Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation B
et attestation de conformité

Commerçant ayant uniquement des machines d'impression ou uniquement des terminaux autonomes par ligne directe — Sans stockage électronique de données de titulaires de carte

Version 3.0

Février 2014

Modifications apportées au document

Date	Version	Description
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.
Octobre 2010	2.0	Harmonisation du contenu avec les conditions de la nouvelle norme PCI DSS v2.0 et des procédures de test.
Février 2014	3.0	Aligner le contenu avec les exigences et les procédures de test de PCI DSS v3.0, et incorporer des options de réponse supplémentaires.

Table des matières

Avant de commencer

Le SAQ B a été élaboré pour répondre aux conditions applicables aux commerçants qui traitent les données de titulaires de carte uniquement par des périphériques d'impression ou des terminaux autonomes à liaison directe. Les commerçants SAQ B peuvent être des commerçants directs (carte présente) ou des commerçants par courrier/téléphone (carte non présente) et ils ne stockent pas ces données sur un système informatique.

Commerçants SAQ B confirmer que, pour ce réseau de paiement :

- La société n'utilise qu'un périphérique d'impression et/ou des terminaux autonomes à liaison directe (connectés au processeur par une ligne téléphonique) pour prendre les informations de carte de paiement du client ;
- Les terminaux autonomes à liaison directe ne sont pas connectés à des systèmes au sein de l'environnement ;
- Les terminaux autonomes à liaison directe ne sont pas connectés à Internet ;
- La société ne transmet pas de données de titulaires de carte sur un réseau (ni sur un réseau interne, ni sur Internet) ;
- La société conserve uniquement des reçus ou des rapports papier avec les données de titulaire de carte, sans recevoir ces documents au format électronique ; **et**
- votre société ne stocke pas de données de titulaires de carte sous forme électronique.

Ce SAQ n'est pas applicable à tous les réseaux de commerce électronique.

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 votre environnement qui ne sont pas couvertes par ce SAQ, cela peut être une indication du fait que ce SAQ n'est pas adapté à votre environnement. En outre, vous devez vous conformer à toutes les conditions PCI DSS applicables afin d'être conforme à la norme PCI DSS.

Étapes d'achèvement de l'auto-évaluation PCI DSS

1. Identifier le SAQ applicable pour votre environnement – Consultez les *Instructions et directives relatives aux questionnaires d'auto-évaluation* sur le site Internet de PCI SSC pour de plus amples informations.
2. Confirmez que les paramètres de votre environnement sont corrects et correspondent aux critères d'éligibilité pour le SAQ que vous utilisez (ainsi que le définit la partie 2g de l'attestation de conformité).
3. Évaluer la conformité de votre environnement aux conditions applicables de la norme PCI DSS.
4. Complétez toutes les sections de ce document :
   - Section 1 (Parties 1 & 2 de l'AOC) – Informations relatives à l'évaluation et résumé.
   - Section 2 – Questionnaire d'auto-évaluation PCI DSS (SAQ B)
   - Section 3 (Parties 3 & 4 de l'AOC) – Détails de validation et d'attestation, plan d'action pour les conditions de non-conformité (s'il y a lieu)
5. Envoyer le SAQ et l'attestation de conformité, ainsi que toute autre documentation requise, telle que des rapports d'analyse ASV, à votre acquéreur, à la marque de paiement ou autre demandeur.

Comprendre le questionnaire d'auto-évaluation

Les questions contenues dans la colonne de « Question PCI DSS » de ce questionnaire d'auto-évaluation se basent sur les exigences de PCI DSS.

Les ressources supplémentaires qui apportent des conseils sur les exigences PCI DSS et comment remplir le questionnaire d'auto-évaluation ont été incluses pour aider au processus d'évaluation. Un aperçu de certaines de ces ressources est inclus ci-dessous :

Document	Inclut :
PCI DSS *(Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données PCI)*	• Lignes directrices relatives à la portée • Ligne directrice relative à l'intention de toutes les exigences de la norme PCI DSS • Détails des procédures de test • Détails sur les contrôles compensatoires
Instructions pour le SAQ et documents de lignes directrices	• Informations concernant tous les SAQ et leurs critères d'éligibilité • Comment déterminer le SAQ qui s'applique à votre organisation
Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS	• Descriptions et définitions des termes utilisés dans le PCI DSS et les questionnaires d'auto-évaluation

Ces ressources, comme de nombreuses autres, se trouvent le site Web du PCI SSC *(www.pcisecuritystandards.org)*. Les organisations sont encouragées à examiner le PCI DSS ainsi que les autres documents justificatifs avant de commencer une évaluation.

