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

Questionnaire d’auto-évaluation D
et attestation de conformité pour les commerçants

Tous les autres commerçants qualifiés SAQ

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 et l'option de rapport de la norme PCI DSS v2 pour la condition 11.3.
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.*
Janvier 2017	3.2	1.1	Mise à jour de la numérotation des versions afin de s'harmoniser avec d'autres SAQ
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 D pour commerçants s'applique aux commerçants qualifiés SAQ ne satisfaisant pas aux critères des types de SAQ. Les exemples d'environnement de commerçants qui pourraient utiliser le SAQ D pourraient inclure, entre autres :

- Les commerçants du commerce électronique qui acceptent les données du titulaire de carte sur leur site Web
- Les commerçants qui stockent les données de titulaires de carte sous forme électronique
- Les commerçants qui ne stockent pas de données de titulaires de carte sous forme électronique, mais qui ne répondent pas aux critères d'un autre type de SAQ
- Les commerçants dont les environnements répondent aux critères d'un autre type de SAQ, mais pour l'environnement desquels des conditions PCI DSS supplémentaires sont applicables

Alors que de nombreuses organisations complétant un SAQ D auront besoin de valider leur conformité à toutes les conditions PCI DSS, certaines ayant des modèles commerciaux très particuliers ne seront pas concernées par certaines conditions. Voir la directive ci-dessous pour de plus amples informations concernant l'exclusion de certaines conditions spécifiques.

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

(a) 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.

(b) Confirmez que la portée de votre environnement est correcte et correspond aux critères d'éligibilité pour le SAQ que vous utilisez.

(c) Évaluer la conformité de votre environnement aux conditions de la norme PCI DSS.

(d) Complétez toutes les sections de ce document :

- Section 1 (Parties 1 & 2 de l'AOC) – Informations relatives à l'évaluation et résumé
- Section 2 – Questionnaire d'auto-évaluation PCI DSS (SAQ D)
- 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)

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

Comprendre le questionnaire d'auto-évaluation

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

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

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

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

Tests attendus

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

Remplir le questionnaire d'auto-évaluation

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

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

Réponse	Quand utiliser cette réponse :
Oui	Le test attendu a été effectué et tous les éléments de la condition ont été remplis ainsi qu'il est précisé.
Oui, avec CCW (Fiche de contrôle compensatoire)	Le test attendu a été effectué et tous les éléments de la condition ont été remplis avec l'aide d'un contrôle compensatoire. Pour toutes les réponses de cette colonne, remplir la fiche de contrôle compensatoire (CCW) dans l'annexe B du SAQ. Les informations concernant l'utilisation des contrôles compensatoires et les conseils pour aider à remplir la fiche se trouvent dans le PCI DSS.

Réponse	Quand utiliser cette réponse :
Non	Certains, ou la totalité, des éléments de la condition n'ont pas été remplis, sont en cours de mise en œuvre, ou nécessitent d'autres tests avant de savoir s'ils sont en place.
S.O. (Sans objet)	La condition ne s'applique pas à l'environnement de l'organisation. (Voir ci-dessous les exemples de *directives de non-applicabilité de certaines conditions particulières spécifiques*). Toutes les réponses de cette colonne nécessitent une explication justificative dans l'Annexe C du SAQ.
Non testé	La condition n'a pas été prise en considération dans l'évaluation et n'a été testée d'aucune manière. (Voir ci-dessous *Comprendre les différences entre Non applicable et Non testé* pour des exemples de circonstances où cette option doit être utilisée.) Toutes les réponses de cette colonne nécessitent une explication justificative dans l'Annexe D du SAQ.

Directives de non-applicabilité de certaines conditions particulières

Alors que de nombreuses organisations complétant un SAQ D auront besoin de valider leur conformité à toutes les conditions PCI DSS, certaines ayant des modèles commerciaux très particuliers ne seront pas concernées par certaines conditions. Par exemple, une société qui n'utilise en aucun cas la technologie sans fil n'est pas contrainte de se conformer aux rubriques de la norme PCI DSS spécifiques à la gestion de la technologie sans fil. De même, une organisation qui à aucun moment ne stocke électroniquement de données de titulaires de carte n'a pas besoin de valider les conditions liées au stockage sécurisé des données de titulaires de carte (par exemple, la condition 3.4).

Les exemples de conditions ayant une applicabilité spécifique comprennent :

- Les questions spécifiques aux technologies sans fil (par exemple, les conditions 1.2.3, 2.1.1 et 4.1.1) doivent uniquement être adressées si un réseau sans fil est présent dans votre réseau. 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.
- Les questions spécifiques au développement d'application et au codage sécurisé (conditions 6.3 et 6.5) doivent uniquement être adressées si l'organisation conçoit ses propres applications personnalisées.
- Les questions concernant les conditions 9.1.1 et 9.3 doivent uniquement être adressées pour les uniquement pour les installations possédant des « zones sensibles », ainsi qu'elles sont définies ici : 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. Cela exclut les zones où seuls des terminaux point de vente sont présents, comme les zones de caisse dans un magasin de vente au détail, mais comprennent les salles de serveurs administratifs d'un tel magasin qui stocke des données de titulaires de carte et possède des zones de stockage pour de grandes quantités de données de titulaires de carte.

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. ».

Comprendre la différence entre Non applicable et Non testé

Les conditions qui sont considérées comme n'étant pas applicables à un environnement spécifique doivent être vérifiées comme telles. En utilisant l'exemple de réseau sans fil ci-dessus, pour qu'une organisation sélectionne « S.O. » pour les conditions 1.2.3, 2.1.1 et 4.1.1, l'organisation doit d'abord confirmer qu'aucune technologie sans fil n'est utilisée dans son CDE (environnement des données du titulaire de cartes) ou ne se connecte à celui-ci. Une fois que ce point est confirmé, l'organisation peut sélectionner « S.O. » pour ces conditions spécifiques,

Si un environnement est entièrement exclu de l'examen sans considérer s'il *pourrait* s'appliquer, l'option « Non testé » devrait être sélectionnée. Les exemples de situations où cela peut se produire peuvent inclure :

- Un acquéreur peut demander à une organisation de valider un sous-ensemble de conditions - par exemple : en utilisant l'approche prioritaire pour valider certaines étapes importantes.
- Une organisation peut souhaiter valider un nouveau contrôle de sécurité qui a uniquement un impact sur un sous-ensemble de conditions - par exemple, implémentation d'une nouvelle méthodologie de cryptage qui requiert l'évaluation des conditions PCI DSS 2, 3 et 4.
- L'organisation d'un prestataire de servie peut offrir un service qui ne recouvre qu'un nombre limité de conditions PCI DSS - par exemple, un fournisseur de stockage physique peut souhaiter valider uniquement les contrôles de sécurité physiques selon la condition PCI DSS 9 pour son installation de stockage.

Dans ces scénarios, l'organisation souhaite uniquement valider certaines conditions PCI DSS, bien que d'autres conditions puissent également s'appliquer à son environnement.

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 2f. Prestataires de services tiers	
	☐ 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.*

