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

Questionnaire d'auto-évaluation C
et attestation de conformité

Commerçants possédant des systèmes d'application de paiement connectés à Internet –
Aucun stockage électronique de données du titulaire de carte

Destiné à une utilisation avec PCI DSS version 3.2.1

Juin 2018

Modifications apportées au document

Date	Version de PCI DSS	Révision SAQ	Description
Octobre 2008	1.2		Harmonisation du contenu avec la nouvelle procédure PCI DSS v1.2 et implémentation des changements mineurs notés depuis la v1.1 d'origine.
Octobre 2010	2.0		Harmonisation du contenu avec les conditions de la nouvelle norme PCI DSS v2.0 et des procédures de test.
Février 2014	3.0		Aligner le contenu avec les exigences et les procédures de test de PCI DSS v3.0, et incorporer des options de réponse supplémentaires.
Avril 2015	3.1		Mise à jour afin de s'harmoniser avec la norme PCI DSS v3.1. Pour plus de détails sur les modifications de PCI DSS, veuillez consulter *PCI DSS – Récapitulatif des changements entre les versions 3.0 et 3.1 de la norme PCI DSS*.
Juillet 2015	3.1	1.1	Mise à jour 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.* Conditions ajoutées de PCI DSS v3.2 Conditions 8, 9 et Annexe A2.
Janvier 2017	3.2	1.1	Modifications du document actualisées pour clarifier les conditions ajoutées dans la mise à jour d'avril 2016. Note ajoutée en bas de page de la section « Avant de Commencer » pour clarifier l'intention des systèmes autorisés. Cases à cocher rectifiées dans les Conditions 8.1.6 et 11.3.4.
Juin 2018	3.2.1	1.0	Mise à jour afin de s'harmoniser avec la norme PCI DSS v3.2.1. Pour plus de détails sur les modifications de PCI DSS, veuillez consulter *PCI DSS – Récapitulatif des changements entre les versions 3.2 et 3.2.1 de la norme PCI DSS.*

Remerciements

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

Table des matières

Avant de commencer

Le SAQ C a été élaboré pour satisfaire aux conditions applicables aux commerçants dont les systèmes d'application de paiement (par exemple, des systèmes points de vente) sont connectés à Internet (par exemple, par DSL, câble modem, etc.).

Les commerçants SAQ C traitent les données de titulaires de carte par des systèmes de point de vente (POS) ou d'autres systèmes d'application de paiement connectés à Internet, ne stockent pas de données de titulaires de carte sur des systèmes informatiques, et peuvent être des commerçants réels (carte présente), soit des commerçants de vente par courrier/téléphone (carte absente).

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

- Votre société possède un système d'application de paiement et une connexion Internet sur le même périphérique et/ou le même réseau local (LAN) ;
- Le système d'application de paiement/périphérique Internet n'est pas connecté à d'autres systèmes de votre environnement (cela peut être réalisé par une segmentation réseau en isolant le système d'application de paiement/périphérique Internet de tous les autres systèmes) [1];
- L'emplacement physique de l'environnement de POS n'est pas connecté aux autres locaux ou emplacements et tout LAN est uniquement destiné à un seul emplacement ;
- Toutes les données du titulaire de carte, que la société conserve sur papier (par exemple les rapports ou les reçus imprimés), et ces documents ne sont pas reçus par voie 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—consulter les *Instructions et directives relatives aux questionnaires d'auto-évaluation* sur le site Web de PCI SSC pour de plus amples informations.
2. Confirmez que les paramètres de votre environnement sont corrects et correspondent aux critères d'éligibilité pour le SAQ que vous utilisez (ainsi que le définit la partie 2g de l'attestation de conformité).
3. Évaluer la conformité de votre environnement aux conditions applicables de la norme PCI DSS.
4. Complétez toutes les sections de ce document :
    - Section 1 (Parties 1 & 2 de l'AOC) – Informations relatives à l'évaluation et résumé

[1] Ce critère n'est pas destiné à interdire à plus d'un type de système autorisé (à savoir, un système d'application de paiement) d'être sur la même zone de réseau, dans la mesure où les systèmes autorisés sont isolés des autres types de systèmes (par ex., en réalisant une segmentation réseau). De plus, ce critère n'est pas destiné à empêcher le type de système prévu de pouvoir transmettre les données d'une transaction à un tiers, comme un acquéreur ou un service de traitement de paiement, pour le traitement sur un réseau.

- Section 2 – Questionnaire d'auto-évaluation PCI DSS (SAQ C)
- Section 3 (Parties 3 & 4 de l'AOC) – Détails de validation et d'attestation, plan d'action pour les conditions de non-conformité (s'il y a lieu)

5. Envoyer le SAQ et l'attestation de conformité (AOC), ainsi que toute autre documentation requise, comme des rapports d'analyse ASV, à votre acquéreur, à la marque de paiement ou autre demandeur.

Comprendre le questionnaire d'auto-évaluation

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

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

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

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

Tests attendus

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

Remplir le questionnaire d’auto-évaluation

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

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

Réponse	Quand utiliser cette réponse :
Oui	Le test attendu a été effectué et tous les éléments de la condition ont été remplis ainsi qu’il est précisé.
Oui, avec CCW (Fiche de contrôle compensatoire)	Le test attendu a été

Réponse	Quand utiliser cette réponse :
	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,

Réponse	Quand utiliser cette réponse :
	remplir la fiche de contrôle compensatoire (CCW) dans l'annexe B du SAQ. Les informations concernant l'utilisation des contrôles compensatoires

Réponse	Quand utiliser cette réponse :
	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,

Réponse	Quand utiliser cette réponse :
	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

Réponse	Quand utiliser cette réponse :
	nt de l'organisation. (Voir ci-dessous les exemples de *directives de non-applicabilité de certaines conditions particulières spécifiques*). Toutes

Réponse	Quand utiliser cette réponse :
	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 C auront besoin de valider leur conformité à toutes les conditions PCI DSS de ce SAQ, certaines organisations ayant des modèles commerciaux très particuliers trouveront que certaines conditions ne sont pas applicables.

