Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation A et attestation de conformité

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

Version 2.0

Octobre 2010

Modifications apportées au document

Date	Version	Description
1er Octobre 2008	1.2	Harmonisation du contenu avec la nouvelle procédure PCI DSS v1.2 et implémentation des changements mineurs notés depuis la v1.1 d'origine.
28 Octobre 2010	2.0	Harmonisation du contenu avec les conditions de la nouvelle norme PCI DSS et des procédures de test.

Copyright 2010 PCI Security Standards Council LLC

Table des matières

Copyright 2010 PCI Security Standards Council LLC

Norme de sécurité des données du PCI : documents connexes

Les documents suivants ont été élaborés pour aider les commerçants et les prestataires de services à comprendre la norme de sécurité des données du secteur des cartes de paiement (PCI DSS) et le SAQ PCI DSS.

Document	Public visé
Norme de sécurité des données du PCI : Conditions et procédures d'évaluation de sécurité	Tous les commerçants et les prestataires de services
Navigation dans la norme PCI DSS : Comprendre l'objectif des conditions	Tous les commerçants et les prestataires de services
Norme de sécurité des données du PCI : Instructions et directives relatives à l'auto-évaluation	Tous les commerçants et les prestataires de services
Norme de sécurité des données du PCI : Questionnaire d'auto-évaluation A et attestation	Commerçants qualifiés [1]
Norme de sécurité des données du PCI : Questionnaire d'auto-évaluation B et attestation	Commerçants qualifiés [1]
Norme de sécurité des données du PCI : Questionnaire d'auto-évaluation C-VT et attestation	Commerçants qualifiés [1]
Norme de sécurité des données du PCI : Questionnaire d'auto-évaluation C et attestation	Commerçants qualifiés [1]
Norme de sécurité des données du PCI : Questionnaire d'auto-évaluation D et attestation	Commerçants qualifiés et prestataires de services [1]
Norme de sécurité des données du PCI et norme de sécurité des données d'application de paiement : Glossaire des termes, 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 relatives à l'auto-évaluation*, « Sélectionner le SAQ et l'attestation les plus appropriés à l'organisation ».

Copyright 2010 PCI Security Standards Council LLC

Avant de commencer

Compléter le questionnaire d'auto-évaluation

Le SAQ A a été conçu pour répondre aux conditions applicables aux commerçants qui conservent uniquement des reçus ou des rapports papier avec des données de titulaire de carte, qui ne stockent pas de données de titulaire de carte au format électronique et qui ne traitent pas ni ne transmettent des données de titulaire de carte sur leurs systèmes ou dans leur locaux.

Les commerçants SAQ A, définis ici et dans le document *Instructions et directives relatives au questionnaire d'auto-évaluation PCI DSS*, ne stockent pas de données de titulaires de carte au format électronique et ne traitent ni ne transmettent des données de titulaires de carte sur leurs systèmes ou dans leurs locaux. Ces commerçants valident leur conformité en complétant un SAQ A et l'attestation de conformité associée, confirmant que :

- la société traite uniquement les transactions de carte absente (commerce électronique ou commande par courrier/téléphone) ;
- la société ne stocke, ne traite ni ne transmet des données de titulaires de carte sur ses systèmes ou dans ses locaux, mais confie la gestion de toutes ces fonctions à un ou plusieurs prestataires de services tiers ;
- la société a confirmé que la ou les tiers qui gèrent le stockage, le traitement et/ou la transmission des données de titulaire de carte sont conforme à la norme PCI DSS ;
- la société conserve uniquement des reçus ou rapports papiers avec des données de titulaire de carte, et ces documents ne sont pas reçu de manière électronique ; et
- ƒla société ne stocke aucune donnée de titulaires de cartes sous forme électronique.

Cette option ne peut s’appliquer aux commerçants avec un environnement de point de vente traditionnel.