Section 2 : Questionnaire d'auto-évaluation D pour les commerçants

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.	Non testé
1.1	Les standards de configurations de pare-feu et de routeurs sont-ils établis pour inclure les points suivants :						
1.1.1	Un processus formel existe-t-il pour l'approbation et le test de toutes les connexions réseau et des changements apportés aux configurations de pare-feu et de routeur ?	▪ Examiner le processus documenté. ▪ Interroger le personnel. ▪ Examiner les configurations de réseau.	☐	☐	☐	☐	☐
1.1.2	(a) Existe-t-il un schéma du réseau actualisé qui comprend toutes les connexions entre l'environnement des données de titulaires de carte et les autres réseaux, y compris les réseaux sans fil ?	▪ Examiner le schéma du réseau actualisé. ▪ Examiner les configurations de réseau.	☐	☐	☐	☐	☐
	(b) Existe-t-il un processus pour garantir que le schéma est tenu à jour ?	▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
1.1.3	(a) Existe-t-il un schéma actualisé montrant le flux des données de titulaires de carte dans les systèmes et les réseaux ?	▪ Examiner le schéma actualisé des flux de données. ▪ Examiner les configurations de réseau.	☐	☐	☐	☐	☐
	(b) Existe-t-il un processus pour garantir que le schéma est tenu à jour ?	▪ Interroger le personnel.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
1.1.4	(a) Un pare-feu est-il requis et implémenté au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne ?	▪ Examiner les standards de configuration de pare-feu. ▪ Observer les configurations de réseau pour vérifier qu'un ou plusieurs pare-feux sont en place.	☐	☐	☐	☐	☐
	(b) Le schéma de réseau actuel est-il conforme aux normes de configuration des pare-feu ?	▪ Comparer les standards de configuration du pare-feu au schéma actualisé du réseau.	☐	☐	☐	☐	☐
1.1.5	Les groupes, rôles et responsabilités pour la gestion logique des composants du réseau sont-ils assignés et documentés dans les standards de configuration de pare-feu et de routeur ?	▪ Examiner les standards de configuration du pare-feu et du routeur. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
1.1.6	(a) Est-ce que les normes de configuration du pare-feu et du routeur comprennent une liste documentée des services, des protocoles et des ports, y compris la justification commerciale et l'approbation pour chacun de ces éléments ?	▪ Examiner les standards de configuration du pare-feu et du routeur.	☐	☐	☐	☐	☐
	(b) Tous les services, protocoles et ports non sécurisés sont-ils identifiés et les fonctions de sécurité sont-elles documentées et implémentées pour chaque service identifié ?	▪ Examiner les standards de configuration du pare-feu et du routeur. ▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐	☐
1.1.7	(a) Les standards de configuration des pare-feu et des routeurs exigent-ils l'examen des règles des pare-feu et des routeurs au moins tous les six mois ?	▪ Examiner les standards de configuration du pare-feu et du routeur.	☐	☐	☐	☐	☐
	(b) Les règles de pare-feu et de routeur sont-elles vérifiées au moins tous les six mois ?	▪ Examiner la documentation des examens de pare-feu.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
1.2.2	Les fichiers de configuration de routeur sont-ils sécurisés des accès non autorisés et synchronisés — par exemple, la configuration en cours d'exécution (ou active) correspond-elle à la configuration de démarrage (utilisée lorsque les machines sont mises en route) ?	▪ Examiner les standards de configuration du pare-feu et du routeur. ▪ Examiner les fichiers de configuration du routeur et les configurations du routeur.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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 :						
1.3.1	Une zone démilitarisée (DMZ) est-elle en place pour restreindre le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public ?	▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐	☐
1.3.2	Le trafic Internet entrant est-il restreint aux adresses IP dans la zone démilitarisée ?	▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐	☐
1.3.3	Des mesures anti-usurpation sont-elles mises en œuvre pour détecter et pour empêcher les adresses IP de source frauduleuses de pénétrer sur le réseau ? (Par exemple, bloquer le trafic originaire d'Internet avec une adresse interne).	▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
1.3.6	Les composants du système qui stockent les données de titulaires de carte (comme une base de données) se trouvent-ils dans une zone de réseau interne, isolée de la zone démilitarisée et des autres réseaux non approuvés ?	▪ 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.	Non testé
1.3.7	(a) Des moyens sont-ils en place pour prévenir la divulgation d'adresses IP et d'informations d'acheminement confidentielles sur Internet ? ***Remarque :*** *Quelques-unes des méthodes permettant de dissimuler les adresses IP sont présentées ci-après :* • Traduction d'adresse réseau (Network Address Translation, NAT) ; • Protéger les serveurs contenant des données de titulaires de carte derrière des serveurs proxy/pare-feu ; • Retrait ou filtrage des annonces d'acheminement pour les réseaux privés employant des adresses enregistrées ; • Utilisation interne de l'espace d'adresse RFC1918 au lieu d'adresses enregistrées.	▪ Examiner les configurations du pare-feu et du routeur.	☐	☐	☐	☐	☐
	(b) La divulgation d'adresses IP et d'informations d'acheminement confidentielles à des entités externes est-elle autorisée ?	▪ Examiner les configurations du pare-feu et du routeur. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
1.4	(a) Un logiciel de pare-feu personnel (ou une fonctionnalité équivalente) est-il installé et actif sur tout appareil informatique portable (y compris les appareils appartenant à la société et/ou à l'employé) équipé d'une connexion à Internet en dehors du réseau (par exemple, les ordinateurs portables utilisés par les employés), et qui est également utilisé pour accéder au CDE ?	▪ Examiner les politiques et les standards de configuration. ▪ Examiner les appareils mobiles et/ou les appareils appartenant aux employés.	☐	☐	☐	☐	☐
	(b) Le logiciel de pare-feu personnel (ou fonctionnalité équivalente) est-il configuré selon des paramètres spécifiques, effectivement en fonctionnement et de sorte qu'il ne puisse pas être modifié par les utilisateurs d'appareils portables et/ou appartenant à des employés ?	▪ Examiner les politiques et les standards de configuration. ▪ Examiner les appareils mobiles et/ou les appareils appartenant aux employés.	☐	☐	☐	☐	☐

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

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.	Non testé
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.	Non testé
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.**	**Non testé**
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.**	**Non testé**
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.	Non testé
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.	Non testé
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.	Non testé
	(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.	☐	☐	☐	☐	☐
2.4	(a) Un inventaire est-il conservé pour les composants du système qui sont dans la portée du PCI DSS, y compris une liste des composants logiciels et matériels, et une description du fonctionnement/de l'utilisation de chacun ?	▪ Examiner l'inventaire du système.	☐	☐	☐	☐	☐
	(b) l'inventaire documenté est-il tenu à jour ?	▪ 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.	☐	☐	☐	☐	☐
2.6	*Cette condition s'applique uniquement aux prestataires de services.*						

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.	Non testé
3.1	Les politiques, processus et procédures de conservation et d'élimination de données sont-elles déployées comme suit :						
	(a) La quantité de données stockées et le délai de conservation sont-ils limités aux obligations légales, réglementaires et/ou commerciales ?	▪ Examiner les politiques et procédures de conservation et d'élimination des données. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(b) Des processus définis sont-ils en place pour supprimer les données de titulaires de carte de manière sécurisée lorsqu'elles ne sont plus requises pour des raisons légales, réglementaires et/ou commerciales ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Examiner le mécanisme de suppression.	☐	☐	☐	☐	☐
	(c) Des conditions spécifiques de conservation spécifiques des données de titulaires de carte sont-elles en place ? *Par exemple, les données de titulaires de carte doivent être détenues durant une période X pour des raisons professionnelles Y.*	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Examiner les exigences en matière de conservation.	☐	☐	☐	☐	☐
	(d) Un processus trimestriel est-il en place pour l'identification et la suppression sécurisée des données de titulaires de carte stockées excédant les conditions de conservation définies ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Observer les processus de suppression.	☐	☐	☐	☐	☐
	(e) Est-ce que toutes les données de titulaires de carte stockées respectent les conditions définies dans la politique de conservation des données ?	▪ Examiner les fichiers et les enregistrements du système.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
3.2	(a) *Cette procédure de test s'applique uniquement aux émetteurs.*						
	(b) *Cette procédure de test s'applique uniquement aux émetteurs.*						
	(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'identification 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.	Non testé
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	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
3.4	Le PAN est-il rendu illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes ? ▪ Hachage unilatéral s'appuyant sur une méthode cryptographique robuste (la totalité du PAN doit être hachée) ; ▪ Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ; ▪ Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ; ▪ Cryptographie robuste associée aux processus et procédures de gestion des clés. ***Remarque :*** *Il s'agit d'un effort relativement peu important pour un individu malveillant de reconstruire les données du PAN d'origine, s'il a à la fois accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachées et tronquées du même PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être en place pour garantir que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.*	▪ Examiner la documentation du vendeur. ▪ Examiner le référentiel de données. ▪ Examiner les supports amovibles. ▪ Examiner les journaux d'audit, y compris les journaux d'applications de paiement.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
3.4.1	Si un cryptage par disque est utilisé (plutôt qu'un cryptage de base de données au niveau fichier ou colonne), l'accès est-il géré comme suit : ***Remarque :*** *En outre, cette condition s'applique à toutes les autres conditions de gestion des clés et de cryptage PCI DSS.*						
	(a) L'accès logique aux systèmes de fichier cryptés est-il géré indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas de bases de données de comptes d'utilisateur locales ou d'éléments d'authentification de connexion au réseau générique) ?	▪ Examiner les configurations du système. ▪ Observer le processus d'authentification.	☐	☐	☐	☐	☐
	(b) Les clés cryptographiques sont-elles stockées de manière sécurisée (par exemple, sur des supports amovibles correctement protégés avec des contrôles d'accès stricts) ?	▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(c) Les données de titulaires de carte sur les supports amovibles sont-elles cryptées où qu'elles soient stockées ? ***Remarque :*** *Si le cryptage de disque n'est pas utilisé pour crypter les supports amovibles, les données stockées sur ce support devront être rendues illisibles par une autre méthode.*	▪ Examiner les configurations du système. ▪ Observer les processus.	☐	☐	☐	☐	☐
3.5	Les clés utilisées pour sécuriser des données de titulaires de carte sont-elles protégées contre la divulgation et les utilisations malveillantes comme suit : ***Remarque :*** *Cette condition s'applique aux clés utilisées pour crypter les données de titulaires de carte stockées ainsi qu'aux clés de cryptage de clés utilisées pour protéger les clés de cryptage de données. Ces clés de cryptage de clés doivent être au moins aussi robustes que la clé de cryptage de données.*						

