



**Payment Card Industry (PCI)
Data Security Standard**

Questionnaire d'auto-évaluation A et attestation de conformité

**Aucun stockage, traitement ou transmission
électronique des données de titulaire de carte**

Version 1.2

Octobre 2008

Modifications apportées au document

Date	Version	Description
1 ^{er} octobre 2008	1.2	Aligner le contenu avec la nouvelle procédure PCI DSS v1.2 et implémenter les changements mineurs notés depuis la v1.1 d'origine.

Table des matières

Modifications apportées au document	i
Normes PCI DSS : Documents connexes	ii
Avant de commencer	iii
Compléter le questionnaire d’auto-évaluation	iii
Étapes de mise en conformité avec les normes PCI DSS	iii
Directives sur la non-applicabilité de certaines exigences spécifiques	iii
Attestation de conformité, SAQ A	1
Questionnaire d’auto-évaluation A	4
Mise en œuvre de mesures de contrôle d’accès strictes	4
<i>Exigence 9 : Restreindre l’accès physique aux données de titulaire de carte</i>	4
Gestion d’une politique de sécurité des informations	5
<i>Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants</i>	5
Annexe A : (non utilisée)	6
Annexe B : Contrôles compensatoires	7
Annexe C : Fiche de contrôles compensatoires	9
Fiche de contrôles compensatoires – Exemple complété	10
Annexe D : Explication de non-applicabilité	11

Normes PCI DSS : Documents connexes

Les documents suivants ont été conçus de manière à aider les commerçants et les prestataires de services à comprendre les normes PCI DSS et le questionnaire d'auto-évaluation PCI DSS.

Document	Public
<i>Normes de sécurité des données de la PCI : Conditions et procédures d'évaluation de sécurité</i>	Tous les commerçants et les prestataires de services
<i>Navigation dans les normes PCI DSS : Comprendre l'objectif des exigences</i>	Tous les commerçants et les prestataires de services
<i>Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation</i>	Tous les commerçants et les prestataires de services
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation A et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation B et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation C et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation D et attestation</i>	Commerçants ¹ et tous les prestataires de services
<i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>	Tous les commerçants et les prestataires de services

¹ Pour déterminer le questionnaire d'auto-évaluation approprié, consultez le document *Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation*, « Sélection du questionnaire d'auto-évaluation et de l'attestation les plus appropriés pour votre entreprise ».

Avant de commencer

Compléter le questionnaire d'auto-évaluation

Le SAQ A a été conçu pour répondre aux besoins des commerçants qui ne conservent que des reçus ou des rapports sur papier avec les données de titulaire de carte, qui ne stockent aucune donnée de titulaire de carte au format électronique et qui ne traitent ou ne transmettent aucune donnée de titulaire de carte dans leurs locaux.

Ces commerçants, répondant au type de validation SAQ 1 selon ce document et les instructions et directives sur le questionnaire d'auto-évaluation PCI DSS, ne stockent aucune donnée de titulaire de carte au format électronique, ne traitent ou ne transmettent aucune donnée de titulaire de carte dans leurs locaux. Ils doivent obtenir une validation de conformité en complétant le SAQ A et l'attestation de conformité associée, en confirmant les éléments suivants :

- Votre entreprise ne traite que des transactions carte absente (commerce électronique ou commande par courrier/téléphone).
- Votre entreprise ne stocke, ne traite ou ne transmet aucune donnée de titulaire de carte dans vos locaux. La gestion de toutes ces fonctions est confiée à un ou plusieurs prestataires de services tiers.
- Votre entreprise est en mesure de confirmer la conformité de la gestion du ou des prestataires de services tiers en matière de stockage, de traitement et/ou de transmission de données de titulaire de carte avec les normes PCI DSS.
- Votre entreprise ne conserve que des reçus ou des rapports sur papier avec les données de titulaire de carte, et ces documents ne sont pas reçus au format électronique.
- Votre entreprise ne stocke aucune donnée de titulaire de carte au format électronique.

Cette option ne peut s'appliquer aux commerçants avec un environnement de point de vente en face-à-face.

Étapes de mise en conformité avec les normes PCI DSS

1. Complétez le questionnaire d'auto-évaluation (SAQ A) conformément aux instructions du document *Instructions et directives sur l'auto-évaluation*.
2. Complétez l'attestation de conformité dans son intégralité.
3. Envoyez le questionnaire et l'attestation de conformité, avec tout autre justificatif requis, à votre acquéreur.

