Comment et **pourquoi** être conforme au PCI DSS ?

BONNES PRATIQUES
PAROLES D'EXPERTS
CHIFFRES CLÉS

Livre blanc

evidence by xmco®

L'accélérateur de votre certification **PCI DSS**

Sommaire

1 Qu'est-ce que le PCI DSS et **pourquoi se conformer** à ce standard de **sécurité de paiement** ? ..... p. 3

2 Le prix d'une cyberattaque et les conséquences du **non-respect du standard PCI DSS** ..... p. 06

3 Comment déterminer son SAQ et comment **se mettre en conformité** ? ..... p. 9

4 **e-commerce** : entre RGPD et PCI DSS ..... p. 13

5 Les 3 conseils de notre expert PCI DSS pour **se lancer sereinement** ..... p. 16

evidence by xmco®

1 Qu'est-ce que le PCI DSS et **pourquoi se conformer** à ce standard de **sécurité de paiement** ?

Le PCI DSS en bref

Créé en 2004, le PCI DSS[1] est un **référentiel de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique**. La norme PCI DSS est établie par les cinq principaux réseaux cartes et est gérée par le Conseil des normes de sécurité PCI, appelé PCI SSC[2]. Ce dernier a publié une documentation de 139 pages et environs 250 exigences de sécurité.

Ce standard a été créé afin d'augmenter le contrôle des informations du titulaire de la carte dans le but de réduire l'utilisation frauduleuse des instruments de paiement.

Il est de la responsabilité de l'entreprise d'assurer la sécurité des données de ses clients. **Le PCI DSS demande aux entreprises de construire un réseau informatique sécurisé permettant de gérer les vulnérabilités et de suivre les correctifs**. Les entreprises se doivent, entre autres, de mettre en place des mécanismes de contrôle d'accès.

Ainsi, sa mise en conformité est un signe fort donné par une entreprise à ses clients et partenaires. Elle indique qu'elle a pris des mesures appropriées pour protéger les données des titulaires de cartes de paiement.

Prévenir
les violations des données bancaires

Construire
et maintenir un réseau sécurisé

Protéger
les porteurs de cartes bancaires

Qui est soumis au PCI DSS ?

Toute organisation qui transmet, traite ou stocke des données bancaires issues des cartes de paiement de se mettre en conformité vis-à-vis de ce standard :

- **Les plateformes de paiement**
- **Les commerçants**
- **Les prestataires de paiement**

evidence by xmco

(1) Payment Card Industry Data Security Standard. **(2)** Payment Card Industry Security Standards Council.

Qui l'exige ?

Les marques, banques, partenaires ou services de cartes de paiement dans un cadre contractuel.
Les partenaires commerciaux en prérequis à un contrat commercial.

Le standard n'est pas obligatoire dans toutes les régions du monde. Seules les cartes appartenant aux réseaux des 5 marques de cartes (American Express, JCB International, MasterCard and Visa Inc, Discover) du PCI SSC requièrent cette conformité. Cela ne concerne pas les transactions avec d'autres réseaux de cartes bancaires comme Unionpay.

Les origines du standard PCI DSS

Selon la Fevad[3], le marché de l'e-commerce a explosé ces 20 dernières années. **Ce sont désormais 103,4 milliards d'euros dépensés en ligne en France en 2020 contre seulement 5,5 milliards en 2004**. Mais le secteur de la finance constate les dérives des fraudes sur les moyens de paiement et la dispersion des programmes normatifs de sécurité, qui pourtant répondent aux mêmes exigences.

L'Observatoire de la sécurité des moyens de paiement met en exergue **une augmentation de la fraude de 7% entre 2018 et 2019**. En valeur ce sont 470 millions d'euros, contre 439 en 2018 qui sont concernés.

Le grand public sollicite de plus en plus des outils, comme la Perceval. La plate-forme permet, après avoir fait opposition auprès de sa banque, de signaler toute utilisation frauduleuse d'une carte bancaire aux forces de l'ordre. **Le Ministère de l'Intérieur annonce qu'en 2018 la plateforme reçoit presque 300 signalements par jour contre 450 par jour en 2019**.

A l'ère d'internet, les banques comme leurs clients doivent disposer d'une référence commune en matière de sécurité et de protection des données.