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
3.5.1	*Cette condition s'applique uniquement aux prestataires de services.*						
3.5.2	L'accès aux clés cryptographiques est-il restreint au plus petit nombre d'opérateurs possible ?	▪ Examiner les listes d'accès utilisateur.	☐	☐	☐	☐	☐
3.5.3	Les clés cryptographiques secrètes et privées utilisées pour crypter/décrypter les données de titulaires de carte sont-elles stockées sous l'une (ou sous plusieurs) des formes suivantes en permanence ? ▪ Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stockée séparément de la clé de cryptage de données ; ▪ Dans un périphérique cryptographique sécurisé (comme un module de sécurité matériel (hôte) ou un dispositif de point d'interaction approuvé PTS) ; ▪ En tant que deux composants de clé ou partages de clé de pleine longueur au moins, conformément à la méthode acceptée par l'industrie. ***Remarque :*** *Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes.*	▪ Examiner les procédures documentées. ▪ Examiner les configurations du système et les emplacements de stockage des clés, y compris les clés de cryptage de clés.	☐	☐	☐	☐	☐
3.5.4	Les clés cryptographiques sont-elles stockées dans aussi peu d'endroits que possible ?	▪ Examiner les emplacements de stockage des clés. ▪ Observer les processus.	☐	☐	☐	☐	☐
3.6	(a) Tous les processus et les procédures de gestion des clés cryptographiques sont-ils intégralement détaillés et déployés pour les clés cryptographiques servant au cryptage des données de titulaires de carte ?	▪ Examiner les procédures de gestion des clés.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(c) Des processus et procédures de gestion des clés sont-ils déployés pour exiger ce qui suit :						
3.6.1	Les procédures de clés cryptographiques comprennent-elles la génération de clés cryptographiques robustes ?	▪ Examiner les procédures de gestion des clés. ▪ Observer les procédures de génération de clés.	☐	☐	☐	☐	☐
3.6.2	Les procédures de clés cryptographiques comprennent-elles la distribution sécurisée de clés cryptographiques ?	▪ Examiner les procédures de gestion des clés. ▪ Observer la méthode de distribution des clés.	☐	☐	☐	☐	☐
3.6.3	Les procédures de clés cryptographiques comprennent-elles le stockage sécurisé de clés cryptographiques ?	▪ Examiner les procédures de gestion des clés. ▪ Observer la méthode de stockage sécurisé des clés.	☐	☐	☐	☐	☐
3.6.4	Les procédures de clés cryptographiques comprennent-elles des changements pour les clés ayant atteint la fin de leur cryptopériode (par exemple, après la fin d'une période définie et/ou après la production d'une certaine quantité de cryptogrammes par une clé donnée), comme l'a défini le fournisseur de l'application associée ou le propriétaire de la clé, et selon les meilleures pratiques et directives du secteur (par exemple, la publication spéciale NIST 800-57) ?	▪ Examiner les procédures de gestion des clés. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
3.6.5	(a) Les procédures de clés cryptographiques comprennent-elles le retrait ou le changement des clés (par exemple, en les archivant, détruisant, et/ou révoquant selon le cas), lorsque le degré d'intégrité d'une clé est affaibli (par exemple, le départ d'un employé ayant connaissance du texte clair d'une clé) ?	▪ Examiner les procédures de gestion des clés. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(b) Les procédures de clés cryptographiques comprennent-elles le remplacement des clés compromises ou suspectées de l'être ?	▪ Examiner les procédures de gestion des clés. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(c) Si des clés cryptographiques retirées ou remplacées sont conservées, ces clés sont-elles utilisées uniquement à des fins de décryptage/vérification et non pour des opérations de cryptage ?	▪ Examiner les procédures de gestion des clés. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
3.6.6	Si des opérations de gestion de clé en texte clair sont utilisées, les procédures de clé cryptographiques comprennent-elles le fractionnement des connaissances et le double contrôle des clés cryptographiques comme suit : ▪ Est-ce que la procédure de fractionnement des connaissances nécessite que les composants de clé soient sous le contrôle d'au moins deux personnes qui ne connaissent que leur propre composant de clé ? ET ▪ Les procédures de double contrôle des clés nécessitent qu'au moins deux personnes soient requises pour effectuer les opérations de gestion de clé et qu'une personne n'ait pas accès aux matériaux d'authentification (par exemple les mots de passe ou les clés) d'une autre ? ***Remarque :*** *La génération, la transmission, le chargement, le stockage et la destruction de clés sont quelques-uns des exemples d'interventions de gestion manuelle des clés.*	▪ Examiner les procédures de gestion des clés. ▪ Interroger le personnel et/ou. ▪ Observer les processus.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	**Oui, avec CCW**	**Non**	**S.O.**	**Non testé**
3.6.7	Les procédures de clés cryptographiques comprennent-elles la prévention d'une substitution non autorisée des clés cryptographiques ?	▪ Examiner les procédures. ▪ Interroger le personnel et/ou ▪ Observer les processus.	☐	☐	☐	☐	☐
3.6.8	Les opérateurs chargés de la gestion de clés cryptographiques doivent-ils reconnaître (par écrit ou de manière électronique) formellement qu'ils comprennent et acceptent leurs responsabilités ?	▪ Examiner les procédures. ▪ Examiner la documentation ou les autres justifications.	☐	☐	☐	☐	☐
3.7	Les politiques de sécurité et les procédures opérationnelles pour la protection des données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
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.	Non testé
	(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	(a) Les PAN sont-ils rendus illisibles ou sécurisés avec une méthode de cryptographie robuste chaque fois qu'ils sont envoyés par des technologies de messagerie pour utilisateurs finaux (par exemple, les e-mails, la messagerie instantanée, les SMS, le chat, etc.) ?	▪ Observer les processus. ▪ Examiner les transmissions sortantes.	☐	☐	☐	☐	☐
	(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.	☐	☐	☐	☐	☐
4.3	Les politiques de sécurité et les procédures opérationnelles pour le cryptage des transmissions de données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
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.	Non testé
	(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.	☐	☐	☐	☐	☐
5.4	Les politiques de sécurité et les procédures opérationnelles pour la protection des systèmes contre les logiciels malveillants sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ 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.	Non testé
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.	Non testé
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.	☐	☐	☐	☐	☐
6.3	(a) Les processus de conception de logiciel sont-ils basés sur les normes/meilleures pratiques du secteur ?	▪ Examiner les processus de conception de logiciels. ▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(b) La sécurité des informations est-elle intégrée à l'ensemble du cycle de vie de la conception d'un logiciel ?	▪ Examiner les processus de conception de logiciels. ▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(c) Les applications logicielles sont-elles conçues conformément à la norme PCI DSS (par exemple, authentification et connexion sécurisées) ?	▪ Examiner les processus de conception de logiciels. ▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(d) Les processus de développement garantissent de qui suit en 6.3.1 - 6.3.2 :						
6.3.1	Les comptes de développement, de test et/ou les comptes d'application personnalisés, les ID d'utilisateur et des mots de passe sont-ils supprimés avant l'activation des applications ou leur mise à la disposition des clients ?	▪ Examiner les processus de conception de logiciels. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.3.2	La totalité du code d'application personnalisé est-elle examinée avant la mise en production ou la mise à la disposition des clients afin d'identifier toute vulnérabilité de codage éventuelle (à l'aide de processus manuels ou automatiques comme suit : ▪ Les modifications de code sont-elles examinées par des individus autres que l'auteur initial du code et par des individus compétents en la matière de techniques d'analyse de code et de pratiques de codage sécurisées ? ▪ Les examens de code garantissent-ils que le code est développé conformément aux directives de codage sécurisé ? ▪ Les corrections appropriées sont-elles implémentées avant la publication ? ▪ Les résultats de la révision du code sont-ils passés en revue et approuvés par les responsables avant la publication ? ***Remarque** : Cette condition s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de conception du système. Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers. Les applications Web destinées au public font également l'objet de contrôles supplémentaires afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par la condition 6.6 de la norme PCI DSS.*	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Examiner les changements récents et les registres de changements.	☐	☐	☐	☐	☐
6.4	Les processus et procédures de contrôle des modifications sont-ils suivis pour tous les changements des composants du système de manière à comprendre ce qui suit :						

