Industrie des cartes de paiement (PCI)
Norme de sécurité des données

Questionnaire d'auto-évaluation A
et attestation de conformité

Commerçants carte absente, toutes les fonctions de données de titulaires de carte sont entièrement sous-traitées

Destiné à une utilisation avec PCI DSS version 3.2.1

Juin 2018

Modifications apportées au document

Date	Version de PCI DSS	Révision SAQ	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.
Avril 2015	3.1		Mise à jour afin de s'harmoniser avec la norme PCI DSS v3.1. Pour plus de détails sur les modifications de PCI DSS, veuillez consulter *PCI DSS – Récapitulatif des changements entre les versions 3.0 et 3.1 de la norme PCI DSS*.
Juillet 2015	3.1	1.1	Mise à jour de la numérotation des versions afin de s'harmoniser avec d'autres SAQ.
Avril 2016	3.2	1.0	Mise à jour afin de s'harmoniser avec la norme PCI DSS v3.2. Pour plus de détails sur les modifications de PCI DSS, veuillez consulter *PCI DSS – Récapitulatif des changements entre les versions 3.1 et 3.2 de la norme PCI DSS.* Conditions ajoutées de PCI DSS v3.2 Conditions 2, 8 et 12.
Janvier 2017	3.2	1.1	Modifications du document actualisées pour clarifier les conditions ajoutées dans la mise à jour d'avril 2016. Note ajoutée à la section « Avant de Commencer » pour clarifier l'intention d'inclure les Conditions 2 et 8 de PCI DSS.
Juin 2018	3.2.1	1.0	Mise à jour afin de s'harmoniser avec la norme PCI DSS v3.2.1. Pour plus de détails sur les modifications de PCI DSS, veuillez consulter *PCI DSS – Récapitulatif des changements entre les versions 3.2 et 3.2.1 de la norme PCI DSS.* Condition 6.2 ajoutée à partir de PCI DSS v3.2.1.

Remerciements

Le texte en anglais devra, à toutes fins, être considéré comme la version officielle de ce document, et dans la mesure où il existerait toute ambiguïté ou incohérence entre ce texte et le texte en anglais, le texte en anglais en ce lieu prévaudra.

Table des matières

Avant de commencer

Le SAQ A a été conçu pour répondre aux conditions applicables aux commerçants dont les fonctions liées aux données de titulaires de carte sont entièrement sous-traitées à des tiers validés, où le commerçant conserve uniquement des rapports ou des reçus sur papier avec les données de titulaires de carte.

Les commerçants SAQ A peuvent être des commerçants du commerce électronique ou commande par courrier/téléphone (carte absente) et ils ne stockent, ne traitent et ne transmettent pas de données de titulaires de carte au format électronique dans leurs systèmes ou leurs locaux.

Les commerçants SAQ A ont confirmé que, pour ce réseau de paiement :

- Votre société accepte uniquement les transactions carte absente (commerce électronique ou commande par courrier/téléphone) ;
- Tous les traitements de données de titulaires de carte sont entièrement sous-traités à des prestataires de services tiers dont la conformité à la norme PCI DSS est validée ;
- Votre 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 tiers ;
- Votre société a confirmé que le ou les tiers qui gèrent le stockage, le traitement et/ou la transmission des données du titulaire de carte sont conformes à la norme PCI DSS ; et
- Toutes les données du titulaire de carte que votre société conserve sur papier (par exemple les rapports ou les reçus imprimés), et ces documents ne sont pas reçus par voie électronique.

En outre, pour les réseaux de commerce électronique :

- Tous les éléments de la ou des pages de paiement livrées au navigateur du client proviennent uniquement et directement du ou de plusieurs prestataires de service tiers, dont la conformité à la norme PCI DSS est validée.

Ce SAQ n'est pas applicable à tous les réseaux face à face.

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.

Remarque : *Pour ce questionnaire d'auto-évaluation (SAQ), les conditions PCI DSS qui règlent la protection des systèmes informatiques (par exemple, les conditions 2, 6 et 8) s'appliquent aux commerçants en ligne qui redirigent les clients de leur site Internet vers un tiers pour traiter le paiement, et notamment vers le serveur Web du commerçant sur lequel se trouve le mécanisme de redirection. Les commerçants de la vente par correspondance, par téléphone (MOTO) ou en ligne qui ont complètement externalisé toutes les opérations (lorsqu'il n'y a aucun mécanisme de redirection du commerçant vers un tiers) et qui n'ont donc aucun système concerné par ce SAQ, considéreront que ces conditions sont « inapplicables ». Référez-vous aux conseils dans les pages suivantes pour savoir comment signaler les conditions qui ne sont pas applicables.*

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

1. Identifier le SAQ applicable pour votre environnement—consulter les *Instructions et directives relatives aux questionnaires d'auto-évaluation* sur le site Web 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 A)
    - 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 (AOC), ainsi que toute autre documentation requise, comme 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.
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 :		
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) ☐ Commerce électronique ☐ Carte présente (face à face)	Quels réseaux de paiement sont couverts par ce SAQ ? ☐ Commande postale/commande par téléphone (MOTO) ☐ 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 2. Résumé (suite)

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 les données du titulaire de carte ?	