C'est le constat de cinq sociétés de cartes de paiement qui créent le PCI SSC. Son objectif est d'unifier les règles en matière de sécurité pour les sociétés traitant des données de cartes bancaires.

Les programmes de ces fondateurs sont alors harmonisés sur un standard commun appelé PCI DSS dont la dernière version a vu le jour en mai 2018. Ce standard évolue de manière continue en prenant en

(3) La Fédération du e-commerce et de la vente à distance est l'organisation professionnelle représentative des acteurs du commerce électronique.

compte les nouveaux canaux de paiement, les défis de sécurité liés aux migrations vers des technologies cloud. La version 4.0, aujourd'hui en cours de rédaction, devrait voir le jour en 2021.

Les 3 piliers du PCI DSS

1. **Documentation / Elle sert de référence à toute action de manière à ce que la réalisation d'une quelconque action soit contrôlée et conforme à la procédure associée**. Il faudra alors s'appuyer sur des politiques (PSSI, analyse de risque, gestion des accès...), des procédures (standards de sécurité…), des rapports et compte- rendus (gestion du changement, formulaire des habilitations...).

2. **Organisation /** Pour s'assurer de l'efficacité de cette démarche, il est conseillé d'identifier et de responsabiliser toutes les personnes impliquées sur ce sujet. **Cela impose de définir des responsables, former les parties prenantes et mettre en place des circuits d'information**. L'objectif étant que les mesures de sécurité soient mises en œuvre et maintenues dans le temps.

3. **Configuration /** La conformité n'est pas seulement un mode déclaratif. Il s'agit aussi de l'implémentation technique des mesures de sécurité pour protéger les systèmes impliqués dans le traitement des paiements par carte.

La conformité pour couvrir les risques de vol et de fraude

La carte bancaire est le moyen de paiement favori des acheteurs. **Mais la dématérialisation du paiement par carte ouvre de nombreuses voies aux cybercriminels, faisant des clients des cibles pour les cyberattaques**. Elles peuvent se traduire par des vols de données en ligne ou par des fraudes sur les systèmes de paiement par carte bancaire.

Le PCI DSS est le seul standard qui permet de sécuriser l'environnement qui traite les données de cartes bancaires. Pour protéger entièrement les données personnelles de ses clients il faut aussi suivre les directives annoncées par le RGPD[4].

Les exigences de conformité au PCI DSS correspondent aux bonnes pratiques dans le domaine de la cybersécurité pour protéger les environnements, et rendre le mode de paiement des cartes bancaires plus sûr.

(4) Règlement général sur la protection des données.

2 Le prix d'une cyberattaque et les conséquences du **non-respect du standard PCI DSS**

Toutes les entreprises sont exposées au risque d'une cyberattaque, au point que la question n'est pas de savoir si elles seront attaquées, mais quand ? **Une grande part de ces attaques vise les données personnelles dont les données bancaires**. C'est pourquoi, mesurer les conséquences désastreuses d'une attaque est une étape par laquelle vous devriez passer.

Le risque lié aux attaques informatiques ne cesse de grandir. Et leur coût peut être considérable pour une entreprise, quelle que soit sa taille. **Une étude réalisée par le Ponemon Institute a estimé le coût direct mondial annuel de la cybercriminalité sur les entreprises à 4,5 milliards d'euros jusqu'en 2022**.

Le prix des données bancaires

Les brèches dans les systèmes d'information sont plus fréquentes qu'on ne le croit et exposent les entreprises à des risques de sécurité. **Des cyberattaques qui ciblent en priorité les données personnelles des collaborateurs et celles des clients des entreprises**. Ces informations sont recherchées car elles permettent d'accéder aux comptes bancaires des propriétaires de cartes ou de revendre ces données sur les marchés noirs numériques.

Les cyberattaquants se fournissent sur le Dark Web en malwares, qui sont les vecteurs de ces attaques. Ils bénéficient parfois d'un support pour ces produits !

Une étude réalisée par PrivacyAffairs.com en 2020 confirme que les données bancaires et personnelles sont lucratives :

Le prix d'un malware vari entre 70$ et 6 000$ selon son efficacité et sa diffusion.

Le prix des données de cartes bancaires varie entre 12$ à 65$.

Un compte PayPal se négocie entre 150$ et 320$ selon le crédit disponible.

Un compte de messagerie Gmail s'achète 155$.

Un compte Facebook s'achète 75$.

