

LES SERVICES D'ABOVE SÉCURITÉ



Pourquoi se conformer aux normes PCI DSS?

Les organisations décident de se conformer aux normes du PCI Security Standards Council pour plusieurs raisons. Souvent, la motivation vient des partenaires; parce que le volume de transaction est élevé ou à la suite d'un incident de sécurité. Parfois, les organisations décident elles-mêmes de s'y conformer. Peu d'organisations veulent rejoindre les rangs de celles qui ont vécu une fraude majeure!

Peu importe la raison, se conformer aux normes PCI DSS permet à une organisation de limiter de façon importante ses risques informationnels.

Qu'est-ce que la norme PCI DSS?

PCI DSS, la norme de sécurité des données reliées à l'industrie des cartes de paiement (de l'anglais « **Payment Card Industry Data Security Standard** »), est un ensemble complet de conditions de sécurité pour les sociétés qui traitent, transmettent ou conservent les données de cartes de paiement. Cette norme a pour objectif d'aider les organisations en protégeant activement les données des comptes client. Elle reflète la majorité des meilleures pratiques adoptées pour protéger les informations confidentielles.

Ces meilleures pratiques incluent les exigences pour la gestion de la sécurité, les politiques, les procédures, l'architecture réseau, la conception logicielle et d'autres mesures de protection critiques. Les commerçants et les prestataires de service qui font la transaction, la conservation ou le traitement de l'information de comptes de cartes de paiement doivent adhérer aux 12 principes de sécurité, regroupés dans les six objectifs suivants :

- Création et gestion d'un réseau sécurisé
- Protection des données des titulaires des cartes de crédit
- Mise à jour d'un programme de gestion des vulnérabilités
- Mise en œuvre de mesures de contrôle d'accès strictes
- Surveillance et test réguliers des réseaux
- Gestion d'une politique de sécurité des informations

Quelles sont les exigences du standard PCI DSS?

Tel que demandé par les différentes marques de cartes de paiement, les commerçants ainsi que les prestataires de service doivent se conformer au standard PCI DSS dans sa totalité. De plus, chaque marque de carte de paiement a son propre programme de conformité comme façon de promouvoir l'adoption du standard. D'après la quantité des transactions, le modèle d'affaires, et d'après d'autres critères additionnels, les marques des cartes de paiement ont défini des exigences et validations de conformité spécifiques. Ces exigences de validation vont du questionnaire d'auto-évaluation à l'évaluation annuelle devant être effectuée sur place par un évaluateur de sécurité qualifié (Qualified Security Assessor, QSA).

Quelles sont les implications de la non-conformité?

Le non-respect de la conformité peut entraîner de sévères pénalités, incluant l'obligation de payer des amendes, la hausse des frais de transaction ou la perte du droit d'accès aux ressources d'un réseau de cartes de paiement.



Conformité à PCI – DSS

Les émetteurs de cartes de crédit accordent une grande importance à ces exigences. Par exemple, en 2006, Visa a perçu 4,6 millions de dollars en amendes versus 3,4 millions en 2005. Cet émetteur de cartes a annoncé que les commerçants qui gardent les données confidentielles des cartes de crédit seront passibles d'amendes allant jusqu'à 10 000 \$ par mois. *American Express*, pour sa part, condamne les commerçants à des amendes allant jusqu'à 15 000 \$ par jour lors du non-respect de la conformité et leur impose l'emploi d'un prestataire de tierce partie pour s'assurer de rendre les systèmes conformes.

Comment Above Sécurité peut vous aider dans vos efforts vers la conformité PCI DSS?

En tant qu'évaluateur de sécurité qualifié (*Qualified Security Assessor, QSA*) et profitant d'une grande expertise dans le domaine de la sécurité de l'information, Above Sécurité possède les compétences nécessaires pour vous fournir l'ensemble des services professionnels pour accompagner votre organisation vers la conformité PCI DSS :

Analyse d'écart PCI DSS. Il s'agit d'une évaluation complète des mesures de sécurité par rapport aux exigences du PCI DSS. Le résultat de ce processus orientera vos efforts vers l'amélioration de votre posture de sécurité d'un point de vue du personnel, des procédures, ainsi que de la technologie, et vous aidera à vous conformer au standard PCI DSS.

Des services conseils pour la conception d'une architecture réseau sécurisée.

Une adéquate segmentation peut en effet aider votre organisation à réduire la portée ainsi que les coûts de l'évaluation PCI DSS. Les experts d'Above Sécurité peuvent réviser et évaluer la conception de votre réseau actuel afin de vous fournir des recommandations qui faciliteront la conformité au standard PCI DSS.

Des évaluations annuelles PCI DSS sur place. Tel que requis par le standard PCI DSS, cette évaluation consiste en une vérification complète du programme de sécurité de l'information établi par votre société en relation avec les obligations PCI (incluant toutes les composantes impliquées dans la transmission, la conservation et le traitement de l'information de cartes de paiement). Après l'évaluation satisfaisante de tous les contrôles PCI DSS, une « **Attestation de Conformité** » sera délivrée à votre banque acquéreur ainsi qu'à votre marque de carte de paiement comme une déclaration de votre état de conformité avec le standard PCI DSS.

Une assistance lorsque le questionnaire d'auto-évaluation PCI DSS doit être rempli. Ce service est conçu pour les commerçants et les prestataires de services qui ne sont pas soumis à la conduite d'une évaluation annuelle sur site. Dans ce cas, les experts d'Above Sécurité vous aideront à identifier le questionnaire d'auto-évaluation approprié selon les spécificités de votre modèle d'affaires, le volume des transactions effectuées et les exigences additionnelles de la part de votre marque de carte de paiement. Nos experts vous guideront lors du processus de remplissage du questionnaire et de la production du document d'« **Attestation de Conformité** ».

Le logo Qualified Security Assessor du PCI Security Standards Council est une marque de commerce du PCI Security Standards Council aux États-Unis d'Amérique et dans les autres pays. Above sécurité a complété avec succès le processus d'accréditation pour être un évaluateur de qualité certifié.

Contactez-nous:

1919, boul. Lionel-Bertrand
Bureau 203
Boisbriand, Qc J7H 1N8
Canada

Téléphone:
1- 450-430-8166

Sans frais (Amérique du Nord):
1-866-430-8166

info@abovesecurite.com

www.abovesecurite.com



ABOVE SÉCURITÉ
L'INTÉGRITÉ AVANT TOUT DEPUIS 1999