Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation A
et attestation de conformité

Toutes les fonctions de données de titulaire de carte sous-traitées. Aucun stockage, traitement ou transmission électronique des données de titulaire de carte

Version 2.0

Octobre 2010

Modifications apportées au document

Date	Version	Description
1er octobre 2008	1.2	Harmonisation du contenu avec les nouvelles normes PCI DSS v1.2 et mise en œuvre des changements mineurs notés depuis la v1.1 d'origine.
28 octobre 2010	2.0	Harmonisation du contenu avec les nouvelles exigences PCI DSS v2.0 et les procédures de test.

Table des matières

Normes de sécurité des données du PCI : documents connexes

Les documents suivants ont été développés de manière à aider les commerçants et les prestataires de services à comprendre les normes de sécurité des données du secteur des cartes de paiement (PCI DSS) et le QAÉ relatif à ces normes.

Document	Public
Normes de sécurité des données du PCI : Conditions et procédures d'évaluation de sécurité	Tous les commerçants et les prestataires de services
Parcourir les PCI DSS : Comprendre l'objectif des exigences	Tous les commerçants et les prestataires de services
Normes de sécurité des données du PCI : Instructions et directives concernant l'auto-évaluation	Tous les commerçants et les prestataires de services
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation A et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation B et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation C-VT et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation C et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation D et attestation	Commerçants admissibles et prestataires de services[1]
Normes de sécurité des données du PCI et Normes de sécurité des données de l'application de paiement : Glossaire, abréviations et acronymes	Tous les commerçants et les prestataires de services

[1] Pour définir le questionnaire d'auto-évaluation approprié, consulter le document *Normes de sécurité des données du PCI : Instructions et directives concernant l'auto-évaluation*, « Sélection du questionnaire d'auto-évaluation et de l'attestation les plus appropriés pour l'organisation ».

Avant de commencer

Remplir le questionnaire d'auto-évaluation

Le QAÉ A a été développé 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 sur leurs systèmes ou dans leurs locaux.

Les commerçants QAÉ A, définis ici et selo*n les instructions et directives concernant 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 sur leurs systèmes ou dans leurs locaux. Ils doivent obtenir une validation de conformité en remplissant le QAÉ A et l'attestation de conformité associée, en confirmant les éléments suivants **:**

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

Chaque section du questionnaire est consacrée à un thème de sécurité spécifique, selon les exigences des *Conditions et procédures d'évaluation de sécurité des normes PCI DSS*. Cette version abrégée du QAÉ comprend des questions qui s'appliquent à un type spécifique d'environnement de petit commerçant, tel qu'il est défini dans les critères d'admissibilité ci-dessus. S'il existe des exigences PCI DSS applicables à un environnement qui ne sont pas couvertes dans ce QAÉ, cela peut indiquer que ce QAÉ n'est pas adapté à cet environnement. En outre, il faut se conformer à toutes les exigences PCI DSS applicables pour être conforme aux normes PCI DSS.

Étapes de mise en conformité avec les normes PCI DSS

1. Évaluer la conformité d'un environnement aux normes PCI DSS.
2. Remplir le questionnaire d'auto-évaluation (QAÉ A) selon les instructions du document *Instructions et directives concernant le questionnaire d'auto-évaluation.*
3. Remplir l'attestation de conformité dans son intégralité.
4. Envoyer le questionnaire et l'attestation de conformité, avec tout autre justificatif requis, à l'acquéreur.

Directives sur la non-applicabilité de certaines exigences spécifiques

Non applicabilité : les exigences jugées non applicables à un environnement doivent être définies comme telles par la mention « s.o. » dans la colonne « Spécial » du QAÉ. En conséquence, remplir la fiche « Explication de non applicabilité » dans l'annexe pour chaque entrée « s.o. ».