Partie 2c. Emplacements

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

Type de local	Nombre de locaux de ce type	Emplacement(s) du local (ville, pays)
Exemple : Commerces de détail	*3*	*Boston, Massachusetts, États-Unis*

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	
			☐ 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 titulaires de carte (CDE).* • *Composants critiques du système dans le CDE, comme les appareils de POS, les bases de données, les serveurs Web,*	

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

Partie 2. Résumé (suite)

Partie 2f. Prestataires de services tiers

Est-ce que votre société a recours à un intégrateur et revendeur qualifié (QIR) ?	☐ Oui ☐ Non
Si oui :	
Nom de la société QIR :	
Nom individuel QIR :	
Description des services fournis par QIR :	
Est-ce que votre société partage des données de titulaires de carte avec des prestataires de service tiers (par exemple, intégrateurs et revendeurs qualifiés (QIR), 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 participer au questionnaire SAQ A

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

☐	Les commerçants acceptent uniquement les transactions carte absente (commerce électronique ou commande par courrier/téléphone) ;
☐	Tous les traitements de données de titulaires de carte sont entièrement sous-traités à des prestataires de services tiers dont la conformité à la norme PCI DSS est validée ;
☐	Le commerçant 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 tiers ;
☐	Le commerçant a confirmé que le ou les tiers qui gèrent le stockage, le traitement et/ou la transmission des données de titulaires de carte sont conformes à la norme PCI DSS ; **et**

☐	Toutes les données de titulaires de carte, que le commerçant conserve sur papier (par exemple les rapports ou les reçus imprimés), et ces documents ne sont pas reçus par voie électronique.
☐	*En outre, pour les réseaux de commerce électronique :* Tous les éléments de la ou des pages de paiement livrées au navigateur du client proviennent uniquement et directement du ou de plusieurs prestataires de service tiers, dont la conformité à la norme PCI DSS est validée.

Section 2 : 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 d'achèvement de l'auto-évaluation :

Créer et maintenir un réseau et des systèmes sécurisés

Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.1	(a) Les paramètres par défaut définis par le fournisseur sont-ils toujours changés avant l'installation d'un système sur le réseau ? *Cette pratique s'applique à TOUS les mots de passe par défaut, y compris mais sans s'y limiter, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, les comptes d'application et de système, les terminaux de point de vente (POS), les applications de paiement, les chaînes de communauté de protocoles de gestion de réseau simple [SNMP], etc.).*	▪ Examiner les politiques et les procédures. ▪ Examiner la documentation du vendeur. ▪ Observer les configurations du système et les paramètres de compte. ▪ Interroger le personnel.	☐	☐	☐	☐
	(b) Les comptes par défaut inutiles sont-ils supprimés ou désactivés avant l'installation d'un système sur le réseau ?	▪ Examiner les politiques et les procédures. ▪ Examiner la documentation du vendeur. ▪ Examiner les configurations du système et les paramètres de compte. ▪ Interroger le personnel.	☐	☐	☐	☐

Gestion d'un programme de gestion des vulnérabilités

Condition 6 : Développer et maintenir des systèmes et des applications sécurisés

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
6.2	(a) Tous les logiciels et les composants du système sont-ils protégés des vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐
	(b) Les correctifs de sécurité essentiels sont-ils installés dans le mois qui suit leur publication ?	▪ Examiner les politiques et les procédures. ▪ Examiner les composants de système. ▪ Comparer la liste des correctifs de sécurité installés aux listes de correctifs récents fournis par les vendeurs.	☐	☐	☐	☐

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 8 : Identifier et authentifier l'accès aux composants du système