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). Noter que la condition 11.1 (utilisation de processus pour identifier les points d'accès sans fil non autorisés) doit être adressée même si vous n'utilisez pas de technologies sans fil dans votre réseau, puisque le processus détecte tout appareil escroc ou non autorisé susceptible d'avoir été ajouté sans que vous le sachiez.

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 votre acquéreur (la banque du commerçant) ou les marques de paiement pour déterminer les procédures de rapport et de demande.

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

Partie 1a. Informations sur le commerçant

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

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

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

Partie 2. Résumé

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

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

Quels types de réseaux de paiement votre entreprise sert-elle ?	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 2. Résumé *(suite)*

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

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

Partie 2c. Emplacements

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

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

Partie 2d. Applications de paiement

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

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

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

Partie 2e. Description de l'environnement

Donner une description ***détaillée*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions entrantes et sortantes à l'environnement de données de titulaires de carte (CDE).* • *Composants critiques du système dans le CDE, comme les appareils de POS, les bases de données, les*	

serveurs Web, etc., ainsi que les autres composants de paiement nécessaires, le cas échéant.	
Est-ce que votre entreprise utilise la segmentation de réseau pour affecter la portée de votre environnement PCI DSS ? *(Consulter la section « Segmentation réseau » de PCI DSS pour les recommandations concernant la segmentation réseau.)*	☐ Oui ☐ Non

Partie 2. Résumé *(suite)*

Partie 2f. Prestataires de services tiers

Est-ce que votre société a recours à un intégrateur et revendeur qualifié (QIR) ?	☐ Oui ☐ Non

Si oui :

Nom de la société QIR :	
Nom individuel QIR :	
Description des services fournis par QIR :	

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

Si oui :

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

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

Partie 2g. Admissibilité à participer au questionnaire SAQ C

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 a un système d'application de paiement et une connexion à Internet sur le même appareil et/ou le même réseau local (LAN) ;
☐	Le système d'application de paiement/périphérique Internet n'est relié à aucun autre système de l'environnement du commerçant ;
☐	L'emplacement physique de l'environnement de POS n'est pas connecté aux autres locaux ou emplacements et tout LAN est uniquement destiné à un seul emplacement ;

☐	Le commerçant ne stocke pas de données de titulaires de carte sous forme électronique ; **et**
☐	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.

Section 2 : Questionnaire d'auto-évaluation C

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

Date d'achèvement de l'auto-évaluation :

