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

Questionnaire d'auto-évaluation P2PE

et attestation de conformité

Commerçants utilisant des terminaux de paiement matériels dans une solution PCI SSC listée P2PE uniquement – Aucun stockage électronique de données de titulaires de carte

Destiné à une utilisation avec PCI DSS version 3.2

Avril 2016

Modifications apportées au document

Date	Version de PCI DSS	Révision SAQ	Description
S.O.	1.0		Non utilisé.
Mai 2012	2.0		Créer un SAQ P2PE-HW pour les commerçants utilisant uniquement des terminaux matériels dans le cadre d'une solution P2PE validée et listée par PCI SSC. Ce SAQ est destiné à une utilisation avec PCI DSS v2.0.
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*. Suppression de la mention « HW » dans le titre de SAQ, car elle peut être utilisée par les commerçants munis d'une solution HW/HW ou HW/P2PE hybride.
Juillet 2015	3.1	1.1	Mise à jour pour supprimer les références aux « meilleures pratiques » avant le 30 juin 2015.
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*.

Table des matières

Avant de commencer

Critère d'éligibilité des commerçants pour SAQ P2PE

Le SAQ P2PE a été élaboré pour répondre aux conditions applicables aux commerçants qui traitent les données de titulaires de carte uniquement par des terminaux de paiement matériels inclus dans une solution de cryptage point en point (P2PE) listée par PCI.

Les commerçants SAQ P2PE n'ont pas accès aux données de titulaires de carte en texte clair sur n'importe quel système informatique et ils entrent uniquement les données de compte sur les terminaux de paiement matériels d'une solution P2PE approuvée PCI SSC. Les commerçants SAQ P2PE peuvent être des commerçants directs (carte présente) ou des commerçants par courrier/téléphone (carte non présente). Par exemple, un commerçant par courrier/téléphone peut être éligible pour SAQ P2PE s'il reçoit les données de titulaires de carte sur papier ou par téléphone et qu'il les saisit directement dans un matériel validé P2PE.

Les commerçants SAQ P2PE confirment que, pour ce réseau de paiement :

- Tout service de traitement de paiement est effectué par la solution PCI P2PE approuvée et listée par le PCI SSC.
- Les seuls systèmes dans l'environnement du commerçant qui stockent, traitent ou transmettent les données de compte sont les appareils de point d'interaction (POI) qui sont approuvées pour utilisation avec la solution P2PE validée et listée PCI.
- Votre société ne reçoit ou ne transmet pas par voie électronique les données de titulaires de carte.
- Il n'existe pas d'ancien système de stockage électronique de données de titulaires de carte dans l'environnement.
- Si votre société stocke des données de titulaires de carte, ces données sont uniquement des rapports imprimés ou des copies de bordereaux et ne sont pas reçues par voie électronique **et**
- Votre société a mis en œuvre tous les contrôles du *Mode d'emploi P2PE (PIM)* fourni par le prestataire de la solution P2PE.

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 par les critères d'éligibilité 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.

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 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. Confirmez que vous avez mis en œuvre tous les éléments du PIM.
4. Évaluez la conformité de votre environnement aux conditions applicables de la norme PCI DSS.
5. 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 P2PE)

- Section 3 (Parties 3 & 4 de l'AOC) – Détails de validation et d'attestation, et plan d'action pour les conditions de non-conformité (s'il y a lieu)

6. Envoyer le SAQ et l'attestation de conformité (AOC), ainsi que toute autre documentation requise, à votre l'acquéreur, 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 remplissez 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 comme déclaration des résultats de l'auto-évaluation des *Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données de l'industrie 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 votre 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 concernées) :

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

Quels types de réseaux de paiement votre entreprise sert-elle ?	Quels réseaux de paiement sont couverts par ce SAQ ?
☐ Commande postale/commande par téléphone (MOTO)	☐ Commande postale/commande par téléphone (MOTO)
☐ Commerce électronique	☐ Commerce électronique
☐ Carte présente (face à face)	☐ 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 (par exemple : commerces de détail, siège social, centre de données, centre 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. Solution P2PE

Fournir les informations suivantes concernant la solution PCI P2PE validée qu'utilise votre organisation :

Nom du prestataire de la solution P2PE :	
Nom de la solution P2PE :	
Numéro de référence PCI SSC	
Périphériques de POI P2PE énumérés et utilisés par le commerçant (dépendances de périphériques PTS) :	

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 consacrée à la segmentation de réseau de PCI DSS pour les recommandations concernant la segmentation de réseau)*	☐ Oui ☐ Non