Directives sur la non-applicabilité de certaines exigences spécifiques

Non-applicabilité : Les exigences jugées non applicables à votre environnement doivent être définies comme telles par la mention « s.o. » dans la colonne « Spécial » du SAQ. Vous devez compléter la fiche d'explication de non-applicabilité dans l'annexe pour chaque entrée « s.o. ».

Attestation de conformité, SAQ A

Instructions de transmission

Le commerçant doit compléter cette attestation de conformité pour confirmer son statut de conformité avec le document *Normes de sécurité des données de la Payment Card Industry (PCI DSS) – Conditions et procédures d'évaluation de sécurité*. Il doit ensuite compléter toutes les sections applicables et se reporter aux instructions de transmission au niveau de « Étapes de mise en conformité avec les normes PCI DSS » dans ce document.

Partie 1. Informations sur la société QSA (le cas échéant)

Nom de l'entreprise :					
Nom du principal contact QSA :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 2. Informations sur le commerçant

Nom de l'entreprise :		DBA(s) :			
Nom du contact :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 2a. Type d'entreprise du commerçant (cocher toutes les cases adéquates)

- Détaillant
 Télécommunications
 Épicerie et supermarchés
 Pétrole
 Commerce électronique
 Commande par courrier/téléphone
 Autres (préciser) :

Indiquer les installations et les sites inclus dans l'examen PCI DSS :

Partie 2b. Relations

Votre société entretient-elle une relation avec un ou plusieurs prestataires de services tiers (par exemple, passerelles, prestataires de services d'hébergement sur le Web, tour opérateurs, agents de programmes de fidélité, etc.) ? Oui Non

Votre société entretient-elle une relation avec plusieurs acquéreurs ? Oui Non

Partie 2c. Conditions à remplir pour compléter le SAQ A

Le commerçant déclare être en droit de compléter cette version abrégée du questionnaire d'auto-évaluation en confirmant les éléments suivants :

<input type="checkbox"/>	Le commerçant ne stocke, ne traite ou ne transmet aucune donnée de titulaire de carte dans ses locaux. La gestion de toutes ces fonctions est confiée à un ou plusieurs prestataires de services tiers.
<input type="checkbox"/>	La gestion du ou des prestataires de services tiers en matière de stockage, de traitement et/ou de transmission de données de titulaire de carte est conforme aux normes PCI DSS.
<input type="checkbox"/>	Le commerçant ne stocke aucune donnée de titulaire de carte au format électronique.
<input type="checkbox"/>	Si le commerçant stocke des données de titulaire de carte, il s'agit uniquement de copies ou de rapports sur papier des reçus, et ces documents ne sont pas reçus au format électronique.

Partie 3. Validation PCI DSS

Suite aux résultats du SAQ A du (*completion date*), (*Merchant Company Name*) déclare le statut de conformité suivant (cocher une case) :

- Conforme** : Toutes les sections du SAQ PCI sont complétées et toutes les questions ont reçu la réponse « Oui », d'où une note globale **CONFORME**. (*Merchant Company Name*) est donc en conformité avec les normes PCI DSS.
- Non conforme** : Toutes les sections du SAQ PCI ne sont pas complétées ou certaines questions ont reçu la réponse « Non », d'où une note globale **NON CONFORME**. (*Merchant Company Name*) n'est donc pas en conformité avec les normes PCI DSS.
- **Date cible** de mise en conformité :
 - Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à compléter le plan d'action décrit dans la Partie 4 de ce document. Vérifier cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.

Partie 3a. Confirmation de l'état de conformité

Le commerçant confirme les éléments suivants :

<input type="checkbox"/>	Le questionnaire d'auto-évaluation A des normes PCI DSS, version (<i>SAQ version #</i>), a été complété conformément aux instructions fournies dans ce document.
<input type="checkbox"/>	Toutes les informations présentes dans le questionnaire d'auto-évaluation susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de l'évaluation.
<input type="checkbox"/>	J'ai lu les normes PCI DSS et m'engage à garantir ma conformité avec leurs exigences à tout moment.

Partie 3b. Accusé de réception du commerçant

Signature du représentant du commerçant ↑	Date ↑
Nom du représentant du commerçant ↑	Poste occupé ↑
Nom de l'entreprise représentée ↑	

Partie 4. Plan d'action en cas d'état Non conforme

Sélectionner l'état de conformité approprié pour chaque condition. Si la réponse « Non » est donnée à la moindre condition, indiquer la date à laquelle la société devra se mettre en conformité et une brève description des actions à mettre en œuvre à cette fin. Vérifier cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.