Créer et maintenir un réseau et des systèmes sécurisés

Condition 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.
1.2	Les configurations de pare-feu restreignent-elles les connexions entre les réseaux non approuvés et les composants du système dans l'environnement des données de 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 de titulaires de carte ?	▪ Examiner les standards de configuration du pare-feu et du routeur. ▪ Examiner les configurations du pare-feu et du 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 du pare-feu et du routeur. ▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
1.2.3	Les pare-feu de périmètre sont-ils installés entre tous les réseaux sans-fil et l'environnement des données de titulaires de carte, 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 des données de titulaires de carte ?	▪ Examiner les standards de configuration du pare-feu et du routeur. ▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐
1.3	L'accès public direct entre Internet et les composants du système dans l'environnement des données de titulaires de carte est-il interdit comme suit :					
1.3.4	Le trafic sortant de l'environnement des données de titulaires de carte vers Internet est-il explicitement autorisé ?	▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐
1.3.5	Est-ce que les connexions établies sont les seules autorisées sur le réseau ?	▪ Examiner les configurations du pare-feu et du 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 mais sans s'y limiter, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, les comptes d'application et de système, les terminaux de point de vente (POS), les applications de paiement, les chaînes de communauté de protocoles de gestion de réseau simple [SNMP], etc.).*	▪ Examiner les politiques et les procédures. ▪ Examiner la documentation du vendeur. ▪ Observer les configurations du système et les paramètres de compte. ▪ Interroger le personnel.	☐	☐	☐	☐
	(b) Les comptes par défaut inutiles sont-ils supprimés ou désactivés avant l'installation d'un système sur le réseau ?	▪ Examiner les politiques et les procédures. ▪ Examiner la documentation du vendeur. ▪ Examiner les configurations du système et les paramètres de compte. ▪ Interroger le personnel.	☐	☐	☐	☐
2.1.1	Pour les environnements sans fil connectés à l'environnement des données de 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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
2.1.1 *(suite)*	(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 du système.	☐	☐	☐	☐
	(c) Les mots de passe/locutions de passage 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 du 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 du 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 du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
2.2	(a) Des normes de configurations sont-elles conçues pour tous les composants du système et sont-elles cohérentes avec les normes renforçant les systèmes en vigueur dans le secteur ? *Les sources des normes renforçant les systèmes en vigueur dans le secteur peuvent comprendre, entre autres, l'Institut SANS (SysAdmin Audit Network Security), le NIST (National Institute of Standards Technology), l'ISO (International Organization for Standardization) et le CIS (Center for Internet Security).*	▪ Examiner les standards de configuration du système. ▪ Examiner les standards renforçant les serveurs acceptés par l'industrie. ▪ Examiner les politiques et les procédures. ▪ Interroger le personnel.	☐	☐	☐	☐
	(b) Les normes de configuration du système sont-elles mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités, comme indiqué dans la condition 6.1 ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel.	☐	☐	☐	☐
	(c) Les normes de configuration du système sont-elles appliquées lorsque de nouveaux systèmes sont configurés ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.2 *(suite)*	(d) Les standards de configuration du système comprennent-ils tous les points suivants : - Changement de tous les paramètres par défaut fournis par le fournisseur et élimination de tous les comptes par défaut inutiles ? - Application d'une fonction primaire unique par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents ? - Activation unique des services, protocoles, démons, etc. nécessaires pour le fonctionnement du système ? - Implémentation des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaires que l'on estime non sécurisés ? - Configuration des paramètres de sécurité du système pour empêcher les actes malveillants ? - Suppression de toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus ?	▪ Examiner les standards de configuration du système.	☐	☐	☐	☐
2.2.1	(a) Une seule fonction principale est-elle déployée par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents ? *Par exemple, les serveurs Web, les serveurs de bases de données et les serveurs DNS doivent être déployés sur des serveurs distincts.*	▪ Examiner les configurations du système.	☐	☐	☐	☐
	(b) Si des technologies de virtualisation sont utilisées, une seule fonction principale est-elle déployée par composant de système ou périphérique virtuels ?	▪ Examiner les configurations du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.2.2	(a) Seuls les services, protocoles, démons, etc. nécessaires sont-ils activés pour le fonctionnement du système (les services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction du périphérique sont désactivés) ?	▪ Examiner les standards de configuration. ▪ Examiner les configurations du système.	☐	☐	☐	☐
	(b) Les services, daemons ou protocoles actifs et non sécurisés sont-ils justifiés selon les normes de configuration documentées ?	▪ Examiner les standards de configuration ▪ Interroger le personnel. ▪ Examiner les paramètres de configuration. ▪ Comparer les services activés, etc. aux justifications documentées.	☐	☐	☐	☐
2.2.3	Les fonctions de sécurité supplémentaires sont-elles documentées et implémentées pour tout service, protocole ou démon nécessaires que l'on estime non sécurisés ?	▪ Examiner les standards de configuration. ▪ Examiner les paramètres de configuration.	☐	☐	☐	☐
2.2.4	(a) Les administrateurs système et/ou le personnel paramétrant les composants du système connaissent-ils la configuration des paramètres de sécurité courants pour ces composants du système ?	▪ Interroger le personnel.	☐	☐	☐	☐
	(b) La configuration des paramètres de sécurité courants est-elle comprise dans les normes de configuration du système ?	▪ Examiner les standards de configuration du système.	☐	☐	☐	☐
	(c) La configuration des paramètres de sécurité est-elle installée de manière appropriée sur les composants du système ?	▪ Examiner les composants de système. ▪ Examiner les paramètres de sécurité. ▪ Comparer les paramètres aux standards de configuration du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.2.5	(a) Toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus, ont-elles été supprimées ?	▪ Examiner les paramètres de sécurité sur les composants de système.	☐	☐	☐	☐
	(b) Les fonctions activées sont-elles détaillées et prennent-elles en charge une configuration sécurisée ?	▪ Examiner la documentation. ▪ Examiner les paramètres de sécurité sur les composants de système.	☐	☐	☐	☐
	(c) Seule la fonctionnalité documentée est-elle présente sur les composants de système ?	▪ Examiner la documentation. ▪ Examiner les paramètres de sécurité sur les composants de système.	☐	☐	☐	☐
2.3	L'accès administratif non-console est-il crypté de manière à :					
	(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 de système. ▪ Examiner les configurations du 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 de système. ▪ Examiner les services et les fichiers.	☐	☐	☐	☐
	(c) L'accès administrateur aux interfaces de gestion Web est-il crypté au moyen d'une méthode de cryptage robuste ?	▪ Examiner les composants de système. ▪ Observer un administrateur se connecter.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(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 de système. ▪ Examiner la documentation du vendeur. ▪ Interroger le personnel.	☐	☐	☐	☐
2.5	Les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres de vendeur par défaut et autres paramètres de sécurité sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐

Protection des données du titulaire de carte

Condition 3 : Protéger les données de titulaires de carte 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 du 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 appelées 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 carte,* • *Le numéro de compte primaire (PAN),* • *La date d'expiration et* • *Le code 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 plus que les six premiers/les quatre derniers chiffres du PAN ? ***Remarque :*** *Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données de titulaires de carte, —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 du système. ▪ Observer les affichages de PAN.	☐	☐	☐	☐