Tests attendus

Les instructions de la colonne « Tests attendus » se basent sur les procédures de test du PCI DSS et elles offrent une description détaillée des types d'activités de test qui doivent être effectués afin de vérifier qu'une condition a bien été respectée. Les détails complets des procédures de test de chaque condition se trouvent dans le PCI DSS.

Remplir le questionnaire d'auto-évaluation

Pour chaque question, il existe un choix de réponses pour indiquer le statut de votre société vis-à-vis de cette condition. ***Une seule réponse peut être sélectionnée pour chaque question.***

Une description de la signification de chaque réponse se trouve dans le tableau ci-dessous :

Réponse	Quand utiliser cette réponse :
Oui	Le test attendu a été effectué et tous les éléments de la condition ont été remplis ainsi qu'il est précisé.
Oui, avec CCW (Fiche de contrôle compensatoire)	Le test attendu a été effectué et tous les éléments de la condition ont été remplis avec l'aide d'un contrôle compensatoire. Pour toutes les réponses de cette colonne, remplir la fiche de contrôle compensatoire (CCW) dans l'annexe B du SAQ. Les informations concernant l'utilisation des contrôles compensatoires et les conseils pour aider à remplir la fiche se trouvent dans le PCI DSS.
Non	Certains, ou la totalité, des éléments de la condition n'ont pas été remplis, sont en cours de mise en œuvre, ou nécessitent d'autres tests avant de savoir s'ils sont en place.

Réponse	Quand utiliser cette réponse :
S.O. (Sans objet)	La condition ne s'applique pas à l'environnement de l'organisation. (Voir ci-dessous les exemples de *directives de non-applicabilité de certaines conditions particulières spécifiques*). Toutes les réponses de cette colonne nécessitent une explication justificative dans l'Annexe C du SAQ.

Directives de non-applicabilité de certaines conditions particulières

Si certaines conditions sont considérées comme n'étant pas applicables à votre environnement, sélectionnez l'option « S.O. » pour cette condition spécifique et remplir la fiche « Explication de la non-applicabilité » dans l'annexe C pour chaque indication « S.O. ».

Exceptions légales

Si votre organisation est sujette à une restriction légale qui l'empêche de respecter une condition PCI DSS, cocher la colonne « Non » pour cette condition et remplir l'attestation pertinente dans la partie 3.

Section 1 : Informations relatives à l'évaluation

Instructions de transmission

Ce document doit être complété en tant que déclaration des résultats de l'auto-évaluation du commerçant vis-à-vis des *Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données du secteur des cartes de paiement (PCI DSS).* Complétez toutes les sections : Le commerçant est responsable de s'assurer que chaque section est remplie par les parties pertinentes, le cas échéant. Contacter l'acquéreur (la banque du commerçant) ou la marque de paiement pour déterminer les procédures de rapport et de demande.

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

Partie 1a. Informations sur le commerçant

Nom de la société :			DBA (nom commercial) :		
Nom du contact :			Poste occupé :		
Nom(s) ISA (le cas échéant) :			Poste occupé :		
Téléphone :			E-mail :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					

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

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

Partie 2. Résumé

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

☐ Détaillant	☐ Télécommunications	☐ Épiceries et supermarchés
☐ Pétrole	☐ Commerce électronique	☐ Commande par courrier/téléphone (MOTO)
☐ Autres (préciser) :		

Quels types de réseaux de paiement votre entreprise sert-elle ? ☐ Commande postale/commande par téléphone (MOTO)	Quels réseaux de paiement sont couverts par ce SAQ ? ☐ Commande postale/commande par téléphone (MOTO)

☐ Commerce électronique ☐ Carte présente (face à face)	☐ Commerce électronique ☐ Carte présente (face à face)

Remarque : *Si votre organisation utilise un réseau ou un processus de paiement qui n'est pas couvert par ce SAQ, consultez votre acquéreur ou votre marque de paiement à propos de la validation des autres réseaux.*

Partie 2b. Description de l'entreprise de carte de paiement

Comment et dans quelle mesure votre entreprise stocke-t-elle, traite-t-elle et/ou transmet-elle des données de titulaires de carte ?	