Exigences PCI DSS	Description de l'exigence	État de conformité (cocher une seule option)		Date et actions de mise en conformité (si l'état de conformité est « Non »)
		OUI	NON	
9	Restreindre l'accès physique aux données de titulaire de carte	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gérer une politique de sécurité des informations	<input type="checkbox"/>	<input type="checkbox"/>	

Questionnaire d'auto-évaluation A

Date de réalisation :

Mise en œuvre de mesures de contrôle d'accès strictes

Exigence 9 : Restreindre l'accès physique aux données de titulaire de carte

Question	Réponse :	Oui	Non	Spécial*
9.6	Tous les documents papier et les supports électroniques contenant des données de titulaire de carte sont-ils rangés physiquement en lieu sûr ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) La distribution interne ou externe de tout type de support contenant des données de titulaire de carte est-elle soumise à un contrôle strict ?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les contrôles incluent-ils les procédures suivantes :			
9.7.1	Les supports sont-ils classifiés de manière à les identifier comme contenant des informations confidentielles ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Des processus et procédures sont-ils mis en place pour garantir l'obtention de l'approbation des responsables avant de déplacer tout ou partie des supports contenant des données de titulaire de carte d'une zone sécurisée (en particulier s'ils sont distribués à des personnes) ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Le stockage et l'accessibilité des supports contenant des données de titulaire de carte font-ils l'objet d'un contrôle strict ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Les supports contenant des données de titulaire de carte sont-ils détruits lorsqu'ils ne sont plus nécessaires à des fins commerciales ou juridiques ? La destruction peut prendre diverses formes :	<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de manière à ce qu'il soit impossible de les reconstituer ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Gestion d'une politique de sécurité des informations

Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants

Question		Réponse :	Oui	Non	Spécial*
12.8	Si des données de titulaire de carte sont partagées avec des prestataires de services, des politiques et procédures sont-elles mises en œuvre pour gérer les prestataires de services, et incluent-elles les éléments suivants ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	Une liste des prestataires de services est tenue.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Un accord écrit par lequel les prestataires de services se reconnaissent responsables de la sécurité des données de titulaire de carte en leur possession a été signé.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Un processus de sélection des prestataires de services est bien défini et inclut notamment des contrôles préalables à l'engagement.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Un programme est mis en place pour contrôler la conformité des prestataires de services avec les normes PCI DSS.		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Annexe A : (non utilisée)

Page laissée vide intentionnellement.

Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux exigences PCI DSS telles qu'elles sont stipulées, en raison de contraintes commerciales documentées ou de contraintes techniques légitimes, mais qu'elle a parallèlement suffisamment atténué les risques associés par la mise en œuvre d'autres contrôles, appelés « contrôles compensatoires ».

Les contrôles compensatoires doivent satisfaire aux critères suivants :

1. Respecter l'intention et la rigueur de l'exigence initiale des normes PCI DSS.
2. Fournir une protection similaire à celle de l'exigence initiale des normes PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par l'exigence initiale. (Pour plus d'informations sur chaque exigence PCI DSS, voir *Navigation dans les normes PCI DSS*.)
3. Aller au-delà des autres exigences PCI DSS. (Les contrôles compensatoires ne consistent pas simplement en la conformité avec d'autres exigences PCI DSS.)

Lors de l'évaluation de la portée des contrôles compensatoires, il est essentiel de considérer les points suivants :

Remarque : Les points a) à c) ci-dessous sont cités à titre d'exemple seulement. L'évaluateur qui effectue l'examen des normes PCI DSS doit déterminer et valider la suffisance de tous les contrôles compensatoires. L'efficacité d'un contrôle compensatoire dépend des caractéristiques spécifiques de l'environnement dans lequel il est mis en œuvre, des contrôles de sécurité associés et de la configuration du contrôle proprement dit. Les entreprises doivent avoir conscience qu'un contrôle compensatoire particulier ne sera pas efficace dans tous les environnements.

