défendre son client

- L'audit est toujours un enjeu / une phase critique
 - Sa préparation est fondamentale



Bien choisir son QSA

- Opter pour un accompagnement jusqu'à l'audit
 - Le même QSA est autorisé : principe de PCI-DSS
 - Validation / Réduction du périmètre : 50% du projet
 - Conseil sur sa mise en œuvre, interprétation, démystification, mesures compensatoires : limiter le risque

- Votre QSA en a vu d'autres :
 - Connaissance des spécificité de votre métier de votre organisation
 - Expérience d'architectures similaires
 - Maitrise des relations entre les entités / tiers



Autres apports du QSA

- Stratégie de mise en conformité
 - Audit vs conformité
 - Externalisation vs mise en conformité
 - Stratégie d'audit d'organisations complexes

- Lien avec les banques
 - Définition du niveau de marchand
 - Stratégie de mise en conformité

- Lien avec les réseaux (cas des PSP)
 - Stratégie de mise en conformité
 - Architectures multi-périmètres