Partie 2c. Emplacements

Énumérer les types de locaux et un résumé des emplacements inclus dans l'examen PCI DSS (par exemple : commerces de détail, siège social, centre de données, centre d'appel, etc.)

Type de local	Emplacement(s) du local (ville, pays)

Partie 2d. Application de paiement

Est-ce que l'organisation utilise une ou plusieurs applications de paiement ? ☐ Oui ☐ Non

Fournir les informations suivantes concernant les applications de paiement utilisées par votre organisation :

Nom de l'application de paiement	Numéro de version	Vendeur de l'application	L'application est-elle listée PA-DSS ?	Date d'expiration du listing PA-DSS (le cas échéant)
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	

Partie 2e. Description de l'environnement

Donner une description ***détaillée*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions entrantes et sortantes à l'environnement de données de titulaire de carte (CDE).* • *Composants critiques du système dans le CDE, tels que les appareils de POS, les bases de données, les serveurs Internet, etc., ainsi que les autres composants de paiement nécessaires, le cas échéant.*	
Est-ce que votre entreprise utilise la segmentation de réseau pour affecter la portée de votre	☐ Oui

environnement PCI DSS ? *(Consulter la section « Segmentation de réseau » de PCI DSS pour les recommandations concernant la segmentation de réseau)*	☐ Non

Partie 2f. Prestataires de services tiers

Est-ce que votre société partage des données de titulaire de carte avec des prestataires de service tiers (par exemple, passerelles, services de traitement de paiement, services de prestataires de paiement (PSP), prestataires de services d'hébergement sur le Web, organisateurs de voyages, agents de programmes de fidélisation, etc.) ?	☐ Oui ☐ Non

Si oui :

Nom du prestataire de services :	**Description du service fourni :**

Remarque : *La condition 12.8 s'applique à toutes les entités de cette liste.*

Partie 2g. Admissibilité à utiliser le questionnaire SAQ B

Le commerçant certifie son admissibilité à compléter cette version abrégée du Questionnaire d'auto-évaluation dans la mesure où, pour ce réseau de paiement :

☐	Le commerçant utilise uniquement un périphérique d'impression pour imprimer les informations de carte de paiement des clients et il ne transmet pas de données de titulaires de carte par téléphone ou par Internet ; et/ou Le commerçant utilise que des terminaux autonomes à liaison directe (connectée au prestataire de service de traitement par ligne téléphonique) et les terminaux autonomes ne sont pas reliés à Internet ni à aucun autre système dans l'environnement du commerçant ;
☐	Le commerçant ne transmet pas de données de titulaires de carte sur un réseau (ni sur un réseau interne, ni sur Internet) ;
☐	Le commerçant ne stocke pas de données sur les 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.

Section 2 : Questionnaire d'auto-évaluation B

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 d'achèvement de l'auto-évaluation :

Protection des données du titulaire

Condition 3 : Protéger les données du titulaire stockées

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
3.2	(c) Les données d'identification sensibles sont-elles supprimées ou rendues irrécupérables une fois le processus d'autorisation terminé ?	▪ Examiner les politiques et les procédures ▪ Examiner les configurations de système ▪ Examiner les processus de suppression	☐	☐	☐	☐
	(d) Tous les systèmes adhèrent-ils aux conditions suivantes concernant le non-stockage de données d'authentification sensibles après autorisation (même si elles sont cryptées) :					

