Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation B-IP et attestation de conformité

Commerçants utilisant des terminaux autonomes, à connexion IP de PTS Point d'interaction (POI) – sans stockage électronique de données de titulaires de carte

Version 3.0

Février 2014

Modifications apportées au document

Date	Version	Description
S.O.	1.0	Non utilisé.
S.O.	2.0	Non utilisé.
Février 2014	3.0	Nouveau SAQ pour répondre aux conditions applicables aux commerçants qui traitent les données de titulaires de carte uniquement par des périphériques autonomes au point d'interaction approuvés PTS avec une connexion IP au service de traitement de paiement. Le contenu est harmonisé avec les conditions de la norme PCI DSS v3.0 et des procédures de test.

Table des matières

Avant de commencer

Le SAQ B-IP a été élaboré pour répondre aux conditions applicables aux commerçants qui traitent les données de titulaires de carte uniquement par des périphériques autonomes, approuvés PTS de point d'interaction (POI) avec connexion IP vers le service de traitement de paiement.

Les commerçants SAQ B-IP 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-IP confirmer que, pour ce réseau de paiement :

- Votre société utilise un périphérique autonome approuvé PTS de point d'interaction (à l'exception des SCR), connecté par IP à votre service de traitement de paiement pour prendre les informations de carte de paiement de votre client ;
- Les périphériques de POI à connexion IP sont validés pour le programme PTS POI ainsi qu'il est mentionné sur le site Internet PCI SSC (à l'exception des SCR) ;
- Les périphériques de POI à connexion IP ne sont connectés à aucun autre système dans votre environnement (cela peut être obtenu en utilisant la segmentation de réseau pour isoler les autres périphériques POI des autres systèmes) ;
- La seule transmission de données de titulaire de carte a lieu à partir des périphériques de POI approuvés par PTS vers le service de traitement de paiement ;
- Le périphérique de POI ne dépend pas d'autres appareils (par ex ordinateur, téléphone mobile, tablette, etc.) pour se connecter au service de traitement de paiement ;
- Votre 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-IP)

- 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	Le test attendu a été effectué et tous les éléments de la condition ont été remplis avec l'aide d'un contrôle compensatoire.

Réponse	Quand utiliser cette réponse :
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

Alors que de nombreuses organisations complétant un SAQ B-IP auront besoin de valider leur conformité à toutes les conditions PCI DSS de ce SAQ, certaines organisations ayant des modèles commerciaux très particuliers ne seront pas concernées par certaines conditions. Par exemple, une société qui n'utilise en aucun cas la technologie sans fil n'est pas contrainte de valider sa conformité aux sections de la norme PCI DSS qui sont spécifiques à la gestion de la technologie sans fil (par exemple, les conditions 1.2.3, 2.1.1 et 4.1.1).

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 environnement PCI DSS ?	☐ Oui

(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-IP

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 un périphérique autonome approuvé PTS de point d'interaction (à l'exception des SCR), connecté par IP à son service de traitement de paiement pour prendre les informations de carte de paiement de votre client ;
☐	Les périphériques de POI à connexion IP sont validés pour le programme PTS POI ainsi qu'il est mentionné sur le site Internet PCI SSC (à l'exception des SCR) ;
☐	Les périphériques de POI autonomes à connexion IP ne sont connectés à aucun autre système dans l'environnement du commerçant (cela peut être obtenu en utilisant la segmentation de réseau pour isoler les autres périphériques POI des autres systèmes) ;
☐	La seule transmission de données de titulaire de carte a lieu à partir des périphériques de POI approuvés par PTS vers le service de traitement de paiement ;
☐	Le périphérique de POI ne dépend pas d'autres appareils (par ex ordinateur, téléphone mobile, tablette, etc.) pour se connecter au service de traitement de paiement ;
☐	Le commerçant conserve uniquement des reçus ou des rapports papier avec les données de titulaire de carte, sans recevoir ces documents au format électronique ; **et**
☐	Le commerçant ne stocke pas les données de titulaire de cartes au format électronique.

Section 2 : Questionnaire d'auto-évaluation B-IP

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 :