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.4.1	(a) Les environnements de test/conception sont-ils distincts de l'environnement de production ?	▪ Examiner les processus et les procédures du contrôle de changement. ▪ Examiner la documentation du réseau et les configurations des appareils du réseau.	☐	☐	☐	☐	☐
	(b) Le contrôle d'accès est-il en place pour assurer la séparation entre les environnements de développement test et l'environnement de production ?	▪ Examiner les processus et les procédures du contrôle de changement. ▪ Examiner les paramètres de contrôle d'accès.	☐	☐	☐	☐	☐
6.4.2	Existe-t-il une distinction entre les missions des collaborateurs affectés aux environnements de conception/test et celles du personnel affecté à l'environnement de production ?	▪ Examiner les processus et les procédures du contrôle de changement. ▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
6.4.3	Les données de production (PAN actifs) ***ne sont-elles pas*** utilisées à des fins de test ou de conception ?	▪ Examiner les processus et les procédures du contrôle de changement. ▪ Observer les processus. ▪ Interroger le personnel. ▪ Examiner les données de test.	☐	☐	☐	☐	☐
6.4.4	Les données et les comptes de test sont-ils éliminés des composants de système avant que le système ne devienne actif/passe en phase de production ?	▪ Examiner les processus et les procédures du contrôle de changement. ▪ Observer les processus. ▪ Interroger le personnel. ▪ Examiner les systèmes de production.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.4.5	(a) Est-ce que les procédures relatives au contrôle de changement sont documentées et exigent-elles ce qui suit ? - Documentation de l'impact - Approbation de changement documentée par les parties autorisées - Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système - Procédures de suppression	▪ Examiner les processus et les procédures du contrôle de changement.	☐	☐	☐	☐	☐
	(b) Les opérations suivantes sont-elles effectuées et documentées pour tous les changements :						
6.4.5.1	L'impact est-il documenté ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement.	☐	☐	☐	☐	☐
6.4.5.2	Le changement détaillé est-il approuvé par les responsables appropriés ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement.	☐	☐	☐	☐	☐
6.4.5.3	(a) Un test de fonctionnalité est-il réalisé pour vérifier que le changement ne compromet pas la sécurité du système ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(b) Pour les changements de code personnalisé, les tests de mises à jour du point de vue de la conformité à la condition 6.5 de la norme PCI DSS sont-ils effectués avant leur mise en production ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement.	☐	☐	☐	☐	☐
6.4.5.4	Procédures de suppression ?	▪ Retracer les changements sur la documentation du contrôle de changement. ▪ Examiner la documentation du contrôle de changement.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.5	(a) Les processus de développement de logiciel adressent-ils les vulnérabilités de code les plus fréquentes ?	▪ Examiner les procédures et les politiques de développement de logiciels.	☐	☐	☐	☐	☐
	(b) Est-ce que les développeurs suivent une formation au moins une fois par an pour mettre à jour leurs techniques de codage sécurisé, et savoir notamment comment éviter les vulnérabilités de codage courantes ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Examiner les registres de formation.	☐	☐	☐	☐	☐
	(c) Les applications sont-elles développées sur des directives de codage sécurisé afin de protéger les applications, au minimum, des vulnérabilités suivantes : ***Remarque :*** *Les vulnérabilités décrites aux points 6.5.1 à 6.5.10 faisaient partie des meilleures pratiques du secteur au moment de la publication de cette version de la norme PCI DSS. Cependant, comme les meilleures pratiques de gestion de la vulnérabilité du secteur sont actualisées (par exemple, le guide Open Web Application Security Project [OWASP], le Top 25 SANS CWE, le codage sécurisé CERT, etc.), les meilleures pratiques actuelles doivent être utilisées pour ces conditions.*						
6.5.1	Les techniques de codage adressent-elles les attaques par injection, en particulier injection de commandes SQL ? ***Remarque :*** *Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.*	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.2	Est-ce que les techniques de codage adressent les vulnérabilités de saturation de la mémoire tampon ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.5.3	Les techniques de codage répondent-elles au stockage cryptographique non sécurisé ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.4	Les techniques de codage répondent-elles aux communications non sécurisées ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.5	Les techniques de codage répondent-elles aux manipulations incorrectes des erreurs ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.6	Les techniques de codage adressent-elles toutes les vulnérabilités à « haut risque » identifiées dans le processus d'identification de vulnérabilité (définies par la condition 6.1 de la norme PCI DSS) ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
Pour les applications Web et les interfaces d'application (interne ou externe), les applications sont-elles développées sur la base de directives de codage sécurisé afin de protéger les applications des vulnérabilités suivantes :							
6.5.7	Les techniques de codage adressent-elles les vulnérabilités aux attaques XSS (Cross-Site) ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.5.8	Les techniques de codage adressent-elles le contrôle d'accès inapproprié, tel que des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès URL, le survol de répertoire et la non-restriction de l'accès utilisateur aux fonctions ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.9	Les techniques de codage adressent-elles les attaques CSRF (Cross-Site Request Forgery) ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.5.10	Les techniques de codage adressent-elles la gestion de rupture d'authentification et de session ?	▪ Examiner les politiques et les procédures de développement de logiciels. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
6.6	Pour les applications Web orientées public, les nouvelles menaces et vulnérabilités sont-elles traitées régulièrement et ces applications sont-elles protégées contre les attaques connues à l'aide de *l'une* des méthodes suivantes ? ▪ Réviser les applications Web orientées public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuels, comme suit : - Au moins une fois par an - Après toute modification - Par une société spécialisée dans la sécurité des applications - Que, au minimum, toutes les vulnérabilités de la condition 6.5 sont incluses dans l'évaluation - Toutes les vulnérabilités sont corrigées - L'application est réévaluée après les corrections ***Remarque** : Cette évaluation est différente des scans de vulnérabilité effectués pour la condition 11.2.* – **OU** – ▪ Installation d'une solution technique automatisée pour détecter et empêcher des attaques basées sur le Web (par exemple, un pare-feu d'application Web) comme suit : - Est située devant les applications Web destinées au public pour détecter et empêcher les attaques basées sur le Web. - Fonctionne activement et est mise à jour au besoin. - Génère des journaux d'audit. - Est configurée soit pour bloquer les attaques basées sur le Web soit pour générer une alerte qui fera directement l'objet d'une enquête.	▪ Examiner les processus documentés. ▪ Interroger le personnel. ▪ Examiner les registres des évaluations de la sécurité des applications. ▪ 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.	Non testé
6.7	Les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de systèmes et applications sécurisés sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.**	**Non testé**
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 :						
	▪ Existe-t-il une politique écrite pour le contrôle d'accès, comprenant les points suivants ? - Définir les besoins d'accès et les affectations de privilèges pour chaque rôle - La restriction d'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail, - L'affectation d'accès basée sur la classification et la fonction professionnelles de chaque employé - L'approbation documentée (électroniquement ou par écrit) par les parties autorisées pour tous les accès, y compris la liste de tous les privilèges spécifiques approuvés	▪ Examiner les politiques de contrôle d'accès écrites.	☐	☐	☐	☐	☐
7.1.1	Les besoins d'accès pour chaque rôle sont-ils définis, y compris : ▪ Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste ? ▪ Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources ?	▪ Examiner les rôles et les besoins d'accès.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
7.1.4	L'approbation documentée des parties responsables spécifiant les privilèges requis est-elle documentée ?	▪ Examiner les ID utilisateur. ▪ Comparer avec les approbations documentées. ▪ Comparer les privilèges assignés avec les approbations documentées.	☐	☐	☐	☐	☐
7.2	Un système de contrôle d'accès est-il en place pour que les composants de système restreignent l'accès en fonction du besoin d'information de l'utilisateur et est-il configuré sur « refuser tout », sauf permission spécifique comme suit :						
7.2.1	Des systèmes de contrôle d'accès sont-ils déployés sur tous les composants du système ?	▪ Examiner la documentation du vendeur. ▪ Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
7.2.2	Les systèmes de contrôle d'accès sont-ils configurés pour octroyer les privilèges aux individus en fonction de leur classification et fonction professionnelles ?	▪ Examiner la documentation du vendeur. ▪ Examiner les paramètres de configuration.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
7.2.3	Les systèmes de contrôle d'accès intègrent-ils un paramètre par défaut « refuser tout » ?	▪ Examiner la documentation du vendeur. ▪ Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
7.3	Les politiques de sécurité et les procédures opérationnelles pour restreindre l'accès aux données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
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.	☐	☐	☐	☐	☐
8.1.2	Des compléments, suppressions et modifications des ID et des informations utilisateur, et autres éléments identifiants sont-ils contrôlés, de manière à n'appliquer les ID utilisateurs qu'en fonction de leurs autorisations (y compris avec les privilèges spécifiés) ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les ID des utilisateurs privilégiés et génériques et les autorisations associées. ▪ Observer les configurations du système.	☐	☐	☐	☐	☐
8.1.3	L'accès des utilisateurs qui ne travaillent plus pour la société est-il immédiatement désactivé ou révoqué ?	▪ Examiner les procédures de mots de passe. ▪ Examiner les comptes utilisateur fermés. ▪ Examiner les listes d'accès actuelles. ▪ Observer les appareils d'authentification physique renvoyés.	☐	☐	☐	☐	☐
8.1.4	Les comptes utilisateurs inactifs sont-ils supprimés ou désactivés dans un délai de 90 jours ?	▪ Examiner les procédures de mots de passe. ▪ Observer les comptes utilisateur.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						
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.	☐	☐	☐	☐	☐
8.2	Outre l'assignation d'un ID unique, l'une ou plusieurs des méthodes suivantes sont-elles employées pour authentifier tous les utilisateurs ? ▪ Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; ▪ Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; ▪ Quelque chose concernant l'utilisateur, comme une mesure biométrique.	▪ Examiner les procédures de mots de passe. ▪ Observer les processus d'authentification.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
8.2.1	(a) Une cryptographie robuste est-elle utilisée pour rendre tous les justificatifs d'authentification (comme les mots de passe/locutions de passage) illisibles pendant la transmission et le stockage sur tous les composants du système ?	▪ Examiner les procédures de mots de passe. ▪ Examiner la documentation du vendeur. ▪ Examiner les paramètres de configuration du système. ▪ Observer les fichiers de mots de passe. ▪ Observer les transmissions de données.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						
8.2.2	L'identité de l'utilisateur est-elle vérifiée avant de modifier tout justificatif d'authentification (par exemple, lors des réinitialisations de mot de passe, la délivrance de nouveaux jetons ou la création de nouvelles clés) ?	▪ Observer les procédures d'authentification. ▪ Observer le personnel.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
8.2.4	(a) 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.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						
8.2.5	(a) 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.	☐	☐	☐	☐	☐
	(b) *Cette procédure de test s'applique uniquement aux prestataires de services.*						
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.*						