Condition 4 : Crypter la transmission des données de titulaires de carte 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 sont-ils déployés pour protéger les données de titulaires de carte sensibles lors de leur transmission sur des réseaux publics ouverts ? ***Remarque :*** *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 titulaires de carte sont transmises ou reçues. ▪ Examiner les configurations du système.	☐	☐	☐	☐
	(b) Seuls des clés et/ou certificats approuvés sont-ils acceptés ?	▪ Observer les transmissions entrantes et 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 du système.	☐	☐	☐	☐
	(d) Un niveau de cryptage approprié est-il mis en place pour la méthodologie de cryptage employée (se reporter aux recommandations/meilleures pratiques du fournisseur) ?	▪ Examiner la documentation du vendeur. ▪ Examiner les configurations du 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 TLS, le TLS est-il activé lorsque les données de titulaires de carte 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 de titulaires de carte sont uniquement requises lorsque la mention « HTTPS » apparaît dans l'adresse URL.*	▪ Examiner les configurations du système.	☐	☐	☐	☐
4.1.1	Les meilleures pratiques du secteur 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 de titulaires de carte ?	▪ 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 protégés 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 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
5.1	Des logiciels antivirus sont-ils déployés sur tous les systèmes régulièrement affectés par des logiciels malveillants ?	▪ Examiner les configurations du système.	☐	☐	☐	☐
5.1.1	Les programmes antivirus sont-ils capables de détecter, d'éliminer et de protéger de tous les types de logiciels malveillants connus (par exemple, virus, chevaux de Troie, vers, spyware, adware et dissimulateurs d'activités) ?	▪ Examiner la documentation du vendeur. ▪ Examiner les configurations du système.	☐	☐	☐	☐
5.1.2	Des évaluations régulières ont-elles lieu pour identifier et évaluer l'évolution de la menace posée par les logiciels malveillants afin de confirmer que ces systèmes continuent d'opérer sans être affectés par ces logiciels malveillants ?	▪ Interroger le personnel.	☐	☐	☐	☐
5.2	Les mécanismes anti-virus sont-ils maintenus comme suit :					
	(a) Le logiciel anti-virus et les définitions sont-ils à jour ?	▪ Examiner les politiques et les procédures. ▪ Examiner les configurations antivirus, y compris l'installation du logiciel maître. ▪ Examiner les composants de système.	☐	☐	☐	☐
	(b) Les mises à jour et les analyses périodiques automatiques sont-elles activées et effectuées ?	▪ Examiner les configurations antivirus, y compris l'installation du logiciel maître. ▪ Examiner les composants de système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(c) Tous les mécanismes anti-virus génèrent-ils des journaux d'audit et les journaux sont-ils conservés conformément à la condition 10.7 de la norme PCI DSS ?	▪ Examiner les configurations antivirus. ▪ Examiner les processus de conservation des journaux.	☐	☐	☐	☐
5.3	Les mécanismes anti-virus sont-ils tous : ▪ En fonctionnement actif ? ▪ Incapables d'être désactivés ou altérés par les utilisateurs ? ***Remarque :*** *Les solutions anti-virus peuvent être désactivées temporairement uniquement s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la protection anti-virus doit être désactivée dans un but spécifique, cette désactivation doit donner lieu à une autorisation formelle. Des mesures de sécurité supplémentaires doivent également être mises en œuvre pour la période de temps pendant laquelle la protection anti-virus n'est pas active.*	▪ Examiner les configurations antivirus. ▪ Examiner les composants de système. ▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
6.1	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 de titulaires de carte.*	▪ 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 de système. ▪ Comparer la liste des correctifs de sécurité installés aux listes de correctifs récents fournis par les vendeurs.	☐	☐	☐	☐
6.4.6	Suite à un changement important, est-ce-que toutes les conditions pertinentes PCI DSS sont implémentées sur tous les systèmes et réseaux, qu'ils soient nouveaux ou modifiés, et la documentation est-elle mise à jour, le cas échéant ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement. ▪ Interroger le personnel. ▪ Observer les systèmes ou les réseaux concernés.	☐	☐	☐	☐