Création et gestion d'un réseau sécurisé

Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
1.1.2	(a) Existe-t-il un schéma du réseau actualisé qui comprend toutes les connexions entre l'environnement des données de titulaire de carte et les autres réseaux, y compris les réseaux sans fil ?	▪ Examiner le schéma du réseau actualisé ▪ Examiner les configurations de réseau	☐	☐	☐	☐
	(b) Existe-t-il un processus pour garantir que le schéma est tenu à jour ?	▪ Interroger le personnel responsable	☐	☐	☐	☐
1.1.4	(a) Un pare-feu est-il requis et implémenté au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne ?	▪ Examiner les standards de configuration de pare-feu ▪ Observer les configurations de réseau pour vérifier qu'un ou plusieurs pare-feu sont en place	☐	☐	☐	☐
	(b) Le schéma de réseau actuel est-il conforme aux normes de configuration des pare-feu ?	▪ Comparer les standards de configuration du pare-feu au schéma actualisé du réseau	☐	☐	☐	☐
1.1.6	(a) Les standards de configuration de pare-feu et de routeurs comprennent-ils une liste détaillée des services, protocoles et ports, avec la justification commerciale (protocoles HTTP [Hypertext Transfer Protocol], SSL [Secure Sockets Layer], SSH [Secure Shell] et VPN [Virtual Private Network]) ?	▪ Examiner les standards de configuration de pare-feu et de routeur	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(b) Tous les services, protocoles et ports non sécurisés sont-ils identifiés et les fonctions de sécurité sont-elles documentées et implémentées pour chaque service identifié ? ***Remarque :*** *Les protocoles FTP, Telnet, POP3, IMAP et SNMP sont des exemples de services, protocoles ou ports non sécurisés, mais ne sont pas les seuls.*	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.2	Les configurations de pare-feu restreignent-elles les connexions entre les réseaux non approuvés et les composants du système dans l'environnement des données des titulaires de carte comme suit : ***Remarque :*** *Un « réseau non approuvé » est tout réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.*					
1.2.1	(a) Les trafics entrants et sortants sont-ils restreints au trafic nécessaire à l'environnement des données des titulaires de carte ?	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
	(b) Tous les autres trafics entrants et sortants sont-ils explicitement refusés (par exemple à l'aide d'une instruction « refuser tout » explicite ou d'un refus implicite après une instruction d'autorisation) ?	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.2.3	Les pare-feu de périmètre sont-ils installés entre tous les réseaux sans-fil et l'environnement des données du titulaire, et ces pare-feu sont-ils configurés pour refuser ou, s'il est nécessaire à des fins professionnelles, autoriser uniquement le trafic entre l'environnement sans-fil et l'environnement de données du titulaire de carte ?	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
1.3	L'accès public direct entre Internet et les composants du système dans l'environnement des données de titulaire de carte est-il interdit comme suit :					
1.3.3	Les connexions directes sont-elles interdites pour le trafic entrant ou sortant entre Internet et l'environnement des données des titulaires de carte ?	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.4	Des mesures anti-usurpation sont-elles mises en œuvre pour détecter et pour empêcher les adresses IP de source frauduleuses de pénétrer sur le réseau ? (Par exemple, bloquer le trafic originaire d'Internet avec une adresse interne).	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.5	Le trafic sortant de l'environnement des données des titulaires de carte vers Internet est-il explicitement autorisé ?	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.6	Un contrôle avec état, également connu comme filtrage des paquets dynamique, est-il en place, c'est-à-dire, seules les connexions établies sont autorisées sur le réseau ?	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐

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, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, application ou comptes de système, point de vente (POS) terminaux, 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	☐	☐	☐	☐
2.1.1	Pour les environnements sans fil connectés à l'environnement des données des titulaires de carte ou transmettant ces données, TOUS les paramètres par défaut du vendeur de solutions sans fil sont-ils changés comme suit :					
	(a) Les clés de cryptage par défaut sont-elles modifiées à l'installation et à chaque fois qu'un employé qui les connaît quitte la société ou change de poste ?	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Interroger le personnel	☐	☐	☐	☐
	(b) Les chaînes de communauté SNMP par défaut sur les périphériques sans fil sont-elles modifiées à l'installation ?	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Interroger le personnel ▪ Examiner les configurations de système	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(c) Les mots/phrases de passe par défaut des points d'accès ont-ils été modifiés à l'installation ?	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Examiner les configurations de système	☐	☐	☐	☐
	(d) Le firmware des périphériques sans fil est-il mis à jour de manière à prendre en charge un cryptage robuste pour l'authentification et la transmission sur les réseaux sans fil ?	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Examiner les configurations de système	☐	☐	☐	☐
	(e) Les autres paramètres par défaut liés à la sécurité, définis par le fournisseur des équipements sans fil sont-ils modifiés, le cas échéant ?	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Examiner les configurations de système	☐	☐	☐	☐
2.3	L'accès administratif non-console est-il crypté de manière à : *Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion via le Web et autre accès administratif non-console.*					
	(a) Tous les accès administratifs non-console sont-ils cryptés avec une cryptographie robuste, et une méthode de cryptographie robuste est-elle invoquée avant de demander le mot de passe administrateur ?	▪ Examiner les composants du système ▪ Examiner les configurations de système ▪ Observer un administrateur se connecter	☐	☐	☐	☐
	(b) Tous les fichiers de services du système et de paramètres sont-ils configurés afin de prévenir l'utilisation de Telnet et d'autres commandes de connexions à distances non sécurisées ?	▪ Examiner les composants du système ▪ Examiner les services et les fichiers	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(c) L'accès administrateur aux interfaces de gestion Web est-il crypté au moyen d'une méthode de cryptage robuste ?	▪ Examiner les composants du système ▪ Observer un administrateur se connecter	☐	☐	☐	☐
	(d) Pour la technologie utilisée, une cryptographie robuste est-elle implémentée conformément aux meilleures pratiques du secteur et/ou aux recommandations du fournisseur ?	▪ Examiner les composants du système ▪ Examiner la documentation du vendeur ▪ Interroger le personnel	☐	☐	☐	☐