Partie 2f. Prestataires de services tiers

Est-ce que votre société a recours à un intégrateur et revendeur qualifié (QIR) ? Si oui : Nom de la société QIR : Nom individuel QIR : Description des services fournis par QIR :	☐ Oui ☐ Non
Est-ce que votre société partage les données de titulaires de carte avec des prestataires de service tiers (par exemple, intégrateurs et revendeurs qualifiés (QIR), passerelles, agents de réservation de compagnie aérienne, agents de programme de fidélisation, etc.) ? ***Si oui :***	☐ Oui ☐ Non

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

Remarque : *La condition 12.8 s'applique à toutes les entités mentionnées en réponse à cette question.*

Partie 2g. Admissibilité à participer au questionnaire SAQ P2PE

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

☐	Tout traitement de paiement est effectué par la solution PCI P2PE approuvée et listée par le PCI SSC (selon les critères ci-dessus).
☐	Les seuls systèmes dans l'environnement du commerçant qui stockent, traitent ou transmettent les données de compte sont les appareils de point d'interaction (POI) qui sont approuvées pour utilisation avec la solution P2PE validée et listée PCI.
☐	Le commerçant ne reçoit ou ne transmet pas d'autre manière électronique les données de titulaires de carte.
☐	Le commerçant vérifie qu'il n'existe pas de système ancien de stockage électronique de données de titulaires de carte dans l'environnement.
☐	Si le commerçant stocke des données de titulaires de carte, ces données ne sont que des rapports imprimés ou des copies de bordereaux et ne sont pas reçues par voie électronique **et**
☐	Le commerçant a mis en œuvre tous les contrôles du Mode d'emploi P2PE (PIM) fourni par le prestataire de la solution P2PE.

Section 2 : Questionnaire d'auto-évaluation P2PE

Remarque : *Les questions suivantes sont numérotées conformément aux conditions PCI DSS réelles et aux procédures de test, comme défini dans le document* Conditions et procédures d'évaluation de sécurité de la norme PCI DSS*. Dans la mesure où seul un sous-ensemble des conditions PCI DSS est inclus dans ce SAQ P2PE, il est possible que la numérotation de ces questions ne se suive pas.*

Date d'achèvement de l'auto-évaluation :

Protection des données de titulaires de carte

Condition 3 : Protéger les données de titulaires de carte stockées

Remarque : *La condition 3 s'applique uniquement aux commerçants SAQ P2PE qui disposent de registres sur papier (par exemple des reçus, rapports imprimés, etc.) avec des données de compte, y compris les numéros de comptes principaux (PAN).*

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
3.1	Les politiques, processus et procédures de conservation et d'élimination de données sont-elles déployées comme suit :					
	(a) La quantité de données stockées et le délai de conservation sont-ils limités aux obligations légales, réglementaires et/ou commerciales ?	▪ Examiner les politiques et procédures de conservation et d'élimination des données ▪ Interroger le personnel	☐	☐	☐	☐
	(b) Des processus définis sont-ils en place pour supprimer les données de titulaires de carte de manière sécurisée lorsqu'elles ne sont plus requises pour des raisons légales, réglementaires et/ou commerciales ?	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Examiner le mécanisme de suppression	☐	☐	☐	☐
	(c) Des conditions spécifiques de conservation spécifiques des données de titulaires de carte sont-elles en place ? *Par exemple, les données de titulaires de carte doivent être détenues durant une période X pour des raisons professionnelles Y.*	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Examiner les exigences en matière de conservation	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(d) Un processus trimestriel est-il en place pour l'identification et la suppression sécurisée des données de titulaires de carte stockées excédant les conditions de conservation définies ?	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Observer les processus de suppression	☐	☐	☐	☐
	(e) Est-ce que toutes les données de titulaires de carte stockées respectent les conditions définies dans la politique de conservation des données ?	▪ Examiner les fichiers et les enregistrements du système	☐	☐	☐	☐
Directive : *Les réponses « Oui » pour les conditions du point 3.1 signifient que si un commerçant conserve des documents sur papier (par exemple des reçus ou des rapports sur papier) qui contiennent des données de compte, le commerçant stocke uniquement les documents papier tant qu'ils sont nécessaires pour des raisons légales et/ou commerciales, et il détruit les documents papier dès qu'ils ne sont plus nécessaires.* *Si un commerçant n'imprime jamais ou ne stocke pas de documents papier contenant des données de compte, le commerçant doit cocher la colonne « S.O. » et remplir la fiche « Explication de la non-applicabilité » dans l'annexe C.*						
3.2.2	Pour tout stockage sur support papier, 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 sur support papier	☐	☐	☐	☐
Directive : *Une réponse « Oui » pour la condition 3.2.2 signifie que si le commerça nt écrit le code de sécurité de la carte lorsqu'une transaction est en cours, le commerçant doit détruire le document papier de manière sécurisée (par exemple dans une déchiqueteuse), immédiatement après la fin de la transaction, ou obscurcir le code (par exemple, en le « noircissant » avec un marqueur) avant que le document papier ne soit stocké.* *Si le commerçant ne demande jamais le numéro à trois ou à quatre chiffres imprimés sur le recto ou le verso d'une carte de paiement (« code de sécurité de la carte »), le commerçant doit cocher la colonne « S.O. » et remplir la fiche « Explication de la non-applicabilité » dans l'annexe C.*						