Le coût d'une fuite de données pour l'entreprise

Les attaques se faisant de plus en plus sophistiquées, le coût d'une cyberattaque pour les entreprises ne cesse d'augmenter. **En 2018, Accenture Security l'avait évalué en moyenne à 9,7 millions d'euros pour les entreprises françaises, avec une progression annuelle de 12%**. Les PME ne sont également pas épargnées et les conséquences sont beaucoup plus importantes pour elles.

A ce coût direct s'ajoutent des coûts cachés, qui dans le cadre des fuites de données bancaires peuvent se révéler très élevés, bien au-delà du seul aspect financier. L'image de l'entreprise est une valeur immatérielle difficile à évaluer, que la médiatisation d'un vol de données personnelles peut très rapidement dégrader.

Les 14 coûts directs et indirects à prendre en compte pour évaluer les conséquences d'une cyberattaque :

Coûts financiers émergés, généralement connus

1. Les enquêtes techniques
2. Les dépenses associées à l'information et au conseil des clients.
3. La mise en conformité réglementaire.
4. Les honoraires d'avocat et frais de justice.
5. La sécurisation des données client post-incident.
6. Les relations publiques.
7. L'amélioration des dispositifs de cybersécurité.

Coûts financiers immergés

1. L'augmentation des primes d'assurance.
2. L'augmentation du coût de la dette.
3. Les impacts liés à la perturbation ou l'interruption des activités.
4. L'érosion du chiffre d'affaires liée à la perte de contrats.
5. La dépréciation de la valeur de marque.
6. La perte de propriété intellectuelle.
7. La perte de la confiance accordée par le client.

Les conséquences d'une violation de données peuvent être désastreuses pour la victime comme pour l'entreprise qui a enregistré ses données dans le cadre d'un paiement. L'adhésion au PCI DSS, vous permet de vous protéger, détecter et répondre aux cyberattaques éventuelles.

Les risques face à la non-conformité au PCI DSS

Seulement 27,9% des entreprises interrogées se déclarent totalement conformes au standard PCI DSS ! Les chiffres publiés par la 10e édition du Payment Security Report (PSR) de Verizon dans le monde sont sans appel : la majorité des organisations ne sont pas préparées à affronter une cyberattaque sur les données bancaires. En Amérique du Nord, moins d'une entreprise sur deux (47,9%) dispose de processus pour surveiller les paiements. La mise en application du PCI DSS est pourtant le moyen d'aligner les objectifs de sécurité avec les objectifs économiques de l'entreprise, en particulier le respect et la sécurité des données de ses clients.

Les entreprises qui procèdent à des paiements en ligne doivent prendre conscience des risques encourus en cas de violation des données. Les législateurs, nationaux et européens, ont bien compris l'importance de protéger les données. Ces dernières années nous avons assisté à une prise de conscience sur les données personnelles qui ont mené à l'instauration du RGPD.

De quels risquent parle-t-on ?

- De perte ou vol de données bancaires.
- D'amendes qui peuvent atteindre plusieurs millions d'euros.
- De modification ou résiliation du contrat par le partenaire financier qui procède au traitement des paiements.
- De l'atteinte à la réputation et de perte de confiance dans votre marque.
- D'un arrêt de production pour votre entreprise.

3 Comment déterminer son SAQ et comment **se mettre en conformité** ?

Les premières étapes pour se mettre en conformité avec le PCI DSS.

Avant toute chose, si vous souhaitez vous mettre en conformité avec le PCI DSS, vous devez **accepter d'assumer la responsabilité de la sécurité des données de vos clients**. La démarche est volontaire, même si le marché ou vos partenaires vous l'imposent, et elle repose sur la confiance.

Vous devez comprendre comment fonctionne le processus de traitement des données bancaires de vos clients. Vous devez **accepter d'intervenir sur ce processus** pour construire, maintenir et protéger un réseau sécurisé avec les mécanismes de contrôle et de sécurité.

Enfin, il est nécessaire de **prendre connaissance de la lourde documentation de 139 pages et des 250 contrôles de sécurité**. C'est ce que nous allons évoquer ici.

Les 4 niveaux de la conformité, ou qui fait quoi ?

Le conseil du standard a adapté les exigences de PCI DSS à la diversité des organisations face au traitement des paiements par cartes bancaires. Cette adaptation s'exprime en 4 niveaux qui prennent en compte le volume de transactions sur 12 mois.