Chaque rubrique du questionnaire se concentre sur un domaine particulier de sécurité, en fonction des conditions du document Conditions et procédure d'évaluation de sécurité de la norme PCI DSS. Cette version abrégée du SAQ comprend des questions s'appliquant à un type particulier d'environnement de petit commerçant, tel qu'il est défini dans les critères de qualification ci-dessus. S'il existe des conditions PCI DSS applicables à l'environnement qui ne sont pas couvertes par ce SAQ, cela peut être une indication du fait que ce SAQ n'est pas adapté à cet environnement. En outre, il faut se conformer à toutes les conditions PCI DSS applicables afin d'être conforme à la norme PCI DSS.

Étapes de mise en conformité avec la norme PCI DSS

1. Évaluer la conformité d'un environnement à la norme PCI DSS.

2. Compléter le questionnaire d'auto-évaluation (SAQ A) conformément aux instructions du document *Instructions et directives relatives au questionnaire d'auto-évaluation*.

3. Compléter l'attestation de conformité dans son intégralité.

4. Envoyer le questionnaire et l'attestation de conformité ainsi que toute autre documentation requise par l'acquéreur.

Directives de non-applicabilité de certaines conditions particulières

Non-applicabilité : les conditions jugées non applicables à un environnement doivent être indiquées par la mention « s.o. » dans la colonne « Spécial » du SAQ. En conséquence, compléter la fiche « Explication de non applicabilité » dans l'annexe D pour chaque entrée « s.o. ».

Copyright 2010 PCI Security Standards Council LLC

Attestation de conformité, SAQ A

Instructions de transmission

Le commerçant doit compléter cette attestation de conformité, qui atteste du respect par le commerçant des Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données du secteur des cartes de paiement (PCI DSS). Compléter toutes les rubriques pertinentes et se reporter aux instructions de transmission présentées sous le titre « Étapes de mise en conformité avec la norme PCI DSS » dans ce document.

Partie 1. Informations sur l'évaluateur de sécurité qualifié et le commerçant Partie 1a. Informations sur le commerçant			
Nom de la société :	Mon commerce	DBA:	John Smith
Nom du contact :	Pierre Dupont	Poste occupé :	John Smith
Téléphone :	0684359434	E-mail:	john.smith@yopmail.com
Adresse professionnelle :	25 rue des libert	Ville :	Paris
État/province :	Ile de France	Pays :	France
Numéro commerçant:	987654321	Code postal :	75001
URL:	www.scotiabank.com		

Partie 1b. Informations sur la société QSA (le cas échéant)					
Nom de la société :	QSA Company				
Nom du principal contact QSA :	Jacques Dupon		Poste occupé :	Auditeur QSA	
Téléphone :	0145059585		E-mail:	jacques-dupon@qsa-company.com	
Adresse professionnelle :	45 rue des pommes		Ville :	Paris	
État/province :	Paris	Pays :	France	Code postal :	75002
URL:	www.scotiabank.com				

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

☐ Détaillant	☐ Télécommunications	☑ Épiceries et supermarchés
☐ Pétrole	☐ Commerce électronique	☑ Commande par courrier/téléphone
☐ Autres (préciser) :		
Indiquer les installations et les sites compris dans l'examen PCI DSS :	**L'ensemble des ablissements compris Commerce principal + deux satelites**	

Partie 2a. Relations

La société entretient-elle une relation avec un ou plusieurs agents tiers (par exemple, passerelles, société d'hébergement sur le Web, tour opérateurs, agents de programmes Oui Non ☑ Yes ☐ No

La société entretient-elle une relation avec plusieurs acquéreurs ? ☐ Yes ☑ No

Copyright 2010 PCI Security Standards Council LLC

Partie 2b. Admissibilité à participer au questionnaire SAQ A

Le commerçant certifie son admissibilité à compléter cette version abrégée du Questionnaire d'auto-évaluation pour les motifs suivants :

☑ Le commerçant certifie son admissibilité à compléter cette version abrégée du Questionnaire d'auto-évaluation pour les motifs suivants :

☑ Le ou les prestataires de services tiers qui assurent le stockage, le traitement et/ou la transmission de données de titulaires de carte sont reconnus comme respectant les normes PCI DSS ;

☑ Le commerçant ne stocke aucune donnée de titulaires de carte sous forme électronique et

☑ Si le commerçant stocke des données sur les titulaires de carte, ces données ne sont que des rapports imprimés ou des copies de bordereaux et ne sont pas reçues par voie électronique.