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
8.5.1	*Cette condition s'applique uniquement aux prestataires de services.*						
8.6	Lorsque les autres mécanismes d'authentification sont utilisés (par exemple, des jetons de sécurité logiques ou physiques, des cartes électroniques, certificats, etc.) l'utilisation de ces mécanismes est-elle assignée comme suit ? ▪ Les mécanismes d'authentification doivent être affectés à un compte individuel et non pas partagés par de multiples comptes ▪ Les contrôles logiques et/ou physiques doivent être en place pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Examiner les réglages de configuration du système et/ou les contrôles physiques.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
8.7	L'accès à n'importe quelle base de données contenant des données de titulaires de carte (y compris les accès par les applications, administrateurs et autres utilisateurs) est restreint comme suit :						
	(a) Tous les accès aux bases de données, toutes les consultations et actions exécutées par les utilisateurs dans celles-ci (par exemple, déplacement, copie, suppression d'informations) s'effectuent-ils exclusivement au moyen de méthodes programmées (par exemple, par le biais de procédures stockées) ?	▪ Examiner les politiques et procédures d'authentification des bases de données. ▪ Examiner les réglages de configuration des bases de données et des applications.	☐	☐	☐	☐	☐
	(b) L'accès direct des utilisateurs ou les requêtes aux bases de données sont-ils restreints aux seuls administrateurs de bases de données ?	▪ Examiner les politiques et procédures d'authentification des bases de données. ▪ Examiner les paramètres de contrôle d'accès aux bases de données. ▪ Examiner les réglages de configuration des applications de bases de données.	☐	☐	☐	☐	☐
	(c) Les ID d'application peuvent-ils uniquement être utilisés par les applications (et non par des utilisateurs individuels ou d'autres processus) ?	▪ Examiner les politiques et procédures d'authentification des bases de données. ▪ Examiner les paramètres de contrôle d'accès aux bases de données. ▪ Examiner les réglages de configuration des applications de bases de données.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	Non testé
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.**	**Non testé**
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.	☐	☐	☐	☐	☐
9.1.3	L'accès physique aux points d'accès, passerelles, périphériques portables, matériel réseau/communications et lignes de télécommunication sans fil est-il restreint ?	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Observer les appareils.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
9.2	(a) Des procédures sont-elles élaborées pour facilement distinguer facilement le personnel du site des visiteurs, comme suit : - L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple) ; - Changement des conditions d'accès ; et - La révocation de l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à expiration (telle que les badges d'identification). *Dans le cadre de la condition 9, le terme « personnel du site » 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. Un « visiteur » est défini comme un fournisseur, l'hôte du personnel du site, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée.*	▪ Examiner les politiques et les procédures. ▪ Interroger le personnel. ▪ Observer les méthodes d'identification (par ex., badges). ▪ Observer les processus visiteurs.	☐	☐	☐	☐	☐
	(b) Les méthodes d'identification utilisées (telles que les badges ID) identifient-elles clairement les visiteurs et permettent-elles de distinguer ces derniers du personnel du site ?	▪ Observer les méthodes d'identification.	☐	☐	☐	☐	☐
	(c) L'accès au système de badges est-il restreint au seul personnel autorisé ?	▪ Observer les contrôles physiques et les contrôles d'accès pour le système de badge.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
9.3	L'accès physique aux zones sensibles est-il contrôlé pour le personnel du site comme suit : ▪ L'accès est-il autorisé et basé sur les fonctions professionnelles individuelles ? ▪ L'accès est-il révoqué immédiatement après la cessation des fonctions ? ▪ À la cessation de fonction, tous les mécanismes d'accès physique, tels que les clés, les cartes d'accès, etc. sont-ils rendus ou désactivés ?	▪ Interroger le personnel. ▪ Examiner les listes de contrôle d'accès. ▪ Observer le personnel sur le site. ▪ Comparer les listes des anciens employés aux listes de contrôle d'accès.	☐	☐	☐	☐	☐
9.4	L'identification des visiteurs et des accès respectent-ils les points suivants :						
9.4.1	Les visiteurs sont-ils autorisés avant d'entrer et accompagnés en permanence dans les zones où sont traitées et conservées les données de titulaires de carte ?	▪ Examiner les politiques et les procédures. ▪ Observer les processus visiteurs, y compris les méthodes de contrôle d'accès. ▪ Interroger le personnel. ▪ Observer les visiteurs et l'utilisation des badges.	☐	☐	☐	☐	☐
9.4.2	(a) Les visiteurs sont-ils identifiés et un badge ou une autre forme d'identification leur est-elle remise avec une date limite d'utilisation, qui distingue clairement les visiteurs du personnel du site ?	▪ Observer l'utilisation des badges du personnel et des visiteurs. ▪ Examiner l'identification.	☐	☐	☐	☐	☐
	(b) Les badges des visiteurs, ou autres formes d'identification, portent-ils une date d'expiration ?	▪ Observer le processus. ▪ Examiner l'identification.	☐	☐	☐	☐	☐
9.4.3	Les visiteurs doivent-ils rendre le badge ou une autre forme d'identification physique avant de quitter les locaux ou à la date d'expiration ?	▪ Observer les processus. ▪ Observer les visiteurs qui quittent les locaux.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
9.4.4	(a) Un registre des visites est-il utilisé pour consigner l'accès physique aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de carte ?	▪ Examiner les politiques et les procédures. ▪ Examiner le journal visiteurs. ▪ Observer les processus visiteurs. ▪ Examiner la conservation des journaux.	☐	☐	☐	☐	☐
	(b) Le journal des visiteurs consigne-t-il le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son accès physique ?	▪ Examiner les politiques et les procédures. ▪ Examiner le journal visiteurs.	☐	☐	☐	☐	☐
	(c) Le journal des visiteurs est-il conservé pendant au moins trois mois ?	▪ Examiner les politiques et les procédures. ▪ Examiner la conservation des journaux visiteurs.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
9.5.1	Est-ce que l'emplacement de rangement des sauvegardes sur support est examiné au moins une fois par an pour en confirmer la sécurité ?	▪ Examiner les politiques et procédures en termes de sécurisation physique des locaux de stockage des supports hors site. ▪ Interroger le personnel de la sécurité.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(b) Les contrôles comprennent-ils les éléments suivants :						
9.6.1	Les supports sont-ils classés afin de déterminer la sensibilité des données qu'ils contiennent ?	▪ Examiner les politiques et procédures de classification des supports. ▪ Interroger le personnel de la sécurité.	☐	☐	☐	☐	☐
9.6.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?	▪ Interroger le personnel. ▪ Examiner les journaux de suivi et la documentation relatifs à la distribution des supports.	☐	☐	☐	☐	☐
9.6.3	L'approbation de la direction est-elle obtenue avant le déplacement des supports (particulièrement lorsque le support est distribué aux individus) ?	▪ Interroger le personnel. ▪ Examiner les journaux de suivi et la documentation relatifs à la distribution des supports.	☐	☐	☐	☐	☐
9.7	Un contrôle strict est-il réalisé sur le stockage et l'accessibilité des supports ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐	☐
9.7.1	(a) Les journaux d'inventaire de tous les supports sont-ils correctement maintenus ?	▪ Examiner les journaux d'inventaire.	☐	☐	☐	☐	☐
	(b) Les inventaires réguliers des supports sont-ils effectués au moins une fois par an ?	▪ Examiner les journaux d'inventaire. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	**Oui, avec CCW**	**Non**	**S.O.**	**Non testé**
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.	☐	☐	☐	☐	☐
	(b) Existe-t-il une politique de destruction des médias qui définit les conditions pour les points suivants ? - Les documents papier doivent être déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être constitués. - Les conteneurs de stockage utilisés pour les documents qui sont détruits doivent être sécurisés. - Les données de titulaires de carte sur support électronique doivent être rendues irrécupérables (par exemple, à l'aide d'un programme de nettoyage sécurisé conformément aux normes du secteur en matière d'élimination sécurisée ou par destruction physique du média).	▪ 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 ?	▪ Interroger le personnel. ▪ Examiner les procédures. ▪ 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.	Non testé
9.8.2	Les données de titulaires de carte sur support électronique sont-elles rendues irrécupérables (à l'aide d'un programme de nettoyage sécurisé conformément aux normes du secteur en matière d'élimination sécurisée des informations, ou à l'aide de tout autre procédé de destruction physique des supports) de sorte que les données de titulaires de carte ne puissent pas être reconstituées ?	▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
9.9	Les appareils qui capturent les données de carte de paiement par interaction physique directe avec la carte sont-ils protégés des manipulations malveillantes et des substitutions ? ***Remarque :*** *Cette condition s'applique aux appareils de lecture de carte utilisés dans les transactions pour lesquelles la carte est présente (c'est-à-dire, une lecture de piste ou de puce) au point de vente. Cette condition n'est pas destinée à être appliquée pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.*						
	(a) Est-ce que les politiques et les procédures nécessitent qu'une liste de ces appareils soit conservée ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐	☐
	(b) Est-ce que les politiques et les procédures nécessitent que les appareils soient régulièrement inspectés afin de vérifier qu'aucune manipulation malveillante ou substitution n'a eu lieu ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐	☐
	(c) Est-ce que les politiques et les procédures exigent que le personnel soit formé à être conscient des comportements suspects et à signaler les manipulations malveillantes ou la substitution d'appareil ?	▪ Examiner les politiques et les procédures.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
	(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.	Non testé
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.	☐	☐	☐	☐	☐
9.10	Les politiques de sécurité et les procédures opérationnelles pour restreindre l'accès physique aux données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
10.1	(a) Les cheminements d'audit sont-ils activés et actifs pour les composants du système ?	▪ Observer les processus. ▪ Interroger l'administrateur du système.	☐	☐	☐	☐	☐
	(b) L'accès aux composants du système est-il relié aux utilisateurs individuels ?	▪ Observer les processus. ▪ Interroger l'administrateur du système.	☐	☐	☐	☐	☐