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
3.2.1	La totalité du contenu d'une quelconque piste (sur la bande magnétique au verso d'une carte, données équivalentes sur une puce ou ailleurs) n'est-elle pas stockée après autorisation ? *Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique.* ***Remarque :*** *Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique suivants :* • *Le nom du titulaire de la carte,* • *Le numéro de compte primaire (PAN),* • *La date d'expiration et* • *Le code de service* *Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.*	▪ Examiner les sources de données, y compris : • Les données de transaction entrantes ; • Tous les journaux • Les fichiers d'historique • Les fichiers trace • Le schéma de base de données • Le contenu des bases de données	☐	☐	☐	☐
3.2.2	Le code ou la valeur de vérification de carte (numéro à trois ou quatre chiffres imprimé sur le recto ou le verso d'une carte de paiement) n'est pas stocké après autorisation ?	▪ Examiner les sources de données, y compris : • Les données de transaction entrantes ; • Tous les journaux • Les fichiers d'historique • Les fichiers trace • Le schéma de base de données • Le contenu des bases de données	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
3.2.3	Le code d'identification personnelle (PIN) ou le bloc PIN crypté ne sont pas stockés après autorisation ?	▪ Examiner les sources de données, y compris : • Les données de transaction entrantes ; • Tous les journaux • Les fichiers d'historique • Les fichiers trace • Le schéma de base de données • Le contenu des bases de données	☐	☐	☐	☐
3.3	Le PAN est-il masqué lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel dont le besoin commercial est légitime puisse voir le PAN dans sa totalité ? ***Remarque :*** *Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données du titulaire, par exemple, pour les reçus des points de vente (POS).*	▪ Examiner les politiques et les procédures ▪ Examiner les rôles qui ont besoin d'accéder aux affichages de PAN entier ▪ Examiner les configurations de système ▪ Observer les affichages de PAN	☐	☐	☐	☐

Condition 4 : Crypter la transmission des données du titulaire sur les réseaux publics ouverts

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
4.2	(b) Des politiques sont-elles déployées pour interdire la transmission de PAN non protégé à l'aide de technologies de messagerie pour utilisateurs finaux ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
7.1	L'accès aux composants du système et aux données des titulaires de carte est-il restreint aux seuls individus qui doivent y accéder pour mener à bien leur travail, comme suit :					
7.1.2	L'accès aux ID privilégiés est restreint comme suit : ▪ Au moins de privilèges nécessaires pour la réalisation du travail ? ▪ Uniquement affecté aux rôles qui nécessitent spécifiquement cet accès privilégié ?	▪ Examiner les politiques de contrôle d'accès ▪ Interroger le personnel ▪ Gestion de l'entretien ▪ Examiner les ID d'utilisateur privilégié	☐	☐	☐	☐
7.1.3	Les accès sont-ils basés sur la classification et la fonction professionnelles de chaque employé ?	▪ Examiner les politiques de contrôle d'accès ▪ Gestion de l'entretien ▪ Examiner les ID d'utilisateur	☐	☐	☐	☐