Partie 3. Validation de la norme PCI DSS

En se basant sur les résultats mentionnés dans le questionnaire SAQ A du (*date d'achèvement*), (*Nom de la société du commerçant*) certifie l'état de conformité suivant (cocher une seule réponse) :

☐ Conforme : toutes les rubriques du questionnaire SAQ PCI sont renseignées et toutes les questions ont pour réponse « oui », ce qui justifie sa classification globale comme **CONFORME**, (*Nom de la société du commerçant*) ayant apporté la preuve de sa pleine conformité à la norme PCI DSS.

☑ Non conforme : les rubriques du questionnaire SAQ PCI ne sont pas toutes renseignées ou certaines questions ont pour réponse « non », ce qui justifie sa classification globale comme **NON CONFORME**, (Nom de la société du commerçant) n'ayant pas apporté la preuve de sa pleine conformité à la norme 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 ce qui suit :

☑ Le questionnaire d'auto-évaluation A PCI DSS, version (n° de version du SAQ), a été complété conformément aux instructions fournies.

☑ Toutes les informations présentes dans le SAQ susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de mon évaluation.

☑ J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme PCI DSS à tout moment.

Partie 3b. Reconnaissance par le commerçant

Signature du représentant du commerçant Date

Nom du représentant du commerçant Poste occupé

Société du commerçant représentée

Copyright 2010 PCI Security Standards Council LLC

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*

Condition PCI DSS	Description de la condition	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 des titulaires de cartes		**X**	23/03/2013=>Il n'y as actuellement aucun controle spifique. 01/05/2013=>Les documents seront druit sous peu 31/03/2013=>Mise niveau de la suritvenir.
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel		**X**	01/08/2013=>Selection mettre en place.

Copyright 2010 PCI Security Standards Council LLC

Questionnaire d’auto-évaluation A

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

Date de réalisation : **2013-03-08 10:52:06**

Mise en œuvre de mesures de contrôle d’accès strictes

Condition 9 : Restreindre l’accès physique aux données des titulaires de cartes

	Question PCI DSS Réponse :	Oui	Non	Spécial
9.6	Tous les supports sont-ils physiquement sécurisés (entre autres, ordinateurs, supports électroniques amovibles, réseaux, reçus et rapports sur papier, et fax) ? *Dans le cadre de la condition 9, « support » se rapporte à tout support papier ou électronique contenant des données de titulaires de cartes.*	X		
9.7	(a) Un contrôle strict s'applique-t-il à la distribution interne ou externe d'un type de support ?		X	23/03/2013 => Il n'y as actuellement aucun controle spifique.
	(b) Les contrôles comprennent-ils les éléments suivants :			
9.7.1	Les supports sont-ils classés afin de déterminer la sensibilité des données qu'ils contiennent ?	X		
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d’expédition qui peut faire l’objet d’un suivi ?	X		
9.8	Les registres sont-ils gérés pour suivre tous les supports déplacés d'une zone sécurisée et une approbation de gestion est-elle obtenue avant le déplacement du support (notamment lorsque le support est distribué aux individus) ?	X		
9.9	Un contrôle strict est-il réalisé sur le stockage et l’accessibilité des supports ?	X		
9.10	Tous les supports sont-ils détruits lorsqu'ils ne sont plus utiles pour des raisons professionnelles ou légales ?	X		
	La destruction est-elle réalisée comme suit :			
9.10.1	(a)Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de sorte que les données de titulaires de carte ne puissent pas être reconstituées ?		X	01/05/2013 => Les documents seront druit sous peu
	(b)Les contenants qui stockent des informations à détruire sont-ils sécurisés pour prévenir l'accès à leur contenu ? (Par exemple, un contenant de « documents à déchiqueter » dispose d'une serrure pour prévenir l'accès à son contenu).		X	31/03/2013 => Mise niveau de la suritvenir.