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
3.7	Les politiques de sécurité et les procédures opérationnelles pour la protection des données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles ▪ Interroger le personnel	☐	☐	☐	☐
Directive : *Une réponse « Oui »à la condition 3.7 signifie que, si le commerçant stocke les données de compte sur support papier, il a mis en place des politiques et procédures pour les conditions 3.1, 3.2.2 et 3.3. Cette disposition aide à assurer que le personnel est conscient et suite les politiques de sécurité et les procédures opérationnelles documentées pour la gestion du stockage sécurisé des données de titulaires de carte sur une base continuelle.*						

Mise en œuvre de mesures de contrôle d'accès strictes

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

Remarque : *Les conditions 9.5 et 9.8 s'appliquent uniquement aux commerçants SAQ P2PE qui disposent de registres sur papier (par exemple des reçus, rapports imprimés, etc.) avec des données de compte, y compris les numéros de comptes principaux (PAN).*

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	☐	☐	☐	☐
9.8	(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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

Question PCI DSS	Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
		Oui	**Oui, avec CCW**	**Non**	**S.O.**
Directive : *Les réponses « Oui » pour les conditions 9.5 et 9.8 signifient que le commerçant stocke de manière sécurisée, par exemple en les stockant dans un tiroir qui ferme à clé, une armoire ou un coffre-fort et que le commerçant détruit ces documents papier lorsqu'ils ne sont plus nécessaires pour des raisons commerciales. Cela inclut un document ou une politique écrite pour les employés afin qu'ils sachent comment sécuriser les documents papier contenant des données de compte et comment détruire le document papier lorsqu'il n'est plus nécessaire.* *Si le commerçant ne stocke jamais de documents papier contenant des données de compte, le commerçant doit cocher la colonne « S.O. » et remplir la fiche « Explication de la non-applicabilité » dans l'annexe C.*					
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.*					
(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	☐	☐	☐	☐
(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	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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	☐	☐	☐	☐

Directive : *Les réponses « Oui » aux conditions 9.9 signifient que le commerçant a mis en place des politiques et des procédures sont en place pour les exigences 9.9.1 à 9.9.3 et qu'il conserve une liste actualisée des appareils, conduit des inspections régulières des appareils et forme les employés concernant ce qu'il faut observer pour détecter les appareils ayant subi des manipulations malveillantes ou ayant été remplacés.*

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
9.10	Les politiques de sécurité et les procédures opérationnelles pour restreindre l'accès physique aux données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles ▪ Interroger le personnel	☐	☐	☐	☐
Directive : *Une réponse « Oui »à la condition 9.10 signifie que le commerçant a mis en place des politiques et des procédures pour les conditions 9.5, 9.8 et 9.9, ainsi qu'il s'applique pour votre environnement. Cela aide à assurer que le personnel est conscient des politiques de sécurité et des procédures opérationnelles documentées, et qu'il les respecte.*						

Gestion d'une politique de sécurité des informations

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

Remarque : La condition 12 spécifie que le commerçant doit avoir des politiques de sécurité de l'information pour son personnel, mais ces politiques peuvent être aussi simples ou complexes que nécessaire pour la taille et la complexité des opérations du commerçant. Le document de la politique doit être fourni à tous les membres du personnel afin qu'ils prennent connaissance de leurs responsabilités en matière de protection des terminaux de paiement, des documents sur support papier contenant les données de titulaires de carte, etc. Si un commerçant n'a pas d'employés, il est attendu qu'il comprenne et reconnaisse ses responsabilités en matière de sécurisation du ou des magasins.

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	☐	☐	☐	☐
Directive : *Les réponses « Oui » pour les conditions de 12.1 signifient que le commerçant dispose d'une politique de sécurité qui est raisonnable pour la taille et la complexité des opérations du commerçant, et que la politique est examinée régulièrement et mise à jour si besoin. Par exemple, cette politique peut être un simple document qui explique comment protéger le magasin et les appareils de paiement selon le* Mode d'emploi P2PE (PIM) *et qui doit être contacté en cas d'urgence.*						
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	☐	☐	☐	☐
Directive : *Une réponse « Oui » pour la condition 12.4.1 signifie que la politique de sécurité du commerçant définit les responsabilités de base en matière de sécurité pour tout le personnel, conformément à la taille et à la complexité des opérations du commerçant. Par exemple, la responsabilité de la sécurité doit être définie en fonction des responsabilités de base selon les niveaux des employés, comme les responsabilités attendues d'un directeur/propriétaire et les responsabilités attendues des agents.*						
12.5	Les responsabilités suivantes de gestion de la sécurité des informations sont-elles assignées à un individu ou à une équipe :					