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données de titulaires de carte 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 de 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 ?	▪ Interroger le personnel. ▪ Gestion des entretiens. ▪ Examiner les ID des utilisateurs privilégiés.	☐	☐	☐	☐
7.1.3	L'accès est-il attribué en fonction de la classification et de la fonction professionnelles de chaque membre du personnel ?	▪ Gestion des entretiens. ▪ Examiner les ID 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	Des politiques et des procédures pour les contrôles de gestion d'identification des utilisateurs sont définies et mises en place pour les utilisateurs non consommateurs et les administrateurs sur tous les composants du système comme suit :					
8.1.1	Tous les utilisateurs se voient-ils assigner un ID unique avant d'être autorisés à accéder aux composants du système ou aux données de titulaires de carte ?	▪ Examiner les procédures de mots de passe. ▪ Interroger le personnel.	☐	☐	☐	☐
8.1.5	(a) Les comptes utilisés par les tierces parties pour l'accès, le soutien ou la maintenance des composants du système par accès à distance sont-ils activés uniquement pendant la période nécessaire et désactivés lorsqu'ils ne sont pas utilisés ?	▪ Examiner les procédures de mots de passe. ▪ Interroger le personnel. ▪ Observer les processus.	☐	☐	☐	☐
	(b) Les comptes d'accès à distance tiers sont-ils contrôlés lorsqu'ils sont utilisés ?	▪ Interroger le personnel. ▪ Observer les processus.	☐	☐	☐	☐
8.1.6	(a) Les tentatives d'accès répétées sont-elles restreintes en verrouillant l'ID utilisateur après six tentatives au maximum ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐
8.1.7	Une fois un compte utilisateur verrouillé, la durée de verrouillage est-elle réglée à un minimum de 30 minutes ou jusqu'à ce que l'administrateur active l'ID utilisateur ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐
8.1.8	Si une session reste inactive plus de 15 minutes, est-il demandé à l'utilisateur de se réauthentifier (par exemple, en saisissant de nouveau son mot de passe) pour réactiver le terminal ou la session ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.2	Outre l'assignation d'un ID unique, l'une ou plusieurs des méthodes suivantes sont-elles employées pour authentifier tous les utilisateurs ? ▪ Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; ▪ Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; ▪ Quelque chose concernant l'utilisateur, comme une mesure biométrique.	▪ Examiner les procédures de mots de passe. ▪ Observer les processus d'authentification.	☐	☐	☐	☐
8.2.3	(a) Les paramètres de mot de passe utilisateur sont-ils configurés de sorte que les mots/phrases de passe respectent les points suivants ? - Des mots de passe d'une longueur d'au moins sept caractères - Contenant à la fois des caractères numériques et des caractères alphabétiques Autrement, les mots de passe/locutions de passage doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.	▪ Examiner les paramètres de configuration du système pour vérifier les paramètres des mots de passe.	☐	☐	☐	☐
8.2.4	Les mots de passe/locutions de passage des utilisateurs sont-ils changés au moins tous les 90 jours ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐
8.2.5	Un individu doit-il soumettre un nouveau mot de passe/une nouvelle locution de passage différent(e) des quatre derniers/dernières mots de passe/locutions de passage qu'il a utilisé(e)s ?	▪ Examiner les procédures de mots de passe. ▪ Essayer les composants de système. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.2.6	Les mots de passe/locutions de passage sont-ils définis sur une valeur unique pour chaque utilisateur à la première utilisation et suite à une réinitialisation, et chaque utilisateur doit-il modifier son mot de passe immédiatement après la première utilisation ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les paramètres de configuration du système. ▪ Observer le personnel de sécurité.	☐	☐	☐	☐
8.3	Est-ce que tous les accès administratifs non-console et tous les accès distants à CDE sont sécurisés par authentification à plusieurs facteurs, comme suit : ***Remarque :*** *L'authentification à plusieurs facteurs requiert d'utiliser au moins deux des trois méthodes d'authentification (voir la condition 8.2 de la norme PCI DSS pour les descriptions 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 plusieurs facteurs.*					
8.3.1	Est-ce que l'authentification à plusieurs facteurs est incorporée pour tous les accès non-console dans CDE pour les membres du personnel dotés d'un accès administratif ?	▪ Examiner les configurations du système. ▪ Observer la connexion de l'administrateur au CDE.	☐	☐	☐	☐
8.3.2	Une authentification à plusieurs facteurs est-elle incorporée pour tous les accès réseau à distance (utilisateur et administrateur, y compris l'accès tiers dans un souci d'assistance et de maintenance) du personnel issu de l'extérieur du réseau de l'entité ?	▪ Examiner les configurations du système. ▪ Observer la connexion du personnel à distance.	☐	☐	☐	☐
8.4	(a) Les politiques et les procédures d'authentification sont-elles documentées et communiquées à tous les utilisateurs ?	▪ Examiner les politiques et les procédures. ▪ Observer la méthode de distribution. ▪ Interroger le personnel. ▪ Interroger les utilisateurs.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(b) Les politiques et les procédures d'authentification comprennent-elles les points suivants ? - Des directives concernant la sélection de justificatifs d'authentification robustes ; - Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ; - Des instructions stipulant qu'il ne faut pas réutiliser les mots de passe ayant déjà été utilisés ; - Des instructions expliquant que les utilisateurs doivent changer de mot de passe s'ils soupçonnent que le mot de passe est compromis.	▪ Examiner les politiques et les procédures. ▪ Examiner la documentation fournie aux utilisateurs.	☐	☐	☐	☐
8.5	Les comptes et mots de passe ou autres méthodes d'authentification de groupe, partagée ou générique sont-ils interdits comme suit : ▪ Les ID d'utilisateur et les comptes génériques sont désactivés ou supprimés ; ▪ Il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ; ▪ Les ID d'utilisateur partagés ou génériques ne sont pas utilisés pour l'administration du moindre composant du système ?	▪ Examiner les politiques et les procédures. ▪ Examiner les listes d'ID utilisateur. ▪ Interroger le personnel.	☐	☐	☐	☐
8.8	Les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
9.1	Des contrôles d'accès aux installations appropriés sont-ils en place pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de carte ?	▪ Observer les contrôles d'accès physiques. ▪ Observer le personnel.	☐	☐	☐	☐
9.1.1	(a) Des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès (ou les deux) sont-ils utilisés pour contrôler l'accès physique des individus aux zones sensibles ? ***Remarque :*** *Par « Zones sensibles », nous entendons tout centre de données, salle de serveur ou zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaires de carte. Cette définition exclut les zones face au public où seuls les terminaux de point de vente sont présents, comme les zones de caisse dans un magasin.*	▪ Examiner les politiques et les procédures. ▪ Observer les mécanismes de contrôle physique. ▪ Observer les fonctions de sécurité.	☐	☐	☐	☐
	(b) Les caméras vidéo et/ou autres mécanismes de contrôle d'accès (ou les deux) sont-ils protégés contre la falsification ou la désactivation ?	▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐
	(c) Des données recueillies à partir des caméras vidéo et/ou mécanismes de contrôle d'accès sont-elles examinées et corrélées avec les autres entrées ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel de la sécurité.	☐	☐	☐	☐
	(d) Des données sont-elles recueillies à partir des caméras vidéo et/ou de mécanismes de contrôle d'accès stockés pour au moins trois mois, sauf disposition contraire de la loi ?	▪ Examiner les processus de conservation des données. ▪ Observer le stockage de données. ▪ Interroger le personnel de la sécurité.	☐	☐	☐	☐