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.1.1	Tous les utilisateurs se voient-ils assigner un ID unique avant d'être autorisés à accéder aux composants du système ou aux données de titulaires de carte ?	▪ Examiner les procédures de mots de passe. ▪ Interroger le personnel.	☐	☐	☐	☐
8.1.3	L'accès des utilisateurs qui ne travaillent plus pour la société est-il immédiatement désactivé ou révoqué ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les comptes utilisateur fermés. ▪ Examiner les listes d'accès actuelles. ▪ Observer les appareils d'authentification physique renvoyés.	☐	☐	☐	☐
8.2	Outre l'assignation d'un ID unique, l'une ou plusieurs des méthodes suivantes sont-elles employées pour authentifier tous les utilisateurs ? ▪ Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; ▪ Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; ▪ Quelque chose concernant l'utilisateur, comme une mesure biométrique.	▪ Examiner les procédures de mots de passe. ▪ Observer les processus d'authentification.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.2.3	(a) Les paramètres de mot de passe utilisateur sont-ils configurés de sorte que les mots de passe/locutions de passage requis respectent les points suivants ? • Des mots de passe d'une longueur d'au moins sept caractères • Contenant à la fois des caractères numériques et des caractères alphabétiques Autrement, les mots de passe/locutions de passage doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.	▪ Examiner les paramètres de configuration du système pour vérifier les paramètres des mots de passe.	☐	☐	☐	☐
8.5	Les comptes et mots de passe ou autres méthodes d'authentification de groupe, partagée ou générique sont-ils interdits comme suit : ▪ Les ID d'utilisateur et les comptes génériques sont désactivés ou supprimés ; ▪ Il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ; ▪ Les ID d'utilisateur partagés ou génériques ne sont pas utilisés pour l'administration du moindre composant du système ?	▪ Examiner les politiques et les procédures. ▪ Examiner les listes d'ID utilisateur. ▪ Interroger le personnel.	☐	☐	☐	☐

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

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 relatifs à la 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 relatifs à la 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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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 des supports.	☐	☐	☐	☐
	(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 des 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 la sécurité des contenants de stockage.	☐	☐	☐	☐

Gestion d'une politique de sécurité des informations

Condition 12 : Maintenir 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 de 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.
12.8	Des politiques et des procédures sont-elles maintenues et mises en œuvre pour gérer les prestataires de service avec lesquels les données de titulaires de carte sont partagées, ou qui sont susceptibles d'affecter la sécurité des données de titulaires de carte, comme suit :					
12.8.1	Est-ce qu'une liste des prestataires de services est conservée, y compris une description du ou des services fournis ?	▪ 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 titulaires de carte 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 de titulaires de carte ? ***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 du plan de réponse aux incidents.	☐	☐	☐	☐

Annexe A : Autres conditions de la norme PCI DSS

Annexe A1 : 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 A2 : Conditions supplémentaires de la norme PCI DSS pour les entités utilisant les protocoles SSL/TLS initial pour les connexions POS POI avec carte à des terminaux

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

Annexe A3 : Validation complémentaire des entités désignées (DESV)

Cette annexe s'applique uniquement aux entités désignées par des marques de paiement ou un acquéreur dans la mesure où une validation supplémentaire des conditions PCI DSS existantes est exigée. Les entités devant valider cette annexe doivent utiliser le modèle de rapport complémentaire DESV et l'attestation complémentaire de conformité à des fins de rapport et consulter la marque de paiement applicable et/ou l'acquéreur pour les procédures de demande.

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 de 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
Exemple :	
3.4	Les données de titulaires 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

Cet AOC dépend des résultats figurant dans SAQ A (Section 2), datés du *(date d'achèvement du SAQ).*

En se basant sur les résultats documentés dans le SAQ A noté ci-dessus, 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 : (***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 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 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 3. Validation PCI DSS *(suite)*

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 de l'évaluateur de sécurité qualifié (QSA) (le cas échéant)

Si un QSA a pris part ou a contribué à cette évaluation, décrire la fonction remplie :	

Signature du cadre supérieur dûment autorisé de la société QSA ↗	*Date :*
Nom du cadre supérieur dûment autorisé :	*Société QSA :*

Partie 3d. Implication de l'évaluateur de sécurité interne (ISA) (le cas échéant)

Si un ou des ISA ont pris part ou ont contribué à cette évaluation, identifier le personnel ISA et décrire la fonction remplie :	

[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	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.	☐	☐	
6	Développer et gérer des systèmes et des applications sécurisés.	☐	☐	
8	Identifier et authentifier l'accès à tous les composants de système.	☐	☐	
9	Restreindre l'accès physique aux données des titulaires de cartes.	☐	☐	
12	Maintenir une politique qui adresse les informations de sécurité pour l'ensemble du personnel.	☐	☐	

** Les conditions PCI DSS indiquées ici se rapportent aux questions posées dans la Section 2 du SAQ.*