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) :					
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	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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	☐	☐	☐	☐
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.**
4.1	(a) Des protocoles de cryptographie et de sécurité robustes, SSL/TLS ou IPSEC par exemple, sont-ils déployés pour protéger les données des titulaires de carte sensibles lors de leur transmission sur des réseaux publics ouverts ? *Les exemples de réseaux ouverts et publics comprennent notamment Internet, les technologies sans fil, y compris 802.11 et Bluetooth ; les technologies cellulaires, par exemple Système Global pour communication Mobile (GSM), Code division accès multiple (CDMA) et Service radio paquet général (GPRS).*	▪ Examiner les standards documentés ▪ Examiner les politiques et les procédures ▪ Examiner tous les emplacements où les données de titulaire de carte sont transmises ou reçues ▪ Examiner les configurations de système	☐	☐	☐	☐
	(b) Seuls des clés/certificats approuvés sont-ils acceptés ?	▪ Observer les transmissions entrantes ou sortantes ▪ Examiner les clés et les certificats	☐	☐	☐	☐
	(c) Les protocoles de sécurité sont-ils déployés pour utiliser uniquement des configurations sécurisées et ne pas prendre en charge des versions ou configurations non sécurisées ?	▪ Examiner les configurations de système	☐	☐	☐	☐
	(d) Un niveau de cryptage approprié est-il mi en place pour la méthodologie de cryptage employée (se reporter aux recommandations/meilleures pratiques du fournisseur) ?	▪ Examiner la documentation du vendeur ▪ Examiner les configurations de système	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(e) Pour les implémentations SSL/TLS, le SSL/TLS est activé lorsque les données du titulaire sont transmises ou reçues ? *Par exemple, pour les implémentations basées sur le navigateur :* • *La mention « HTTPS » apparaît comme protocole de l'adresse URL (Universal Record Locator, localisateur uniforme de ressource) du navigateur et* • *Les données du titulaire sont uniquement requises lorsque la mention « HTTPS » apparaît dans l'adresse URL.*	▪ Examiner les configurations de système	☐	☐	☐	☐
4.1.1	Les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont-elles déployées pour appliquer un cryptage robuste à l'authentification et la transmission pour des réseaux sans fil transmettant des données de titulaires de carte ou connectés à l'environnement des données des titulaires de carte ? ***Remarque :*** *L'utilisation du protocole WEP comme contrôle de sécurité est interdite.*	▪ Examiner les standards documentés ▪ Examiner les réseaux sans fil ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐
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	☐	☐	☐	☐

Gestion d'un programme de gestion des vulnérabilités

Condition 6 : Développer et gérer 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.**
6.1	Existe-t-il un processus pour identifier les vulnérabilités de sécurité, y compris les points suivants : ▪ Pour utiliser des sources externes fiables pour les informations sur les vulnérabilités ? ▪ Pour assigner un classement du risque des vulnérabilités qui comprend une identification des vulnérabilités à « haut risque » et des vulnérabilités « critiques » ? ***Remarque** : Le classement des risques doit se baser sur les meilleures pratiques du secteur, ainsi que sur la prise en compte de l'impact potentiel. Par exemple, les critères de classement des vulnérabilités peuvent inclure la prise en compte du score de base CVSS et/ou la classification par le fournisseur et/ou le type de système affecté.* *Les méthodes d'évaluation de vulnérabilité et d'affectation des classements de risque varieront selon l'environnement de l'organisation et la stratégie d'évaluation des risques. Le classement de risque doit, au minimum, identifier toutes les vulnérabilités considérées comme posant un « risque élevé » pour l'environnement. En plus du classement de risque, les vulnérabilités peuvent être considérées comme « critiques » si elles constituent une menace imminente pour l'environnement, ont un impact critique sur les systèmes et/ou si elles sont susceptibles de compromettre l'application si elles ne sont pas résolues. Les exemples de systèmes critiques peuvent inclure les systèmes de sécurité, les dispositifs et systèmes ouverts au public, les bases de données et autres systèmes qui stockent, traitent ou transmettent des données du titulaire.*	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐

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 ? ***Remarque** : Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.*	▪ Examiner les politiques et les procédures ▪ Examiner les composants du système ▪ Comparer la liste des correctifs de sécurité installés aux listes de correctifs fournis par les vendeurs	☐	☐	☐	☐