Copyright 2010 PCI Security Standards Council LLC

Gestion d’une politique de sécurité des informations

Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel

	Question PCI DSS Réponse :	Oui	Non	Spécial
12.8	Si les données de titulaires de cartes sont partagées avec des prestataires de services, des politiques et procédures sont-elles en place et maintenues pour gérer les prestataires de services comme suit ?			s.o
12.8.1	Une liste des prestataires de services est-elle tenue ?	X		
12.8.2	Fait-on signer un accord écrit aux prestataires de services, par lequel ils se reconnaissent responsables de la sécurité des données de titulaires de cartes en leur possession ?		X	01/08/2013 => Selection mettre en place.
12.8.3	Existe-t-il un processus de sélection des prestataires de services, comprenant notamment des contrôles préalables à l'engagement ?	X		
12.8.4	Existe-t-il un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS ?			s.o

Copyright 2010 PCI Security Standards Council LLC

Annexe A : (non utilisée)

Page laissée volontairement vide

Copyright 2010 PCI Security Standards Council LLC

Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux conditions PCI DSS telles qu\'elles sont stipulées, en raison de contraintes commerciales renseignées 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 la condition initiale de la norme PCI DSS.

2. Fournir une protection similaire à celle de la condition initiale de la norme PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par la condition initiale. (Pour plus d'informations sur chaque condition PCI DSS, voir Navigation dans la norme PCI DSS).

3. Aller au-delà des autres conditions PCI DSS (Les contrôles compensatoires ne consistent pas simplement en la conformité à d'autres conditions PCI DSS).

Lors de l'évaluation de la portée des contrôles compensatoires, 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 de la norme 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 déployé, 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 conditions existantes de la norme 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 restreindre les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut pas utiliser d\autres conditions de mot de passe de la norme 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 la norme PCI DSS pour l'élément examiné (à savoir les mots de passe).

b) Les conditions existantes de la norme 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 la norme 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 la condition initiale en résolvant les risques d'interception des mots de passe administrateur en texte clair, et (2) elle est correctement configurée et elle est déployée dans un environnement sécurisé.

c) Les conditions existantes de la norme 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 titulaires de cartes illisibles conformément à la condition 3.4 (par exemple, par cryptage), un contrôle compensatoire pourrait consister en un périphérique ou un ensemble de périphériques, 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. Correspondre aux risques supplémentaires qu'implique la non conformité à la condition de la norme PCI DSS.

L'évaluateur doit évaluer soigneusement les contrôles compensatoires pendant chaque évaluation annuelle de la norme PCI DSS afin de confirmer que chaque contrôle compensatoire couvre de manière appropriée le risque ciblé par la condition initiale de la norme 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.

Copyright 2010 PCI Security Standards Council LLC

Annexe C : Fiche de contrôles compensatoires

Se référer à cette fiche pour définir des contrôles compensatoires pour toute condition 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 conditions :

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité à la condition 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.	

Copyright 2010 PCI Security Standards Council LLC

Annexe D : Explication de non applicabilité

Si les mentions « s.o.» ou « sans objet » ont été saisies dans la colonne « Spécial », utiliser cette fiche de travail pour expliquer pourquoi la condition relative n'est pas applicable à l'organisation.

Condition	Raison pour laquelle la condition n'est pas applicable
12.8.1	Nous ne possons aucune liste de prtataire

Copyright 2010 PCI Security Standards Council LLC