Attestation de conformité, QAÉ A

Instructions de transmission

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

Partie 1. Renseignements sur le commerçant et l'évaluateur de sécurité qualifié

Partie 1a. Renseignements sur la société du commerçant

Nom de la société :		DBA(s) :			
Nom du contact :		Poste occupé :			
Téléphone :		Courriel :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

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

Nom de la société :					
Nom du principal contact QSA :		Poste occupé :			
Téléphone :		Courriel :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

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

☐ Détaillant ☐ Télécommunications ☐ Épiceries et supermarchés

☐ Pétrole ☐ Commerce électronique ☐ Vente par correspondance/téléphone ☐ Autres (veuillez préciser) :

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

Partie 2a. Relations

La société entretient-elle une relation avec un ou plusieurs prestataires de services tiers (par exemple, passerelles, société d'hébergement sur le Web, tour opérateurs, agents de ☐ Oui ☐ Non

programmes de fidélité, etc.)?	
La société entretient-elle une relation avec plusieurs acquéreurs?	☐ Oui ☐ Non

Partie 2b. Conditions à remplir pour compléter le QAÉ A

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

☐	le commerçant ne stocke, ne traite ou ne transmet aucune donnée de titulaire de carte sur ses systèmes ou dans ses locaux mais la gestion de toutes ces fonctions est confiée à un ou plusieurs prestataires de services tiers;
☐	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 aux normes PCI DSS est confirmée;
☐	le commerçant ne stocke aucune donnée de titulaire de carte au format électronique; **et**
☐	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 des PCI DSS

Suite aux résultats du QAÉ A du *(date à laquelle il a été rempli)*, *(Nom de la société du commerçant)* déclare le statut de conformité suivant (cocher une case) :

☐ **Conforme :** toutes les sections du QAÉ PCI sont remplies et toutes les questions ont reçu la réponse « Oui », d'où une évaluation globale **CONFORME**, *(Nom de la société du commerçant)* est donc conforme aux normes PCI DSS.

☐ **Non conforme :** les sections du QAÉ PCI n'ont pas toutes été remplies ou certaines questions ont reçu la réponse « Non », d'où une évaluation globale **NON CONFORME**, *(Nom de la société du commerçant)* n'est donc pas conforme aux normes PCI DSS.

- **Date cible** de mise en conformité :
- Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à remplir le plan d'action décrit dans la Partie 4 de ce document. *Vérifier ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir 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 :

☐	Le questionnaire d'auto-évaluation A des PCI DSS, version *(n° de version du QAÉ)*, a été rempli selon les instructions fournies dans ce document.
☐	Tous les renseignements présents dans le questionnaire d'auto-évaluation mentionné ci-dessus ainsi que dans cette attestation illustrent honnêtement les résultats de l'évaluation.
☐	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 ↑	*Titre ↑*

Nom de la société représentée ↑

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

Sélectionner l'état de conformité approprié pour chaque exigence. Si la réponse « NON » est donnée à la moindre exigence, 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 ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

Exigence 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	Limiter l'accès physique aux données de titulaire de carte	☐	☐	
12	Gérer une politique qui adresse les renseignements de sécurité à tout le personnel	☐	☐	

Questionnaire d'auto-évaluation A

Remarque : *les questions suivantes sont numérotées conformément aux exigences et procédures de test des normes PCI DSS, comme défini dans le document* Conditions et procédures d'évaluation de sécurité des normes PCI DSS*.*

Date de réalisation :