10.2	Des journaux d'audit automatisés sont-ils en place pour tous les composants du système afin de reconstituer les événements suivants :						
10.2.1	Tous les accès des utilisateurs aux données de titulaires de carte ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
10.2.3	Accès à tous les journaux d'audit ?	▪ 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.	Non testé
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.	☐	☐	☐	☐	☐
10.2.6	Initialisation, interruption ou pause des journaux d'audit ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐	☐
10.2.7	Création et suppression d'objets au niveau système ?	▪ 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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
10.3.2	Type d'événement ?	▪ Interroger le personnel. ▪ Observer les journaux d'audit. ▪ Examiner les paramètres des journaux d'audit.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
10.4	Toutes les horloges et heures du système essentiel sont-elles synchronisées par l'utilisation d'une technologie de synchronisation temporelle, et cette technologie est-elle maintenue à jour ? ***Remarque :*** *Le protocole Network Time Protocol (NTP - Protocole d'Heure Réseau) est un exemple de technologie de synchronisation temporelle.*	▪ Examiner les standards et les processus de configuration de l'heure.	☐	☐	☐	☐	☐
10.4.1	Les processus suivants sont-ils mis en œuvre pour que l'heure des systèmes critiques soit correcte et la même pour tous :						
	(a) Seuls le ou les serveurs d'heure centrale désignée reçoivent des signaux de sources externes et ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné) ?	▪ Examiner les standards et les processus de configuration de l'heure. ▪ Examiner les paramètres du système liés à l'heure.	☐	☐	☐	☐	☐
	(b) Lorsqu'il y a plus d'un serveur d'heure désigné, les serveurs d'heure sont-ils basés l'un sur l'autre pour conserver une heure précise ?	▪ Examiner les standards et les processus de configuration de l'heure. ▪ Examiner les paramètres du système liés à l'heure.	☐	☐	☐	☐	☐
	(c) Les systèmes reçoivent-ils l'heure uniquement à partir des serveurs d'heure centrale désignés ?	▪ Examiner les standards et les processus de configuration de l'heure. ▪ Examiner les paramètres du système liés à l'heure.	☐	☐	☐	☐	☐
10.4.2	Les données temporelles sont-elles protégées comme suit : (a) L'accès aux données temporelles est-il restreint au seul personnel ayant un besoin professionnel d'accéder à de telles données ?	▪ Examiner les configurations du système et les paramètres de synchronisation de l'heure.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(b) Les changements des réglages de l'heure sur les systèmes essentiels sont-ils connectés, surveillés et révisés ?	▪ Examiner les configurations du système ainsi que les paramètres et journaux de synchronisation de l'heure.	☐	☐	☐	☐	☐
10.4.3	Les paramètres temporels sont-ils reçus de sources temporelles spécifiques reconnues par le secteur ? (Cela permet de prévenir un changement de l'heure par un individu malveillant). *Il est également possible de crypter ces mises à jour avec une clé symétrique, et de créer des listes de contrôle d'accès qui indiquent les adresses IP des machines clientes qui recevront les mises à jour temporelles (afin d'empêcher toute utilisation non autorisée des serveurs d'horloge internes).*	▪ Examiner les configurations du système.	☐	☐	☐	☐	☐
10.5	Les journaux d'audit sont-ils sécurisés de manière à ne pas pouvoir être altérés, comme suit :						
10.5.1	L'affichage des journaux d'audit est-il restreint aux utilisateurs qui en ont besoin pour mener à bien leur travail ?	▪ Interroger les administrateurs du système. ▪ Examiner les configurations et les permissions du système.	☐	☐	☐	☐	☐
10.5.2	Les fichiers journaux d'audit existants sont-ils protégés contre toute modification non autorisée par des mécanismes de contrôle d'accès, leur isolation physique et/ou l'isolation du réseau ?	▪ Interroger les administrateurs du système. ▪ Examiner les configurations et les permissions du système.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
10.5.3	Les fichiers journaux d'audit sont-ils sauvegardés rapidement sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer ?	▪ Interroger les administrateurs du système. ▪ Examiner les configurations et les permissions du système.	☐	☐	☐	☐	☐
10.5.4	Les registres des technologies orientées vers l'extérieur (par exemple, sans-fil, pare-feu, DNS, messagerie) sont-ils écrits sur un serveur de journal interne centralisé et sécurisé ou un support ?	▪ Interroger les administrateurs du système. ▪ Examiner les configurations et les permissions du système.	☐	☐	☐	☐	☐
10.5.5	Un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications est-il utilisé sur les registres pour s'assurer que les données qu'ils contiennent ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte) ?	▪ Examiner les réglages, les fichiers contrôlés et les résultats des activités de contrôle.	☐	☐	☐	☐	☐
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.	Non testé
10.6.1	(a) Les politiques et les procédures de sécurité écrites sont-elles définies pour examiner les points suivants 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.	☐	☐	☐	☐	☐
	(b) Les journaux et événements de sécurité sont-ils examinés au moins une fois par jour ?	▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
10.6.2	(a) Les politiques et les procédures écrites sont-elles définies pour l'examen régulier des journaux de tous les autres composants du système, manuellement ou à l'aide d'outils de journalisation, conformément aux politiques et à la stratégie de gestion des risques de l'organisation ?	▪ Examiner les politiques de sécurité et les procédures.	☐	☐	☐	☐	☐
	(b) Les analyses de tous les autres composants du système sont-elles effectuées selon les politiques et la stratégie de gestion des risques de l'organisation ?	▪ Examiner la documentation d'évaluation des risques. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
10.6.3	(a) Les politiques et les procédures écrites sont-elles définies pour le suivi des exceptions et des anomalies identifiées pendant le processus d'examen ?	▪ Examiner les politiques de sécurité et les procédures.	☐	☐	☐	☐	☐
	(b) Le suivi des exceptions et des anomalies est-il effectué ?	▪ Observer les processus. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
10.7	(a) Les politiques de conservation des journaux d'audit sont-elles en place et exigent-elles que les journaux soient conservés pendant une année au moins, en gardant à portée de main les journaux des trois derniers mois au moins pour une analyse immédiate (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde) ?	▪ Examiner les politiques de sécurité et les procédures.	☐	☐	☐	☐	☐
	(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.	☐	☐	☐	☐	☐
10.8	*Cette condition s'applique uniquement aux prestataires de services.*						
10.9	Les politiques de sécurité et les procédures opérationnelles en place pour restreindre l'accès aux données de titulaires de carte sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
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.	☐	☐	☐	☐	☐
	(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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	**Oui, avec CCW**	**Non**	**S.O.**	**Non testé**
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.	Non testé
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.	Non testé
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.**	**Non testé**
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.	Non testé
11.3	Est-ce que la méthodologie de test de pénétration comprend les points suivants ? ▪ Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115) ▪ Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques ▪ Comprend un test depuis l'intérieur et l'extérieur du système ▪ Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée ▪ Définit les tests de pénétration de couche d'application pour qu'ils comprennent, au minimum les vulnérabilités indiquées dans la Condition 6.5 ▪ Définit les tests de pénétration de couche d'application pour qu'ils comprennent les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation ▪ Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois ▪ Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation	▪ Examiner la méthodologie du test de pénétration. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
11.3.1	(a) Les tests d'intrusion *externes* sont-ils effectués selon la méthodologie définie, au moins une fois par an et après toute modification significative de l'infrastructure ou de l'application de l'environnement (telle qu'une mise à jour du système d'exploitation, l'ajout d'un sous-réseau à l'environnement ou d'un serveur Web) ?	▪ Examiner la portée du travail. ▪ Examiner les résultats du dernier test de pénétration externe.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
	(b) 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.	☐	☐	☐	☐	☐
11.3.2	(a) Les tests d'intrusion *internes* sont-ils effectués selon la méthodologie définie, au moins une fois par an et après toute modification significative de l'infrastructure ou de l'application de l'environnement (telle qu'une mise à jour du système d'exploitation, l'ajout d'un sous-réseau à l'environnement ou d'un serveur Web) ?	▪ Examiner la portée du travail. ▪ Examiner les résultats du dernier test de pénétration interne.	☐	☐	☐	☐	☐
	(b) 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.	☐	☐	☐	☐	☐
11.3.3	Les vulnérabilités exploitables découvertes pendant le test d'intrusion sont-elles corrigées et suivies par un renouvellement des tests pour vérifier les corrections ?	▪ Examiner les résultats du test de pénétration.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	**Oui, avec CCW**	**Non**	**S.O.**	**Non testé**
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.	Non testé
11.3.4.1	*Cette condition s'applique uniquement aux prestataires de services.*						
11.4	(a) Les techniques d'intrusion-détection et/ou d'intrusion-prévention pour détecter et/ou qui empêchent les intrusions dans le réseau pour le contrôle du trafic sont-elles : - Au périmètre de l'environnement de données de titulaires de carte ; et - Aux points critiques de l'environnement de données de titulaires de carte.	▪ Examiner les configurations du système. ▪ Examiner les schémas du réseau.	☐	☐	☐	☐	☐
	(b) Les techniques d'intrusion-détection et/ou d'intrusion-prévention sont-elles configurées pour alerter le personnel en cas de soupçon de compromis ?	▪ Examiner les configurations du système. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
	(c) Tous les moteurs de détection et de prévention des intrusions, les références et les signatures sont-ils tenus à jour ?	▪ Examiner les configurations IDS/IPS. ▪ Examiner la documentation du vendeur.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	**Oui, avec CCW**	**Non**	**S.O.**	**Non testé**
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.**	**Non testé**
11.5 *(suite)*	(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.	☐	☐	☐	☐	☐
11.6	Les politiques de sécurité et les procédures opérationnelles pour le contrôle et les tests de sécurité sont-elles : ▪ Documentées ▪ Utilisées ▪ Connues de toutes les parties concernées ?	▪ Examiner les politiques de sécurité et les procédures opérationnelles. ▪ Interroger le personnel.	☐	☐	☐	☐	☐