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.	☐	☐	☐	☐
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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
9.6.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?	▪ Interroger le personnel. ▪ Examiner les journaux de suivi et la documentation relatifs à la distribution des supports.	☐	☐	☐	☐
9.6.3	L'approbation de la direction est-elle obtenue avant le déplacement des supports (particulièrement lorsque le support est distribué aux individus) ?	▪ Interroger le personnel. ▪ Examiner les journaux de suivi et la documentation relatifs à la distribution des supports.	☐	☐	☐	☐
9.7	Un contrôle strict est-il réalisé sur le stockage et l'accessibilité des supports ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐
9.8	(a) Tous les supports sont-ils détruits lorsqu'ils ne sont plus utiles pour des raisons professionnelles ou légales ?	▪ Examiner les politiques et procédures de destruction régulière des supports.	☐	☐	☐	☐
	(c) La destruction des supports est-elle réalisée comme suit :					
9.8.1	(a) Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de sorte que les données de titulaires de carte ne puissent pas être reconstituées ?	▪ Examiner les politiques et procédures de destruction régulière 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.	☐	☐	☐	☐

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(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 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 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
10.2	Des journaux d'audit automatisés sont-ils en place pour tous les composants du système afin de reconstituer les événements suivants :					
10.2.2	Toutes les actions exécutées par des utilisateurs ayant des droits root ou administrateur ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.2.4	Les tentatives d'accès logique non valides ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.2.5	L'utilisation et la modification des mécanismes d'identification et d'authentification,—y compris notamment la création de nouveaux comptes et l'élévation de privilèges,—et toutes les modifications, additions ou suppressions aux comptes avec privilèges racines ou administratifs ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.3	Les journaux d'audit comprennent-ils au moins les entrées suivantes pour chaque événement :					
10.3.1	Identification des utilisateurs ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.3.2	Type d'événement ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
10.3.3	Date et heure ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.3.4	Indication de succès ou d'échec ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.3.5	Origine de l'événement ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.3.6	Identité ou nom des données, du composant du système ou de la ressource affectés ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐
10.6	Les journaux et les événements de sécurité de tous les composants du système sont-ils analysés pour identifier les anomalies ou les activités suspectes comme suit ? ***Remarque :*** *Les outils de journalisation, d'analyse et d'alerte peuvent être utilisés conformément à la condition 10.6.*					

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
10.6.1	(a) Les journaux et événements de sécurité suivants sont-ils examinés au moins une fois par jour, manuellement ou à l'aide d'outils de journalisation ? - Tous les événements de sécurité - Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD - Les journaux de tous les composants critiques du système - Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.)	▪ Examiner les politiques de sécurité et les procédures.	☐	☐	☐	☐
10.6.2	(b) Les journaux de tous les autres composants de système sont-ils examinés régulièrement - soit manuellement, soit à l'aide d'outils de journalisation, sur la base des politiques et de la stratégie de gestion des risques de l'organisation ?	▪ Examiner la documentation d'évaluation des risques. ▪ Interroger le personnel.	☐	☐	☐	☐
10.6.3	(b) Le suivi des exceptions et des anomalies est-il effectué ?	▪ Examiner les politiques de sécurité et les procédures ▪ Observer les processus ▪ Interroger le personnel	☐	☐	☐	☐
10.7	(b) Les journaux d'audit sont-ils conservés pendant au moins un an ?	▪ Interroger le personnel. ▪ Examiner les journaux d'audit.	☐	☐	☐	☐
	(c) Les trois derniers mois de journaux au moins sont-ils disponibles pour analyse ?	▪ Interroger le personnel. ▪ Observer les processus.	☐	☐	☐	☐

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.**
11.1	(a) Les processus sont-ils définis pour la détection et l'identification des points d'accès sans-fil autorisés et non autorisés sur une base trimestrielle ? ***Remarque :*** *Les analyses de réseau sans-fil, les inspections logiques/physiques des composants du système et de l'infrastructure, le contrôle d'accès réseau (NAC) ou les systèmes de détection et/ou de prévention d'intrusions sans-fil sont quelques exemples de méthodes pouvant être utilisées pour ce processus.* *Quelle que soit la méthode utilisée, elle doit être suffisante pour détecter et identifier tous les périphériques non autorisés.*	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐
	(b) La méthodologie détecte-t-elle et identifie-t-elle les points d'accès sans fil non autorisés, notamment au moins ce qui suit ? - Des cartes WLAN insérées dans les composants du système ; - Des appareils portables ou mobiles reliés à un composant du système pour créer un point d'accès sans-fil (par exemple, par USB, etc.) ; et - Des périphériques sans-fil branchés sur un port réseau ou à un périphérique réseau.	▪ Évaluer la méthodologie.	☐	☐	☐	☐
	(c) Si l'analyse sans fil est utilisée pour identifier des points d'accès sans fil autorisés et non autorisés, est-elle exécutée au moins chaque trimestre pour tous les composants de système et toutes les installations ?	▪ Examiner le résultat des dernières analyses du réseau sans fil.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(d) En cas d'utilisation d'une surveillance automatisée (par exemple systèmes de détection et/ou de prévention d'intrusions sans fil, NAC, etc.), la surveillance est-elle configurée pour déclencher des alertes pour notifier le personnel ?	▪ Examiner les paramètres de configuration.	☐	☐	☐	☐
11.1.1	Un inventaire des points d'accès sans fil est-il tenu et la justification commerciale est-elle documentée pour tous les points d'accès sans-fil autorisés ?	▪ Examiner les registres d'inventaire.	☐	☐	☐	☐
11.1.2	(a) Le plan de réponse aux incidents définit-il et demande-t-il une réponse au cas où un point d'accès sans-fil non autorisé est détecté ?	▪ Examiner le plan de réponse aux incidents (voir la condition 12.10).	☐	☐	☐	☐
	(b) Des mesures sont-elles prises lorsque des points d'accès non autorisés sont identifiés ?	▪ Interroger le personnel responsable. ▪ Inspecter les dernières analyses du réseau sans fil et les réponses en rapport.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
11.2	Des analyses des vulnérabilités potentielles des réseaux internes et externes sont-elles réalisées au moins une fois par trimestre et après un changement significatif du réseau (par exemple, l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits), comme suit : ***Remarque :*** *De multiples rapports de scan peuvent être combinés pour que le processus de scan trimestriel montre que tous les systèmes ont été scannés et que toutes les vulnérabilités applicables ont été traitées. Une documentation supplémentaire peut être requise pour vérifier que les vulnérabilités qui n'ont pas été résolues sont en phase de l'être.* *Pour la conformité initiale à la norme PCI DSS, il n'est pas obligatoire que quatre scans trimestriels aient été réalisés avec succès si l'évaluateur vérifie que 1) le résultat du dernier scan était réussi, 2) l'entité a documenté les politiques et les procédures exigeant l'exécution de scans trimestriels et 3) toutes les vulnérabilités relevées dans les résultats ont été corrigées, comme indiqué lors de la réexécution du scan. Pour les années qui suivent la vérification PCI DSS initiale, quatre scans trimestriels réussis ont été réalisés.*					