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
9.5	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 support électronique contenant des données de titulaires de carte.*	▪ Examiner les politiques et procédures en termes de sécurisation physique des supports ▪ Interroger le personnel	☐	☐	☐	☐
9.6	(a) Un contrôle strict s'applique-t-il à la distribution interne ou externe d'un type de support ?	▪ Examiner les politiques et procédures de distribution des supports	☐	☐	☐	☐
	(b) Les contrôles comprennent-ils les éléments suivants :					
9.6.1	Les supports sont-ils classés afin de déterminer la sensibilité des données qu'ils contiennent ?	▪ Examiner les politiques et procédures de classification des supports ▪ Interroger le personnel de la sécurité	☐	☐	☐	☐
9.6.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?	▪ Interroger le personnel ▪ Examiner les journaux de suivi et la documentation de distribution des supports	☐	☐	☐	☐
9.6.3	L'approbation de la direction est-elle obtenue avant le déplacement des supports (particulièrement lorsque le support est distribué aux individus) ?	▪ Interroger le personnel ▪ Examiner les journaux de suivi et la documentation de distribution des supports	☐	☐	☐	☐
9.7	Un contrôle strict est-il réalisé sur le stockage et l'accessibilité des supports ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐
9.8	(a) Tous les supports sont-ils détruits lorsqu'ils ne sont plus utiles pour des raisons professionnelles ou légales ?	▪ Examiner les politiques et procédures de destruction régulière de supports	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(c) La destruction des supports est-elle réalisée comme suit :					
9.8.1	(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 ?	• Examiner les politiques et procédures de destruction régulière de supports • Interroger le personnel • Observer les processus	☐	☐	☐	☐
	(b) Les contenants utilisés pour stocker les informations à détruire sont-ils sécurisés pour prévenir l'accès à leur contenu ?	• Examiner les politiques et procédures de destruction régulière de supports • Examiner la sécurité des contenants de stockage	☐	☐	☐	☐
9.9	Les appareils qui capturent les données de carte de paiement par interaction physique directe avec la carte sont-ils protégés des manipulations malveillantes et des substitutions ? ***Remarque :*** *Cette condition s'applique aux appareils de lecture de carte utilisés dans les transactions pour lesquelles la carte est présente (c'est-à-dire, une lecture de piste ou de puce) au point de vente. Cette condition n'est pas destinée à être appliquée pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.* ***Remarque :*** *La condition 9.9 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.*					
	(a) Est-ce que les politiques et les procédures nécessitent qu'une liste de ces appareils soit conservée ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐
	(b) Est-ce que les politiques et les procédures nécessitent que les appareils soient régulièrement inspectés afin de vérifier qu'aucune manipulation malveillante ou substitution n'a eu lieu ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(c) Est-ce que les politiques et les procédures exigent que le personnel soit formé à être conscient des comportements suspects et à signaler les manipulations malveillantes ou la substitution d'appareil ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐
9.9.1	(a) Est-ce que la liste d'appareils comprend ce qui suit ? • Marque et modèle de l'appareil ; • L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve l'appareil) ; • Le numéro de série de l'appareil ou autre méthode d'identification unique	▪ Examiner la liste d'appareils	☐	☐	☐	☐
	(b) La liste est-elle précise et à jour ?	▪ Observer l'emplacement des appareils et comparer à la liste	☐	☐	☐	☐
	(c) La liste des appareils est-elle mise à jour lorsque des appareils sont ajoutés, déplacés, retirés du service, etc. ?	▪ Interroger le personnel	☐	☐	☐	☐
9.9.2	(a) Les surfaces des appareils sont-elles régulièrement inspectées comme suit pour voir si elles présentent des signes de manipulations malveillantes (par exemple, l'ajout de copieur de carte sur l'appareil), ou de substitution (par exemple, en inspectant le numéro de série ou autre caractéristique de l'appareil pour vérifier qu'il n'a pas été substitué par un appareil frauduleux) ? ***Remarque :*** *Les exemples de signes qu'un appareil aurait pu être la victime de manipulations malveillantes ou substituées comprennent les fixations de câble ou de dispositifs inattendus à l'appareil, les étiquettes de sécurité manquantes ou modifiées, un boîtier cassé ou de couleur différente, ou un changement du numéro de série ou autres marques externes.*	▪ Interroger le personnel ▪ Observer les processus d'inspection et les comparer aux processus définis	☐	☐	☐	☐
	(b) Le personnel est-il conscient des procédures d'inspection des appareils ?	▪ Interroger le personnel	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
9.9.3	Le personnel est-il formé afin d'être conscient des tentatives de manipulation malveillantes ou de remplacement des appareils, y compris ce qui suit ?					
	(a) Est-ce que le matériel pour le personnel aux points de vente comprend ce qui suit ? • Vérifier l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils. • Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification. • Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues). • Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité).	▪ Examiner le matériel de formation	☐	☐	☐	☐
	(b) Le personnel du point de vente a-t-il reçu une formation et est-il conscient des procédures utilisées pour détecter et signaler les tentatives de manipulation malveillante ou de remplacement des appareils ?	▪ Interroger le personnel des POS	☐	☐	☐	☐

Gestion d'une politique de sécurité des informations

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

Remarque : *Dans le cadre de la condition 12, le terme « personnel » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou ont accès d'une manière ou d'une autre à l'environnement des données des titulaires de carte de la société.*