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.	Non testé
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.	☐	☐	☐	☐	☐
12.2	(a) Est un processus annuel d'évaluation des risques mis en œuvre qui : - Identifie les actifs critiques, les menaces et vulnérabilités, et - Se solde par une analyse formelle et documentée de risques ? *Les exemples de méthodologies d'évaluation des risques comprennent entre autres les directives OCTAVE, ISO 27005 et NIST SP 800-30.*	▪ Examiner le processus d'évaluation annuelle des risques. ▪ Interroger le personnel.	☐	☐	☐	☐	☐
	(b) Le processus d'évaluation des risques est-il effectué au moins une fois pas an et à la suite des changements importants apportés à l'environnement (par exemple, acquisition, fusion, déménagement, etc.) ?	▪ Examiner la documentation d'évaluation des risques. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
12.3.4	Une méthode permettant de déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils) ?	▪ 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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
12.3.6	Emplacements acceptables des technologies sur le réseau ?	▪ Examiner les politiques d'utilisation. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.3.7	Liste des produits approuvés par la société ?	▪ Examiner les politiques d'utilisation. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
12.3.10	(a) Lors de l'accès aux données de titulaires de carte au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données de titulaires de carte sur des disques durs locaux et des supports électroniques amovibles, sauf autorisation expresse pour des besoins professionnels ? *Lorsqu'il existe un besoin professionnel autorisé, la politique d'utilisation doit exiger que les données soient protégées selon toutes les conditions applicables de la norme PCI DSS.*	▪ Examiner les politiques d'utilisation. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
	(b) Pour le personnel dûment autorisé, la politique exige-t-elle la protection des données de titulaires de carte conformément aux conditions de la norme PCI DSS ?	▪ 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.	Non testé
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.	☐	☐	☐	☐	☐
12.4.1	*Cette condition s'applique uniquement aux prestataires de services*.						
12.5	(a) La responsabilité de la sécurité des informations est-elle formellement assignée à un chef de la sécurité ou tout autre responsable compétent ?	▪ Examiner la politique et les procédures de sécurité des informations.	☐	☐	☐	☐	☐
	(b) Les responsabilités suivantes de gestion de la sécurité des informations sont-elles assignées à un individu ou à une équipe :						
12.5.1	Définir, renseigner et diffuser les politiques et les procédures de sécurité ?	▪ Examiner la politique et les procédures de sécurité des informations.	☐	☐	☐	☐	☐
12.5.2	Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent ?	▪ Examiner la politique et les procédures de sécurité des informations.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
12.5.4	Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification de comptes ?	▪ Examiner la politique et les procédures de sécurité des informations.	☐	☐	☐	☐	☐
12.5.5	Surveiller et contrôler tous les accès aux données ?	▪ Examiner la politique et les procédures de sécurité des informations.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
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.	☐	☐	☐	☐	☐
	(b) Les procédures du programme de sensibilisation à la sécurité comprennent-elles ce qui suit :						
12.6.1	(a) Le programme de sensibilisation à la sécurité comprend-il plusieurs méthodes de sensibilisation et de formation du personnel (par exemple, affiches, lettres, mémos, formations sur le Web, réunions et promotions) ? ***Remarque :*** *Les méthodes varient selon les postes occupés et le niveau d'accès du personnel aux données de titulaires de carte.*	▪ Examiner le programme de sensibilisation à la sécurité. ▪ Examiner les procédures du programme de sensibilisation à la sécurité. ▪ Examiner les registres de participation au programme de sensibilisation à la sécurité.	☐	☐	☐	☐	☐
	(b) Le personnel est-il formé au moment du recrutement et au moins une fois par an ?	▪ Examiner les procédures et la documentation du programme de sensibilisation à la sécurité.	☐	☐	☐	☐	☐
	(c) Les employés ont-ils complété une formation de sensibilisation et sont-ils conscients de l'importance de la sécurité des données de titulaires de carte ?	▪ Interroger le personnel.	☐	☐	☐	☐	☐
12.6.2	Est-il exigé du personnel de reconnaître au moins une fois par an avoir lu et compris les procédures et la politique de sécurité ?	▪ Examiner les procédures et la documentation du 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.	Non testé
12.7	Les antécédents des employés potentiels (voir la définition du terme « employé » ci-dessus) sont-ils contrôlés avant leur recrutement afin de réduire les risques d'attaques par des sources internes ? *Ces contrôles devraient inclure, par exemple, les antécédents professionnels, le casier judiciaire, les renseignements de solvabilité et la vérification des références.* ***Remarque :** Pour le personnel dont l'embauche potentielle concerne des postes tels que celui de caissier dans un magasin, et qui n'a accès qu'à un numéro de carte à la fois à l'occasion du traitement d'une transaction, cette condition n'est qu'une recommandation.*	▪ Interroger la direction du département des ressources humaines.	☐	☐	☐	☐	☐
12.8	Des politiques et des procédures sont-elles maintenues et mises en œuvre pour gérer les prestataires de service avec lesquels les données de titulaires de carte sont partagées, ou qui sont susceptibles d'affecter la sécurité des données de titulaires de carte, comme suit :						
12.8.1	Est-ce qu'une liste des prestataires de services est conservée, y compris une description du ou des services fournis ?	▪ Examiner les politiques et les procédures. ▪ Observer les processus. ▪ Examiner la liste des prestataires de services.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
12.8.2	Un accord écrit est-il passé par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte ? ***Remarque :*** *La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.*	▪ Respecter les accords écrits. ▪ Examiner les politiques et les procédures.	☐	☐	☐	☐	☐
12.8.3	Existe-t-il un processus de sélection des prestataires de services, comprenant notamment des contrôles préalables à l'engagement ?	▪ Observer les processus. ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative.	☐	☐	☐	☐	☐
12.8.4	Existe-t-il un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an ?	▪ Observer les processus. ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative.	☐	☐	☐	☐	☐
12.8.5	Les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation sont-elles maintenues ?	▪ Observer les processus. ▪ Examiner les politiques et les procédures, ainsi que la documentation justificative.	☐	☐	☐	☐	☐
12.9	*Cette condition s'applique uniquement aux prestataires de services*.						