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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	☐	☐	☐	☐
Directive : *Une réponse « Oui »à la condition 12.5.3 signifie que le commerçant a désigné une personne comme responsable de la réponse aux incidents et du plan d'escalade requise en 12.9.*						
12.6	(a) Un programme formel de sensibilisation à la sécurité est-il en place pour sensibiliser tout le personnel à l'importance de la politique et des procédures de sécurité des données de titulaires de carte ?	▪ Examiner le programme de sensibilisation à la sécurité	☐	☐	☐	☐
Directive : *Les réponses « Oui » pour les conditions de 12.6 signifient que le commerçant dispose d'une politique de sécurité qui est raisonnable pour la taille et la complexité des opérations du commerçant, et que la politique est examinée régulièrement et mise à jour si besoin. Par exemple, un simple programme de sensibilisation peut être constitué d'une brochure placardée dans le bureau ou d'un e-mail envoyé régulièrement aux employés. Les exemples de message de programme de sensibilisation comprennent des descriptions des conseils de sécurité que doivent suivre tous les employés, tels que les méthodes de verrouillage des portes et des contenants de stockage ; comment déterminer si un terminal de paiement a fait l'objet de manipulations malveillantes ; et comment identifier le personnel légitime susceptible de venir pour l'entretien des terminaux matériels de paiement.*						
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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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	☐	☐	☐	☐
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	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
Directive : *Les réponses « Oui » pour les conditions 12.8 signifient que le commerçant possède une liste, ainsi que des accords, avec les prestataires de service avec lesquels ils partagent les données de titulaires de carte. Par exemple, ces accords doivent être applicables si un commerçant utilise une entreprise de conservation de documents pour stocker des documents sur support papier qui contiennent des données de compte.*						
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	☐	☐	☐	☐
Directive : *Les réponses « Oui » pour les conditions de 12.10 signifient que le commerçant a documenté un plan de réponse aux incidents et d'escalade à utiliser en cas d'urgence, conformément à la taille et à la complexité des opérations du commerçant. Par exemple, ce plan peut simplement être un document placardé dans le bureau qui mentionne la personne à contacter pour diverses situations ainsi qu'un examen annuel pour confirmer que cette liste demeure d'actualité ; ou bien il peut s'agir d'un plan total de réponse aux incidents, y compris les locaux de secours « d'urgence »et les procédures complètes de test annuel. Ce plan doit être facilement disponible à la totalité du personnel, en tant que ressource en cas d'urgence.*						

Annexe A : Autres conditions de la norme PCI DSS

Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé

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

Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial

Cette annexe n'est pas utilisée pour les évaluations des commerçants SAQ P2PE.

Annexe A3 : Validation complémentaire des entités désignées (DESV)

Cette annexe s'applique uniquement aux entités désignées par une ou 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 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
Exemple :	
12.8	Les données de titulaires de carte ne sont jamais partagées avec des prestataires de services.

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

Cet AOC dépend des résultats figurant dans SAQ P2PE (Section 2), en date du *(date d'achèvement du SAQ).*

En se basant sur les résultats documentés dans le SAQ P2PE noté ci-dessus, les signataires identifiés dans les parties 3b-3d confirment le statut de conformité pour l'entité identifiée dans la partie 2 de ce document ***(biffer la mention applicable) :***

☐	**Conforme :** Toutes les sections du SAQ P2PE pour la norme PCI DSS sont remplies et toutes les questions ont 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 :** Toutes les sections du SAQ P2PE de la norme PCI DSS ne sont pas sont remplies, ou toutes les questions n'ont pas eu une réponse affirmative, ce qui justifie une classification globale comme **NON CONFORME**, ainsi, *(nom de la société de 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 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.*
☐	**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 PCI DSS P2PE, version *(numéro de version du SAQ)*, a été rempli 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, ainsi qu'elle s'applique à mon environnement, à tout moment.

Partie 3a. Reconnaissance du statut (suite)	
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.
☐	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]n'a été trouvée sur AUCUN système examiné pendant cette évaluation.

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 sur bande magnétique après autorisation des transactions. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte, la date d'expiration et le nom du détenteur.

[2] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou à droite de celui-ci ou encore sur la face avant 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 en cas d'état Non conforme

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 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**	**Conformité aux conditions PCI DSS** (cocher une seule option)		**Date et actions de mise en conformité** (si « NON » a été sélectionné pour la moindre des conditions)
		OUI	**NON**	
3	Protéger les données de titulaires de carte stockées	☐	☐	
9	Restreindre l'accès physique aux données de titulaires de carte	☐	☐	
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐	

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