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 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.
8.1.5	(a) Les comptes utilisés par les commerçants pour l'accès, le soutien ou la maintenance des composants du système par accès à distance sont activés uniquement pendant la période de temps nécessaire et désactivés lorsqu'ils ne sont pas utilisés ?	▪ Examiner les procédures de mot de passe ▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐
	(b) Les comptes d'accès à distance des fournisseurs sont-ils surveillés lorsqu'ils sont utilisés ?	▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐
8.3	Une authentification à deux facteurs est-elle incorporée pour les accès à distance du personnel issu de l'extérieur du réseau (y compris pour les utilisateurs et les administrateurs) et pour tous les tiers (y compris l'accès du fournisseur à fin d'assistance ou de maintenance) ? ***Remarque :*** *L'authentification à deux facteurs requiert d'utiliser deux des trois méthodes d'authentification (voir la condition 8.2 pour la description des méthodes d'authentification). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à deux facteurs.* *Les exemples de technologies à deux facteurs comprennent l'authentification à distance et service de renseignements par téléphone (RADIUS) avec jetons ; les systèmes de contrôle d'accès au contrôleur d'accès du terminal (TACACS) avec jetons et les autres technologies permettant une authentification à deux facteurs.*	▪ Examiner les politiques et les procédures ▪ Examiner les configurations de système ▪ Observer le personnel	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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 ; ▪ Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration d'aucun 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 des titulaires de cartes

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
9.1.2	Des contrôles physiques et/ou logiques sont-ils en place pour restreindre l'accès physique aux prises réseau accessibles au public ? *Par exemple, les prises de réseau situées dans les zones publiques et les zones accessibles aux visiteurs doivent être désactivées et uniquement activées lorsque l'accès au réseau est accepté de manière explicite. Autrement, des processus doivent être mis en œuvre pour assurer que les visiteurs sont accompagnés à tout moment dans les zones contenant des prises réseau actives.*	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Observer les locaux	☐	☐	☐	☐

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	☐	☐	☐	☐
	(c) La destruction des supports est-elle réalisée comme suit :					

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

	Question PCI DSS	Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(b) Le personnel est-il conscient des procédures d'inspection des appareils ?	▪ Interroger le personnel	☐	☐	☐	☐
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	☐	☐	☐	☐

Surveillance et test réguliers des réseaux

Condition 11 : Tester régulièrement les processus et les systèmes de sécurité

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
11.2.2	(a) Des analyses trimestrielles de vulnérabilité externe sont-elles réalisées ? ***Remarque :*** *Les scans de vulnérabilité externe doivent être effectués une fois par trimestre par un prestataire de services de scan agréé (ASV) par le PCI SSC (Payment Card Industry Security Standards Council-Conseil des normes de sécurité PCI).* *Consulter le Guide de programme ASV publié sur le site Web du PCI SSC pour connaître les responsabilités du client vis-à-vis du scan, la préparation du scan, etc.*	▪ Examiner les résultats des quatre dernières analyses de vulnérabilité	☐	☐	☐	☐
	(b) Les analyses trimestrielles et les renouvellements d'analyse respectent-ils les conditions du *guide de programme ASV* (par exemple, pas de vulnérabilité supérieure à la note 4.0 du CVSS et aucune défaillance automatique) ?	▪ Examiner les résultats de chaque analyse trimestrielle et de chaque renouvellement d'analyse	☐	☐	☐	☐
	(c) Les analyses trimestrielles de vulnérabilité externe sont-elles effectuées par un prestataire de services d'analyse agréé (ASV) par le PCI SSC ?	▪ Examiner les résultats de chaque analyse trimestrielle et de chaque renouvellement d'analyse	☐	☐	☐	☐

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	☐	☐	☐	☐
12.3.9	Activation des technologies d'accès à distance pour les fournisseurs et les partenaires commerciaux, uniquement lorsque cela est nécessaire, avec désactivation immédiate après usage ?	▪ Examiner les politiques d'utilisation ▪ Interroger le personnel responsable	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
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	☐	☐	☐	☐
12.5	(b) Les responsabilités suivantes de gestion de la sécurité des informations sont-elles 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 implémenté pour sensibiliser tous 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.	☐	☐	☐	☐

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 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	☐	☐	☐	☐
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-IP 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-IP 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	
1	Installer et gérer une configuration de pare-feu pour protéger les données du titulaire	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données du titulaire stockées	☐	☐	
4	Crypter la transmission des données du titulaire sur les réseaux publics ouverts	☐	☐	
6	Développer et maintenir des systèmes et des applications sécurisés	☐	☐	
7	Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître	☐	☐	
8	Identifier et authentifier l'accès à tous les composants du système	☐	☐	
9	Restreindre l'accès physique aux données du titulaire	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