Question PCI DSS		Tests attendus	Réponse (Cocher une seule réponse pour chaque question)				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
12.10	Un plan de réponse aux incidents a-t-il été mis en place afin de répondre immédiatement à une faille du système, comme suit :						
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.	☐	☐	☐	☐	☐

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*				
			Oui	Oui, avec CCW	Non	S.O.	Non testé
12.10.2	Est-ce que le plan est révisé et testé au moins une fois par an, y compris les éléments répertoriés dans la condition 12.10.1 ?	▪ Examiner les procédures du plan de réponse aux incidents. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.10.3	Des membres spécifiques du personnel sont-ils désignés pour répondre aux alertes 24 heures sur 24 et sept jours sur sept ?	▪ Observer les processus. ▪ Examiner les politiques. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.10.4	Une formation appropriée est-elle fournie au personnel chargé de la réponse aux violations de la sécurité ?	▪ Observer les processus. ▪ Examiner les procédures du plan de réponse aux incidents. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.10.5	Est-ce que les alertes issues des systèmes de contrôle de sécurité sont incluses dans le plan de réponse aux incidents ?	▪ Observer les processus. ▪ Examiner les procédures du plan de réponse aux incidents.	☐	☐	☐	☐	☐
12.10.6	Un processus est-il conçu et déployé afin de modifier et développer le plan de réponse aux incidents en fonction des leçons apprises, et en tenant compte de l'évolution du secteur ?	▪ Observer les processus. ▪ Examiner les procédures du plan de réponse aux incidents. ▪ Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.11	*Cette condition s'applique uniquement aux prestataires de services.*						

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.	Non testé
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.	☐	☐	☐	☐	☐
A2.2	*Cette condition s'applique uniquement aux prestataires de services.*						
A2.3	*Cette condition s'applique uniquement aux prestataires de services.*						

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

Annexe D : Explication des conditions non testées

Si la colonne « Non testé » a été cochée dans le questionnaire, utiliser cette fiche de travail pour expliquer pourquoi la condition relative n'a pas été examinée dans le cadre de l'évaluation.

Condition	Décrire la ou les parties de la condition qui n'ont pas été testées	Décrire pourquoi les conditions n'ont pas été testées
Exemples :		
Condition 12	*La condition 12.2 est la seule condition testée. Toutes les autres conditions de la condition 12 ont été exclues.*	*Cette évaluation recouvre uniquement les conditions de l'étape importante 1 de l'approche prioritaire.*
Conditions 1-8, 10-12	*Seule la condition 9 a été examinée pour cette évaluation. Toutes les autres conditions ont été exclues.*	*La société est un fournisseur d'accès physique (CO-LO) et seuls les contrôles de sécurité physiques ont été pris en compte pour cette évaluation.*

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

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

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

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

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

Partie 3a. Reconnaissance du statut

Le ou les signataires confirment :

(Cocher toutes les mentions applicables)

☐	Le questionnaire d'auto-évaluation D PCI DSS, version *(numéro de version du SAQ)*, a été complété conformément aux instructions du document.
☐	Toutes les informations présentes dans le SAQ susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de mon évaluation à tous points de vue.
☐	J'ai vérifié auprès de mon fournisseur d'application de paiement que mon système de paiement ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme, ainsi qu'elle s'applique à mon environnement, à tout moment.
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.

Partie 3. Validation PCI DSS *(suite)*

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

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

Partie 3b. Attestation de commerçant

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

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

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

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

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

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

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

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

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

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

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

Vérifier auprès de la ou des marques de paiement applicables 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	☐	☐