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
11.2.1	(a) Des analyses trimestrielles de vulnérabilité interne sont-elles réalisées ?	▪ Examiner les rapports d'analyse.	☐	☐	☐	☐
	(b) Le processus d'analyse interne trimestriel gère-t-il les vulnérabilités à « haut risque » et inclut-il les renouvellements d'analyse pour vérifier que toutes les vulnérabilités à « haut risque » (comme défini dans la condition 6.1 de la norme PCI DSS) sont résolues ?	▪ Examiner les rapports d'analyse.	☐	☐	☐	☐
	(c) Les analyses internes trimestrielles sont-elles effectuées par une ou plusieurs ressources internes ou un tiers externe qualifié et, le cas échéant, le testeur appartient-il à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV) ?	▪ Interroger le personnel.	☐	☐	☐	☐
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 trimestrielles de vulnérabilité externe.	☐	☐	☐	☐
	(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 externe 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 externe et de chaque renouvellement d'analyse.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
11.2.3	(a) Les analyses internes et externes, ainsi que les renouvellements d'analyse, sont-elles effectuées après tout changement d'importance ? ***Remarque :*** *Les analyses doivent être exécutées par un personnel qualifié.*	▪ Examiner et faire correspondre la documentation du contrôle de changement et les rapports d'analyse.	☐	☐	☐	☐
	(b) Le processus d'analyse comprend-il de nouvelles analyses jusqu'à ce que : - Pour les analyses externes, aucune vulnérabilité supérieure à la note 4.0 du CVSS n'existe, - Pour les analyses internes, un résultat satisfaisant est obtenu ou toutes les vulnérabilités à « haut risque », définies dans la condition 6.1 de la norme PCI DSS, soient résolues ?	▪ Examiner les rapports d'analyse.	☐	☐	☐	☐
	(c) Les analyses sont-elles effectuées par une ou plusieurs ressources internes ou un tiers externe qualifié et, le cas échéant, le testeur appartient-il à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV) ?	▪ Interroger le personnel.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
11.3.4	Si la segmentation est utilisée pour isoler le CDE des autres réseaux :					
	(a) Les procédures de test de pénétration sont-elles définies pour tester toutes les méthodes de segmentation afin de confirmer qu'elles sont opérationnelles et efficaces, et isoler les systèmes hors de portée des systèmes dans CDE ?	▪ Examiner les contrôles de segmentation. ▪ Examiner la méthodologie des tests de pénétration.	☐	☐	☐	☐
	(b) Est-ce que les tests d'intrusion vérifient que les contrôles de segmentation répondent aux critères suivants ? - Effectués au moins une fois par an et après toute modification aux méthodes/contrôles de segmentation. - Couvre toutes les méthodes/contrôles de segmentation utilisées. - Vérifient que les méthodes de segmentation sont opérationnelles et efficaces, et isolent les systèmes hors de portée des systèmes dans CDE.	▪ Examiner les résultats du dernier test de pénétration.	☐	☐	☐	☐
	(c) Les tests ont-ils été effectués par une ressource interne ou un tiers externe qualifié et, le cas échéant, le testeur appartient-il à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV) ?	▪ Interroger le personnel responsable.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
11.5	(a) Un mécanisme de détection de changement (par exemple, des outils de contrôle de l'intégrité des fichiers) est-il déployé pour détecter toute modification non autorisée (y compris des changements, des ajouts et des suppressions) des fichiers critiques du système, des fichiers de configuration ou des fichiers de contenu ? *Exemples de fichiers devant être contrôlés :* • *Exécutables du système* • *Exécutables des applications* • *Fichiers de configuration et de paramètres* • *Fichiers d'historique, d'archive, de registres et d'audit stockés à un emplacement centralisé* • *Les fichiers critiques supplémentaires déterminés par l'entité (par exemple, avec l'évaluation de risque ou par d'autres moyens)*	▪ Observer les configurations du système et les fichiers contrôlés. ▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(b) Le mécanisme de détection des modifications est-il configuré pour alerter le personnel de toute modification non autorisée (y compris des changements, des ajouts et des suppressions) des fichiers critiques du système, des fichiers de configuration ou des fichiers de contenu, et les outils effectuent-ils des comparaisons entre les fichiers critiques au moins une fois par semaine ? ***Remarque :*** *Pour la détection des changements, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les mécanismes de détection des changements tels que les produits de surveillance d'intégrité de fichier sont généralement préconfigurés avec les fichiers critiques pour le système d'exploitation connexe. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).*	▪ Observer les configurations du système et les fichiers contrôlés. ▪ Examiner les résultats des activités de contrôle.	☐	☐	☐	☐
11.5.1	Un processus est-il en place pour répondre aux alertes générées par la solution de détection de modifications ?	▪ Examiner les paramètres de configuration du système.	☐	☐	☐	☐

Gestion d'une politique de sécurité des informations

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

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.1	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.	☐	☐	☐	☐
12.3.2	Authentification de l'utilisation 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.	☐	☐	☐	☐
12.3.6	Emplacements acceptables des technologies sur le réseau ?	▪ 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.
12.3.8	Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique ?	▪ 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.	☐	☐	☐	☐
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 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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.8	Des politiques et des procédures sont-elles maintenues et mises en œuvre pour gérer les prestataires de service avec lesquels les données de titulaires de carte sont partagées, ou qui sont susceptibles d'affecter la sécurité des données de titulaires de carte, comme suit :					
12.8.1	Est-ce qu'une liste des prestataires de services est conservée, y compris une description du ou des services fournis ?	▪ Examiner les politiques et les procédures. ▪ Observer les processus. ▪ Examiner la liste des prestataires de services.	☐	☐	☐	☐
12.8.2	Un accord écrit est-il passé par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte ? ***Remarque :*** *La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.*	▪ Respecter les accords écrits. ▪ Examiner les politiques et les procédures.	☐	☐	☐	☐
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.	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.8.5	Les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation sont-elles maintenues ?	▪ Observer les processus. ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative.	☐	☐	☐	☐
12.10.1	(a) Un plan de réponse aux incidents a-t-il été créé pour être implémenté en cas d'intrusion dans le système ?	▪ Examiner le plan de réponse aux incidents. ▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	(b) Le plan tient-il compte, au minimum des points suivants :					
	- Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Procédures de réponse aux incidents spécifiques ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Procédures de continuité et de reprise des affaires ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Processus de sauvegarde des données ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Analyse des conditions légales en matière de signalement des incidents ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Couverture et réponses de tous les composants stratégiques du système ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐
	- Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement ?	▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐

Annexe A : Autres conditions de la norme PCI DSS

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

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

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
A2.1	*Pour les terminaux POS POI (**chez un commerçant ou sur le lieu de validation du paiement**) utilisant un protocole SSL et/ou TLS initial :* A-t-il été confirmé que les appareils ne présentent pas de failles connues pour le SSL/TLS initial ? ***Remarque :** Cette condition est censée s'appliquer à l'entité équipée d'un terminal POS POI, tel qu'un commerçant. Cette condition ne s'applique pas aux prestataires de services qui font office de point terminal ou de connexion à ces terminaux POS POI. Les conditions A2.2 et A2.3 s'appliquent aux prestataires de services équipés de connexions POS POI.*	▪ Revoir la documentation (par exemple, la documentation fournisseur, les détails de configuration du système/réseau, etc.) et vérifier que les appareils POS POI ne sont pas susceptibles d'attaques connues pour le SSL et le TLS initial.	☐	☐	☐	☐

Annexe A3 : Validation complémentaire des entités désignées (DESV)

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

Annexe B : Fiche de contrôles compensatoires

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

***Remarque :** Seules les entreprises qui ont procédé à une analyse des risques et ont des contraintes commerciales documentées ou des contraintes technologiques légitimes peuvent envisager l'utilisation de contrôles compensatoires pour se mettre en conformité.*

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

Numéro et définition des clauses :

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité à la condition initiale.	
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence de contrôle initial.	
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	

Annexe C : Explication de non-applicabilité

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

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

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

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

En se basant sur les résultats documentés dans le SAQ C noté ci-dessus, les signataires identifiés dans les parties 3b-3d, le cas échéant, confirment le statut de conformité suivant pour l'entité identifiée dans la partie 2 de ce document (***cocher 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 PCI DSS C, version *(n° de version du SAQ)*, a été complété conformément aux instructions fournies.
☐	Toutes les informations présentes dans le SAQ susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de mon évaluation à tous points de vue.
☐	J'ai vérifié auprès de mon fournisseur d'application de paiement que mon système de paiement ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme, ainsi qu'elle s'applique à mon environnement, à tout moment.
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.

Partie 3. Validation PCI DSS *(suite)*

Partie 3a. Reconnaissance du statut *(suite)*

☐	Aucune preuve de stockage de données de bande magnétique[2], de données CAV2, CVC2, CID ou CVV2[3], ou de données de code PIN[4]après transaction n'a été trouvée sur AUCUN système examiné pendant cette évaluation.
☐	Les analyses ASV sont effectuées par le fournisseur d'analyse approuvé par le PCI SSC *(Nom de l'ASV).*

Partie 3b. Attestation de commerçant

Signature du représentant du commerçant ↗	*Date :*
Nom du représentant du commerçant :	*Poste occupé :*

Partie 3c. Reconnaissance de l'évaluateur de sécurité qualifié (QSA) (le cas échéant)

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

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

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

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

[2] 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.

[3] 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.

[4] 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 des titulaires de cartes.	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.	☐	☐	
3	Protéger les données des titulaires de cartes stockées.	☐	☐	
4	Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.	☐	☐	
5	Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes antivirus.	☐	☐	
6	Développer et gérer des systèmes et des applications sécurisés.	☐	☐	
7	Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître.	☐	☐	
8	Identifier et authentifier l'accès à tous les composants de système.	☐	☐	
9	Restreindre l'accès physique aux données des titulaires de cartes..	☐	☐	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes.	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité.	☐	☐	
12	Maintenir une politique qui adresse les informations de sécurité pour l'ensemble du personnel.	☐	☐	

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

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