Mise en œuvre de mesures de contrôle d'accès strictes

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

	Question	Réponse PCI DSS :	Oui	Non	Spécial*
9.6	Tous les supports sont-ils physiquement sécurisés (comprenant, mais sans s'y limiter, les ordinateurs, les supports électroniques amovibles, les reçus papier, les rapports papier et les télécopies)? *Dans le cadre de l'exigence 9, le terme « support » concerne tous les documents papier et les supports électroniques contenant des données de titulaire de carte.*		☐	☐	
9.7	(a) La distribution interne ou externe de tout type de support est-elle soumise à un contrôle strict?		☐	☐	
	(b) Les contrôles comprennent-ils les procédures suivantes :				
9.7.1	Les supports sont-ils classifiés afin que la confidentialité des données puisse être déterminée?		☐	☐	
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition sécurisée qui peut faire l'objet d'un suivi?		☐	☐	
9.8	Les journaux sont-ils gérés pour suivre tous les supports qui sont déplacés d'une zone sécurisée, et l'approbation de gestion est-elle obtenue avant le déplacement des supports (en particulier lorsque le support est distribué aux individus)?		☐	☐	
9.9	Un contrôle strict est-il assuré concernant le stockage et l'accessibilité des supports?		☐	☐	
9.10	Tous les supports sont-ils éliminés lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou juridiques?		☐	☐	
	La destruction est-elle effectuée comme suit :				
9.10.1	(a) Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de manière à ce qu'il soit impossible de les reconstituer?		☐	☐	
	(b) Les conteneurs utilisés pour le stockage des renseignements à détruire sont-ils sécurisés pour empêcher l'accès aux contenus? (Par exemple, un conteneur de « documents à déchiqueter » possède une serrure empêchant l'accès à son contenu)		☐	☐	

Gérer une politique de sécurité des renseignements

Exigence 12 : Gérer une politique qui adresse les renseignements de sécurité à tout le personnel

	Question	Réponse PCI DSS :	Oui	Non	Spécial*
12.8	Si les données de titulaire de carte sont partagées avec des prestataires de services, des politiques et procédures sont-elles gérées et mises en œuvre pour la gestion de ces derniers, comme suit?				
12.8.1		Une liste des prestataires de services est-elle tenue?	☐	☐	
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-t-il été signé?	☐	☐	
12.8.3		Un processus de sélection des prestataires de services est-il bien défini, comprenant notamment des contrôles préalables à l'engagement?	☐	☐	
12.8.4		Un programme est-il mis en place pour contrôler la conformité des prestataires de services aux normes PCI DSS?	☐	☐	

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 de renseignements sur chaque exigence PCI DSS, voir *Parcourir les normes PCI DSS*).
3. Aller au-delà des autres exigences PCI DSS (Les contrôles compensatoires ne consistent pas simplement à se trouver en conformité à 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 sociétés 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 utiliser d'autres exigences PCI DSS relatives aux mots de passe (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 faisant l'objet d'une vérification. Par exemple, l'authentification à deux facteurs est exigée par les normes PCI DSS pour l'accès à distance. L'authentification à deux facteurs *depuis le 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 si : (1) elle satisfait à 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 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 lors de 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 sociétés 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 :

	Renseignements requis	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. Maintenance	Définir les processus et les contrôles en place pour la maintenance 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?*

	Renseignements requis	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	*La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « racine ». La société XYZ ne peut pas gérer le nom d'utilisateur « racine » ni consigner toutes les activités de chaque utilisateur « racine ».*
2. Objectif	Définir l'objectif du contrôle initial; identifier l'objectif satisfait par le contrôle compensatoire.	*L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des renseignements 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.*
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	*L'absence d'ID d'utilisateur unique et le fait de ne pas pouvoir consigner les renseignements d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.*
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.	*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 « racine » 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.*
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	*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 « racine ».*
6. Maintenance	Définir les processus et les contrôles en place pour la maintenance des contrôles compensatoires.	*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 racine sans que leurs activités soient consignées ou suivies.*

Annexe D : Explication de non-applicabilité

Si la mention « s.o. » ou « sans objet » a été saisie dans la colonne « Spécial », il est nécessaire d'utiliser cette fiche pour expliquer les raisons de la non-applicabilité des exigences à l'organisation.

Exigence	Raisons de non-applicabilité
Exemple : *12.8*	*Les données de titulaire de carte ne font l'objet d'aucun partage avec les prestataires de services.*