- a) Les exigences existantes des normes PCI DSS NE peuvent PAS être considérées comme des contrôles compensatoires si elles sont déjà exigées pour l'élément examiné. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être transmis sous forme cryptée afin de limiter les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut pas utiliser d'autres exigences relatives aux mots de passe des normes PCI DSS (blocage des intrus, mots de passe complexes, etc.) pour compenser l'absence de mots de passe cryptés, puisque celles-ci ne limitent pas les risques d'interception des mots de passe en texte clair. Par ailleurs, les autres contrôles de mots de passe sont déjà exigés par les normes PCI DSS pour l'élément examiné (à savoir les mots de passe).
- b) Les exigences existantes des normes PCI DSS PEUVENT être considérées comme des contrôles compensatoires si elles sont exigées dans un autre domaine, mais pas pour l'élément examiné. Par exemple, l'authentification à deux facteurs est exigée par les normes PCI DSS pour l'accès à distance. L'authentification à deux facteurs *à partir du réseau interne* peut aussi être considérée comme un contrôle compensatoire de l'accès administrateur non-console lorsque la transmission des mots de passe cryptés ne peut pas être prise en charge. L'authentification à deux facteurs peut être un contrôle compensatoire acceptable dans les conditions suivantes : (1) elle satisfait l'intention de l'exigence initiale en résolvant les risques d'interception des mots de passe administrateur en texte clair, et (2) elle est correctement configurée et elle est mise en œuvre dans un environnement sécurisé.
- c) Les exigences existantes des normes PCI DSS peuvent être associées à de nouveaux contrôles et constituer alors un contrôle compensatoire. Par exemple, si une société n'est pas en mesure de rendre les données de titulaire de carte illisibles conformément à l'exigence 3.4 (par exemple, par cryptage), un contrôle compensatoire pourrait consister en un dispositif ou un ensemble de dispositifs, d'applications et de contrôles qui assurent : (1) la segmentation du réseau interne ; (2) le filtrage des adresses IP ou MAC ; et (3) l'authentification à deux facteurs à partir du réseau interne.

4. Être proportionnel aux risques supplémentaires qu'implique le non-respect de l'exigence PCI DSS.

L'évaluateur doit évaluer soigneusement les contrôles compensatoires pendant chaque évaluation annuelle des normes PCI DSS afin de confirmer que chaque contrôle compensatoire couvre de manière appropriée le risque ciblé par l'exigence initiale des normes PCI DSS, conformément aux points 1 à 4 présentés ci-dessus. Pour maintenir la conformité, des processus et des contrôles doivent être en place pour garantir que les contrôles compensatoires restent efficaces après l'évaluation.

Annexe C : Fiche de contrôles compensatoires

Se référer à cette fiche pour définir des contrôles compensatoires pour toute exigence où la case « Oui » a été cochée et où des contrôles compensatoires ont été mentionnés dans la colonne « Spécial ».

Remarque : Seules les entreprises qui ont procédé à une analyse des risques et ont des contraintes commerciales documentées ou des contraintes technologiques légitimes peuvent envisager l'utilisation de contrôles compensatoires pour se mettre en conformité.

Numéro et définition des exigences :

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	

Fiche de contrôles compensatoires – Exemple complété

Se référer à cette fiche pour définir des contrôles compensatoires pour toute exigence où la case « Oui » a été cochée et où des contrôles compensatoires ont été mentionnés dans la colonne « Spécial ».

Numéro d'exigence : 8.1—*Tous les utilisateurs sont-ils identifiés avec un nom d'utilisateur unique qui les autorise à accéder aux composants du système ou aux données de titulaire de carte ?*

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	<i>La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « root ». La société XYZ ne peut pas gérer le nom d'utilisateur « root » ni consigner toutes les activités de chaque utilisateur « root ».</i>
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	<i>L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des informations d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière.</i>
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	<i>L'absence d'ID d'utilisateur unique et le fait de ne pas pouvoir consigner les informations d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.</i>
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	<i>Une société XYZ va demander à tous les utilisateurs de se connecter aux serveurs à partir de leur Bureau à l'aide de la commande SU. Cette commande autorise les utilisateurs à accéder au compte « root » et à exécuter des actions sous ce compte, tout en permettant de consigner leurs activités dans le répertoire du journal SU. Il est ainsi possible de suivre les actions de chaque utilisateur par le biais du compte SU.</i>
7. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	<i>La société XYZ démontre à l'évaluateur l'exécution de la commande SU et lui montre que celle-ci permet d'identifier les utilisateurs connectés qui exécutent des actions sous le compte « root ».</i>
8. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	<i>La société XYZ décrit les processus et les procédures mis en place pour éviter la modification, l'altération ou la suppression des configurations SU de sorte que des utilisateurs individuels puissent exécuter des commandes root sans que leurs activités soient consignées ou suivies.</i>