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.1	Une politique de sécurité est-elle établie, publiée, gérée et diffusée à tout le personnel compétent ?	▪ Examiner la politique de sécurité des informations	☐	☐	☐	☐
12.1.1	La politique de sécurité examinée comprend-elle au moins un examen annuel avec une mise à jour chaque fois que l'environnement change ?	▪ Examiner la politique de sécurité des informations ▪ Interroger le personnel responsable	☐	☐	☐	☐
12.3	Les politiques d'utilisation des technologies critiques sont elles développées pour définir l'utilisation adéquate de ces technologies et nécessitent ce qui suit : ***Remarque :*** *Les exemples de technologies critiques comprennent notamment l'accès à distance et les technologies sans-fil, les ordinateurs portables, les tablettes, les supports électroniques amovibles, l'utilisation d'e-mail et d'Internet.*					
12.3.1	Approbation explicite par les parties autorisées pour l'usage des technologies ?	▪ Examiner les politiques d'utilisation ▪ Interroger le personnel responsable	☐	☐	☐	☐
12.3.3	Liste de tous les périphériques et employés disposant d'un accès ?	▪ Examiner les politiques d'utilisation ▪ Interroger le personnel responsable	☐	☐	☐	☐
12.3.5	Usages acceptables des technologies ?	▪ Examiner les politiques d'utilisation ▪ Interroger le personnel responsable	☐	☐	☐	☐
12.4	La politique et les procédures de sécurité définissent-elles les responsabilités de tout le personnel en la matière ?	▪ Examiner la politique et les procédures de sécurité des informations ▪ Interroger un échantillon du personnel responsable	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.5	(b) Les responsabilités suivantes de gestion de la sécurité des informations sont-elles formellement assignées à un individu ou à une équipe :					
12.5.3	Définir, renseigner et diffuser les procédures de remontée et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations ?	▪ Examiner la politique et les procédures de sécurité des informations	☐	☐	☐	☐
12.6	(a) Un programme formel de sensibilisation à la sécurité est-il en place pour sensibiliser les employés à l'importance de la sécurité des données de titulaires de cartes ?	▪ Examiner le programme de sensibilisation à la sécurité	☐	☐	☐	☐
12.8	Des politiques et des procédures sont-elles maintenues et mises en œuvre pour gérer les prestataires de service avec lesquels les données de titulaire de carte sont partagées, ou qui sont susceptibles d'affecter la sécurité des données de titulaire de carte, comme suit :					
12.8.1	Une liste des prestataires de services est-elle tenue ?	▪ Examiner les politiques et les procédures ▪ Observer les processus ▪ Examiner la liste des prestataires de services.	☐	☐	☐	☐
12.8.2	Un accord écrit est-il passé par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données de titulaire qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données du titulaire ? ***Remarque :*** *La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.*	▪ Respecter les accords écrits ▪ Examiner les politiques et les procédures	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.8.3	Existe-t-il un processus de sélection des prestataires de services, comprenant notamment des contrôles préalables à l'engagement ?	▪ Observer les processus ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative	☐	☐	☐	☐
12.8.4	Existe-t-il un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an ?	▪ Observer les processus ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative	☐	☐	☐	☐
12.8.5	Les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation sont-elles maintenues ?	▪ Observer les processus ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative	☐	☐	☐	☐
12.10.1	(a) Un plan de réponse aux incidents a-t-il été créé pour être implémenté en cas d'intrusion dans le système ?	▪ Examiner le plan de réponse aux incidents ▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐

Annexe A : Autres conditions de la norme PCI DSS s'appliquant aux prestataires de services d'hébergement partagé

Cette annexe n'est pas utilisée pour les évaluations des commerçants.

Annexe B : Fiche de contrôles compensatoires

Utiliser cette fiche pour définir les contrôles compensatoires pour toute condition pour laquelle « OUI avec CCW » a été coché.

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.*

Consulter les annexes B, C et D du PCI DSS pour les informations concernant l'utilisation des contrôles compensatoires et les conseils pour aider à remplir cette fiche.

Numéro et définition des clauses :

	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.	

Annexe C : Explication de non-applicabilité

Si la colonne « S.O. » (sans objet) a été cochée dans le questionnaire, utiliser cette fiche de travail pour expliquer pourquoi la condition relative n'est pas applicable à votre organisation.