Le conseil définit ces niveaux de conformité à titre indicatif, cependant ce sont les banques d'acquisition qui l'indiquent contractuellement aux marchands. Le conseil distingue aussi deux types d'entreprises : les "*marchands*" et les "*fournisseurs de services*".

Niveau 1 / Un accompagnement obligatoire par un tiers pour :

- Les marchands qui par an traitent plus de 6 millions de transactions Visa ou MasterCard, ou plus de 2,5 millions de transactions American Express.
- Les fournisseurs de services, le "Niveau 1" est requis à partir de 300 000 transactions.

- Les organismes émetteurs de cartes sont considérés "Niveau 1".
- Les entreprises qui ont subi une atteinte à la sécurité des données.

Les entreprises de ce niveau sont invitées à produire :

- **Une évaluation, un rapport et une attestation de conformité annuel** (ROC1[1] et AOC[2]) effectués par un auditeur qualifié en matière de sécurité (QSA[3]) comme notre cabinet XMCO ou par un contrôleur de gestion si le rapport est signé par un dirigeant de la société ;
- **Une analyse trimestrielle** du réseau par un fournisseur d'analyse approuvé (ASV[4]) ;

Niveau 2, 3 et 4 / Le choix de l'auto-évaluation :

Les entreprises qui relèvent de ces trois niveaux (inférieur à 6 millions de transaction pour les marchands ou 300 000 pour les fournisseurs de services) **sont invitées à répondre à des questionnaires d'auto-évaluation**. Il existe 8 questionnaires de ce type, qui diffèrent selon la méthode d'intégration des paiements.

Pour répondre au besoin des entreprises de niveau 2, 3 et 4, ***evidence***® propose une application simple et didactique pour vous auto-évaluer en 3 étapes :

- Déterminez votre type de SAQ[5]
- Remplissez-le avec l'aide en ligne
- Téléchargez-le !

Les 12 exigences de conformité PCI DSS.

Les 250 contrôles de sécurité formulés par le conseil PCI ont été subdivisés en 12 exigences, auxquelles chaque entreprise, commerçant ou fournisseur de services, doit se plier pour être en conformité :

1. Installer, piloter et mettre à jour une configuration avec pare-feu pour protéger les données des titulaires de cartes bancaires.

2. Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe des systèmes et les autres paramètres de sécurité.

3. Protéger les données des titulaires de cartes, ne pas stocker les données critiques (contenu de la bande magnétique, numéro de vérification, numéro d'identification personnel), et chiffrer les données avant de les stocker.

4. Chiffrer la transmission des données des titulaires de cartes sur les réseaux publics ouverts (Internet, Wi-Fi, cellulaire et satellite).

5. Installer, utiliser et mettre régulièrement à jour les logiciels de gestion des vulnérabilités et les antivirus.

6. Développer et maintenir des systèmes et des applications sécurisés, s'assurer de leur mise à jour.

7. Contrôler les accès, restreindre l'accès aux données aux seules personnes autorisées.

8. Attribuer un identifiant unique à chaque personne ayant accès à un ordinateur, et conserver un historique de ces accès.

9. Limiter et surveiller l'accès physique aux données des cartes bancaires, réglementer ces accès, détruire les supports qui ne sont plus actifs.

10. Contrôler, tracer, surveiller tous les accès aux ressources réseaux et aux données des titulaires de cartes. Les contrôles doivent être journalisés via des pistes d'audit sécurisées afin de détecter et contenir les risques de violations de données. Et les journaux doivent être audités régulièrement.

11. Tester régulièrement les systèmes et processus de sécurité via des tests d'intrusion menés chaque année et après toute modification importante sur le réseau.

12. Maintenir une politique de sécurité des informations pour les employés et les prestataires. Instaurer un programme de sensibilisation et l'alimenter ou le reproduire régulièrement. Communiquer sur les nouveaux protocoles de sécurité.

Les 3 axes de la sécurité des données

Pour les entreprises qui ont fait le choix de collecter et transmettre des données de cartes bancaires de leurs clients, la conformité complète au PCI DSS s'impose. Pour toutes celles qui n'en ont pas le besoin et passent par un prestataire certifié, le nombre de contrôles applicables se trouve réduit. Nous identifions 3 axes principaux :

1. La gestion des données des cartes bancaires : l'entreprise doit collecter et transmettre les données sensibles des cartes bancaires de ses clients en toute sécurité. Elle doit respecter les contrôles du PCI DSS qui s'appliquent à sa structure.

2. La sauvegarde sécurisée des données : avec le chiffrement, le contrôle en continu et les tests de sécurité de l'accès aux données.

3. Le maintien annuel de la conformité : le formulaire de validation doit être complété chaque année. Les contrôles et le niveau de sécurité doivent être maintenus tout au long de l'année.

Un accompagnement nécessaire. Les exigences sont pour la plupart assez simples et relèvent du bon sens mais leur mise en application se révèle plus complexe. Vous pouvez agir seul ou vous faire accompagner pour piloter et suivre un projet de mise en conformité PCI DSS.

(1) ROC : Rapport de conformité contenant des détails sur la conformité d'une entité à la norme PCI DSS. **(2)** Formulaire utilisé par les commerçants et les prestataires de services pour attester des résultats d'une évaluation PCI DSS. **(3)** Un QSA est une personne ou une société autorisée par le PCI SSC à valider l'adhésion d'une organisation aux exigences du PCI DSS. **(4)** ASV : Société agréée par le PCI SSC pour offrir des services d'analyse des vulnérabilités externes. **(5)** Un SAQ est un questionnaire d'auto-certification défini par le PCI SSC donnant la possibilité aux marchands de niveau 2, 3 et 4 de se certifier PCI DSS. Il existe 8 types de SAQ, ils sont attribués en fonction de la méthode d'intégration des paiements.

4 e-commerce : entre RGPD et PCI DSS

La carte bancaire joue un rôle central dans la transaction entre le commerçant et son client. Par conséquent, la sécurité des données personnelles et bancaires, soumises respectivement au RGPD[1] et au PCI DSS, est essentielle et presque induite pour le client.

L'e-commerce ne cesse de se développer !

- En 2019, selon l'Observatoire CB, 71 millions de cartes bancaires en France, distribuées par les prestataires de services de paiement, ont permis d'effectuer environ **500 milliards d'euros de paiements par cartes bancaires**. Sur cette même période, le nombre total de paiements CB a progressé de 8,8 % en volume et 6,4 % en valeur.

- Pendant le premier semestre 2020, malgré ou à cause de la crise Covid, **les ventes e-commerce et à distance ont affiché une croissance de 4,5 %**. Un succès que l'usage du Click & Collect devrait renforcer.

Chaque transaction de paiement en ligne expose les données personnelles et bancaires de l'acheteur, et elle est soumise pour le vendeur à une obligation de sécurité. Il existe 2 règlementations qui peuvent y répondre : **le RGPD[1] pour la protection des données personnelles et le PCI DSS pour la protection des données personnelles bancaires**.

La carte bancaire face au RGPD

L'identité de l'acheteur est incontournable dans l'acte d'achat en ligne. Votre entreprise peut conserver ces informations qui vont alimenter votre base clients. Leur usage s'exerce dans le cadre du RGP.

(1) Règlement général européen sur la protection des données.

Il est nécessaire de recueillir le consentement du client pour conserver ses données. Cela doit prendre la forme d'un acte de volonté univoque, par exemple au moyen d'une case à cocher.

Pour les données bancaires, **le RGPD nous apprend que les commerçants doivent envisager leurs systèmes de paiement en tenant compte des principes de protection des données, dès leur conception**.
Nous comprenons que les données strictement nécessaires - numéro de la carte, date d'expiration, cryptogramme visuel - ne doivent pas être conservées au-delà de la transaction.

Le cas particulier des paiements récurrents et des paiements "on-click". Il existe des cas particuliers qui visent à faciliter les achats. **Ils permettent au commerçant de conserver légitimement les données bancaires des clients qui souscrivent à une offre, pour les exploiter lors des prochaines transactions**.

En souscrivant à un abonnement complémentaire, le client affiche sa volonté de s'inscrire dans une relation régulière avec le commerçant afin de pouvoir acheter fréquemment et facilement. C'est ainsi que lors de l'acte de paiement les coordonnées bancaires du client peuvent s'afficher directement, sans que celui-ci n'ait à les re-saisir.

La CNIL stipule que la conservation des données bancaires peut s'exercer sous réserve de :

- fournir une information complète ;
- permettre d'exercer facilement un droit d'opposition via une case à cocher ;
- permettre facilement et à tout moment la suppression des données bancaires ;
- tenir compte du refus exprimé par le client ;
- mettre en œuvre des mesures de sécurité appropriées.

RGPD et PCI DSS

Dans le cadre du RGPD, l'e-marchand est soumis aux obligations de protection des données personnelles de ses clients, dont les données bancaires sont une composante. Le non-respect de ces obligations, la non-conformité, et perte ou le vol de données peuvent entraîner des sanctions administratives, qui se révèlent dissuasives :

- Une amende de 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour le non-respect des obligations incombant au responsable du traitement et au sous-traitant, à l'organisme de certification et à l'organisme de suivi des codes de conduite ;

- Une amende de 20 millions d'euros ou 4 % du chiffre d'affaires mondial pour le non-respect de l'obligation de consentement et des autres droits des personnes concernées, l'obligation de mettre en place des mesures spécifiques en cas de transferts des données dans un pays non européen, des obligations découlant des droits des États membres, des injonctions et autres mesures de remise à l'ordre prononcées par la CNIL.

Les sanctions administratives ne se substituent pas aux sanctions pénales. Une entreprise qui manque à ses obligations peut donc aussi être poursuivie en justice par les victimes.

- Les peines prononcées peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende selon la gravité des infractions.

Les données de carte bancaire entrent dans la définition des données à caractère personnel introduite par le RGPD. Les entreprises qui doivent appliquer le standard PCI DSS doivent également être conformes au RGPD. Les deux textes se rejoignent dans un objectif commun, protéger les données des clients.

La démarche de conformité PCI DSS pour un e-commerçant

Même si la démarche est volontaire, donc en théorie non soumise à une obligation, l'e-commerçant a donc tout intérêt à adopter la conformité au PCI DSS comme une bonne pratique pour auditer sa cybersécurité et prouver sa conformité par le biais d'une simple auto-évaluation.

Si vous déployez votre propre méthode de paiement, la conformité PCI DSS est un gage de confiance à ne pas négliger. Si vous adhérez à une plateforme de distribution et de paiement, vous devrez vous assurez que vos propres processus sont conformes. Dans beaucoup de cas, c'est votre banque qui vous demandera la certification ; afin d'apporter une garantie.

5 Les 3 conseils de notre expert PCI DSS pour **se lancer sereinement**

Définissez vos objectifs

• S'agit-il d'établir la confiance avec votre banque, vos partenaires, et vos clients ? Ou plutôt de compléter votre mise en place du RGPD ? Ou encore de suivre les bonnes pratiques de sécurité informatique du standard reconnues par l'ensemble du marché ?

Choisissez votre stratégie

Définissez votre périmètre de certification en fonction de vos besoins métier et de votre environnement. Préférez-vous vous appuyer sur un fournisseur de services ? Vous auto-évaluer ? Faire appel à des experts pour gérer votre mise en conformité ?

Si vous n'avez pas besoin de traiter ou de stocker des données de cartes bancaires, ne le faites pas !

Se faire accompagner

Pour gagner du temps dans votre auto-évaluation ou pour choisir votre type de SAQ[1], faites le choix de la simplicité face à ce standard complexe et entourez-vous d'experts.

Stéphane Marcault, expert sécurité et auditeur PCI QSA, répond à nos questions et explique comment fonctionne ***evidence®***, l'application française d'auto-évaluation au PCI DSS.

Pourquoi les entreprises doivent-elles se soumettre à la démarche de conformité PCI DSS ?

[SM] La carte bancaire est un moyen de paiement largement utilisé pour les ventes dématérialisées. Mais le paiement et les données de cartes bancaires sont soumis à énormément de menaces.

Le PCI DSS est un standard mondial de sécurité des données liées aux cartes de paiement, créé et reconnu par les opérateurs des cartes bancaires. **C'est pourquoi le PCI DSS concerne toutes les entreprises qui enregistrent des transactions.**

Son respect permet d'établir une véritable confiance avec sa banque, ses partenaires, et les clients qui paient en ligne.

Pour autant, la certification n'est pas obligatoire ?

[SM] En effet, d'ailleurs **la démarche de certification est rarement volontaire !** C'est souvent à la demande des banques et des fournisseurs de services, ou par la crainte du RGPD que le marchand cherche à se mettre en conformité vis-à-vis du standard PCI DSS.

C'est pourquoi certains préfèrent recourir à des fournisseurs de services certifiés, sur lesquels ils reportent la responsabilité des paiements. D'autres stratégies peuvent également être adoptées comme ne pas s'orienter vers la certification… **Néanmoins, si l'entreprise souhaite gérer les paiements, il lui est fortement conseillé de se mettre en conformité au PCI DSS.**

La mise en conformité peut être segmentée de la manière suivante :

- 1/3 de documentation ;
- 1/3 de procédure ;
- 1/3 de moyens de sécurité.

Il est conseillé de faire un appel à un expert dans le cas où vous n'avez pas toutes les compétences et ressources en interne.

Comment se déroule une démarche de certification ?

[SM] **C'est une démarche qui demande de comprendre l'activité et le métier de l'entreprise afin de définir le périmètre de la certification, mais également d'identifier les flux de cartes bancaires** et par où ils passent. Cette étape préliminaire permet ainsi d'inventorier les équipements et les composants réseaux pour définir un périmètre d'application du standard. Forte de l'analyse de son environnement, l'entreprise pourra alors définir une stratégie de certification.

En fonction de la stratégie déterminée, l'entreprise devra répondre à un ensemble d'exigences présentes dans le questionnaire SAQ. L'entreprise devra mettre en œuvre un ensemble d'actions pour répondre positivement à toutes les exigences du SAQ.

En quoi le service evidence® by XMCO peut-il aider à se certifier ?

[SM] ***evidence***® est une application en ligne qui facilite la démarche de mise en conformité PCI DSS en 3 étapes. **La première étape consiste à déterminer son type de SAQ. La seconde étape consiste à remplir le SAQ et enfin la dernière étape est la communication de ces éléments à sa banque.**

Nous proposons un parcours simple et didactique adapté à de nombreux profils métiers.

***evidence*® accompagne dans l'auto-évaluation PCI DSS, aide à la compréhension et à la mise à niveau des marchands et autres prestataires de services.**
Notre objectif est de simplifier au maximum le processus de mise en conformité cependant, la responsabilité finale incombera toujours à l'entreprise.

Et si l'auto-évaluation proposée par evidence® ne suffit pas ?

[SM] Pour les cas qui « *sortent des cases* » des SAQ classiques, nous proposons un accompagnement personnalisé.

Avoir recours à un cabinet de conseil, à la différence de l'auto-évaluation SAQ, permet d'obtenir une attestation signée par un cabinet certifié QSA , et assure ainsi un transfert de la responsabilité et de la conformité avec les partenaires et les banques.

(1) Un SAQ est un questionnaire d'auto-certification défini par le PCI SSC donnant la possibilité aux marchands de niveau 2, 3 et 4 de se certifier PCI DSS. Il existe 8 types de SAQ, ils sont attribués en fonction de la méthode d'intégration des paiements. **(2)** Un QSA est une personne ou une société autorisée par le PCI SSC à valider l'adhésion d'une organisation aux exigences du PCI DSS.

Ce livre blanc n'aurait été possible sans l'aide de Yves Granmontagne ainsi que l'expertise et l'énergie de toute l'équipe ***evidence*®** *by XMCO.*

Remerciements

evidence by xmco®

L'application française qui simplifie votre mise en conformité **PCI DSS**

- Une **application** SaaS développée par les QSA XMCO
- Des conseils d'**experts** et un accompagnement à chaque étape jusqu'à votre **auto-évaluation**
- Un parcours de questions, simple et didactique, **adapté à votre contexte métier**
- Un SAQ **pré-rempli** détaillant toutes les exigences sur le PCI DSS
- Des **modules de formations** pédagogiques pour sensibiliser vos équipes

www.evidence.xmco.fr

© plusdebleu.com - Crédits photo : ©xmco, ©AdobeStock.com

xmco®
we deliver security expertise since 2002

Acteur français indépendant, XMCO est un cabinet de conseil et d'experts en cybersécurité depuis 2002. XMCO est accrédité PCI QSA depuis 2009. Grâce à son expertise et sa vision pragmatique, le cabinet a su acquérir la confiance de nombreux acteurs et dans tous les domaines.

www.www.xmco.fr