Condition	Raison pour laquelle la condition n'est pas applicable
3.4	Les données de titulaire de carte ne sont jamais stockées sur support électronique

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

En se basant sur les résultats mentionnés dans le SAQ B en date du *(date d'achèvement)*, les signataires identifiés dans les parties 3b-3d, le cas échéant, confirment le statut de conformité suivant pour l'entité identifiée dans la partie 2 de ce document en date du *(date)* : (***biffer la mention applicable) :***

☐	**Conforme :** Toutes les sections du SAQ PCI DSS sont remplies, toutes les questions ayant eu une réponse affirmative, ce qui justifie une classification globale comme **CONFORME**, *ainsi,* (nom de la société de commerçant) a apporté la preuve de sa pleine conformité à la norme PCI DSS.
☐	**Non conforme :** Les sections du questionnaire SAQ PCI DSS ne sont pas toutes complétées ou certaines questions n'ont pas une réponse affirmative, ce qui justifie sa classification globale comme **NON CONFORME**, ainsi *(Nom de la société du commerçant)* n'a 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 auprès de votre acquéreur ou de la ou des marques de paiement avant de compléter la Partie 4.*
☐	**Conforme, mais avec exception légale :** Une ou plusieurs conditions donnent lieu à une mention « Non » en raison d'une restriction légale qui ne permet pas de respecter la condition. Cette option nécessite un examen supplémentaire de la part de l'acquéreur ou de la marque de paiement. *Si elle est cochée, procéder comme suit :*

Condition affectée	Détails de la manière avec laquelle les contraintes locales empêchent que la condition soit respectée.

Partie 3a. Reconnaissance du statut

Le ou les signataires confirment :

(Cocher toutes les mentions applicables)

☐	Le questionnaire d'auto-évaluation B 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 à tous points de vue.
☐	J'ai vérifié auprès de mon fournisseur d'application de paiement que mon système de paiement ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme, ainsi qu'elle s'applique à mon environnement, à tout moment.
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.

Partie 3a. Reconnaissance du statut (suite)	
☐	Aucune preuve de stockage de données de bande magnétique[1], de données CAV2, CVC2, CID ou CVV2[2], ou de données de code PIN [3]après transaction n'a été trouvée sur AUCUN système examiné pendant cette évaluation.
☐	Les analyses ASV sont effectuées par le fournisseur d'analyse approuvé par le PCI SSC *(nom de l'ASV)*

Partie 3b. Attestation de commerçant	
Signature du représentant du commerçant ↗	*Date :*
Nom du représentant du commerçant :	*Poste occupé :*

Partie 3c. Reconnaissance QSA (le cas échéant)	
Si un QSA a pris part ou a aidé à cette évaluation, décrire la fonction remplie :	

Signature du QSA ↗	*Date :*
Nom du QSA :	*Société QSA :*

Partie 3d. Reconnaissance ISA (le cas échéant)	
Si un ISA a pris part ou a aidé à cette évaluation, décrire la fonction remplie :	

Signature de l'ISA ↗	*Date :*
Nom de l'ISA :	*Poste occupé :*

[1] Données encodées sur la bande magnétique ou données équivalentes sur une puce utilisées pour une autorisation lors d'une transaction carte présente. Les entités ne peuvent pas conserver l'ensemble des données de piste après autorisation des transactions. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte primaire (PAN), la date d'expiration et le nom du titulaire de carte.

[2] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou au verso d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

[3] Les données PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

Partie 4. Plan d'action pour les conditions non conformes

Sélectionner la réponse appropriée pour « conforme aux conditions PCI DSS » pour chaque condition. Si votre réponse est « Non » à la moindre condition, vous êtes susceptible de devoir indiquer la date à laquelle votre société s'attend à être conforme à la condition et une brève description des actions prises pour respecter la condition.

Vérifier auprès de votre acquéreur ou de la ou des marques de paiement avant de compléter la Partie 4.

Condition PCI DSS	Description de la condition	Conforme aux conditions de la norme PCI DSS (Sélectionner un point)		Date et actions de mise en conformité (si « NON » a été sélectionné pour la moindre des conditions)
		OUI	NON	
3	Protéger les données du titulaire stockées	☐	☐	
4	Crypter la transmission des données du titulaire sur les réseaux publics ouverts	☐	☐	
7	Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître	☐	☐	
9	Restreindre l'accès physique aux données du titulaire	☐	☐	
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐	