Payment Card Industry
Standard de Sécurité des Données

Questionnaire d'Auto-Évaluation D pour les commerçants et Attestation de Conformité

À utiliser avec le PCI DSS Version 4.0.1

Date de Publication : Octobre 2024

REMERCIEMENTS : La version anglaise de ce document, telle que mise à disposition sur le site Internet du PCI SSC, à toutes fins, est considérée comme la version officielle de ces documents et, dans la mesure où il existe des ambiguïtés ou des incohérences entre la rédaction de ce texte et du texte anglais, la version anglaise disponible à l'endroit mentionné prévaudra.

Versions du Document

Date	PCI DSS Version	Révision du SAQ	Description
Octobre 2008	1.2		Aligner le contenu sur le nouveau standard PCI DSS v1.2 et mettre en œuvre les modifications mineures notées depuis la version initiale v1.1.
Octobre 2010	2.0		Aligner le contenu sur les nouvelles exigences et procédures de test de PCI DSS v2.0.
Février 2014	3.0		Aligner le contenu sur les exigences et les procédures de test du standard PCI DSS v3.0, et incorporer des options de réponse supplémentaires.
Avril 2015	3.1		Mise à jour pour s'aligner sur le PCI DSS v3.1. Pour plus de détails sur les modifications de PCI DSS, voir PCI DSS - Synthèse des modifications du Standard PCI DSS 3.0 à 3.1.
Juillet 2015	3.1	1.1	Mise à jour pour supprimer les références aux « meilleures pratiques » avant le 30 juin 2015 et suppression de l'option de signalement de PCI DSS v2 pour l'exigence 11.3.
Avril 2016	3.2	1.0	Mise à jour pour s'aligner sur le PCI DSS v3.2. Pour plus de détails sur les modifications de PCI DSS, voir PCI DSS - Synthèse des modifications du Standard PCI DSS 3.1 à 3.2.
Janvier 2017	3.2	1.1	Mise à jour de la numérotation des versions pour s'aligner sur les autres SAQ.
Juin 2018	3.2.1	1.0	Mise à jour pour s'aligner sur le PCI DSS v3.2.1. Pour plus de détails sur les modifications de PCI DSS, voir PCI DSS - Synthèse des modifications du Standard PCI DSS 3.2 à 3.2.1.
Avril 2022	4.0	1.0	Mise à jour pour s'aligner sur le PCI DSS v4.0. Pour plus de détails sur les modifications de PCI DSS, voir PCI DSS - Synthèse des modifications du Standard PCI DSS 3.2.1 à 4.0. Réorganisation, reformulation et développement des informations dans la section « Remplir le Questionnaire d'Auto-Évaluation » (précédemment intitulée « Avant de commencer »). Le contenu dans les sections 1 et 3 de l'Attestation de Conformité (AOC) aligné sur le Rapport de PCI DSS v4.0 sur la Conformité AOC. Ajout d'Annexes pour prendre en charge de nouvelles réponses de signalement.

Décembre 2022	4.0	1	Suppression de la mention « En place avec mesures correctives » comme option de rapport du tableau des réponses aux exigences, de la partie 2g de l'attestation de conformité (AOC), de la colonne de réponse de la section 2 du SAQ et de la section 3 de l'AOC. Suppression également de l'ancienne Annexe C. Ajout de la mention « En place avec CCW » à la section 3 de l'AOC. Ajout de directives pour répondre aux exigences futures. Ajout de clarifications mineures et correction d'erreurs typographiques.
Octobre 2024	4.0.1		Mise à jour pour s'aligner sur le PCI DSS v4.0.1. Pour plus de détails sur les modifications apportées au PCI DSS, veuillez consulter la section PCI DSS – Synthèse des modifications du Standard PCI DSS 4.0 à 4.0.1. Ajout du guide de ressources ASV à la section « Ressources PCI SSC supplémentaires ».

Sommaire

Remplir le Questionnaire d'Auto-Évaluation

Critères d'Éligibilité des Commerçants au Questionnaire d'Auto-Évaluation D

Le Questionnaire d'Auto-Évaluation (SAQ) D pour les commerçants s'applique aux commerçants qui sont éligibles à remplir un Questionnaire d'Auto-Évaluation mais qui ne répondent aux critères d'aucun autre type de SAQ. Des exemples d'environnements de commerçants auxquels le SAQ D peut s'appliquer comprennent, sans toutefois s'y limiter :

- Les commerçants e-commerce qui acceptent les données de compte sur leur site Web.
- Les commerçants avec stockage électronique des données de compte.
- Les commerçants qui ne stockent pas électroniquement les données de compte, mais qui ne répondent pas aux critères d'un autre type de SAQ.
- Les commerçants dont les environnements peuvent répondre aux critères d'un autre type de SAQ, mais qui ont des exigences supplémentaires du standard PCI DSS applicables à leur environnement.

Ce SAQ ne s'applique pas aux prestataires de services.

Définition des Données de Compte, des Données de Titulaires de Cartes et des Données d'Authentification Sensibles

Le standard PCI DSS est destiné à toutes les entités qui stockent, traitent ou transmettent des données de titulaires de cartes (CHD) et/ou des données d'authentification sensibles (SAD) ou qui pourraient avoir une incidence sur la sécurité de titulaires de cartes et/ou données d'authentification sensibles. Les données de titulaires de cartes et les données d'authentification sensibles sont considérées comme des données de compte et sont définies comme suit :

Données de Compte	
Les Données du Titulaires de Cartes Comprennent :	**Les Données d'Authentification Sensibles Comprennent :**
• Le Numéro de Compte Primaire (PAN) • Le Nom du Titulaire de Carte • La Date d'Expiration • Code de Service	• Les données de piste complète (données de la bande magnétique ou équivalent sur une puce) • Code de vérification de la carte • Blocs PINs/PIN

Se reporter à la section 2 du standard PCI DSS, *Informations sur l'Applicabilité du standard PCI DSS*, pour plus de détails.

Étapes de la Réalisation de l'Auto-Évaluation du Standard PCI DSS

1. Confirmer en examinant les critères d'éligibilité dans ce SAQ et le document *Instructions et des directives du Questionnaire d'Auto-Évaluation* sur le site Web du PCI SSC qu'il s'agit du bon SAQ pour l'environnement du commerçant.
2. Confirmer que l'environnement du commerçant est correctement défini.
3. Évaluer la conformité de l'environnement avec les exigences du standard PCI DSS.
4. Remplir toutes les sections de ce document :
   - Section 1 : Informations sur l'évaluation (Parties 1 et 2 de l'Attestation de Conformité (AOC) - Coordonnées et Synthèse).
   - Section 2 : Questionnaire d'Auto-Évaluation D pour les commerçants.
   - Section 3 : Détails de la Validation et de l'Attestation (parties 3 et 4 de l'AOC - Validation et Plan d'Action pour les Exigences Non Conformes du standard PCI DSS (si la partie 4 est applicable)).
5. Soumettre le SAQ et l'AOC, ainsi que toute autre documentation demandée, telle que les rapports d'analyse ASV, à l'organisation demandeuse (les organismes qui gèrent les programmes de conformité tels que les marques de paiement et les acquéreurs).

Tests Prévus

Les instructions fournies dans la colonne « Tests Prévus » sont basées sur les procédures de test du standard PCI DSS et fournissent une description de haut niveau des types d'activités de test qu'un commerçant est censé effectuer afin de vérifier qu'une exigence a été satisfaite.

L'intention derrière chaque méthode de test est décrite comme suit :

- Examiner : Le commerçant évalue de manière critique les justificatifs des données disponibles. Les exemples courants incluent les documents (électroniques ou physiques), les captures d'écran, les fichiers de configuration, les journaux d'audit et les fichiers de données.
- Observer : Le commerçant observe une action ou voit quelque chose dans l'environnement. Des exemples de sujets d'observation incluent le personnel effectuant une tâche ou un processus, les composants système exécutant une fonction ou répondant à une entrée, les conditions environnementales et les mesures de sécurité physiques.
- Interroger : Le commerçant s'entretient avec le personnel individuel. Les objectifs de l'entretien peuvent inclure la confirmation de l'exécution d'une activité, des descriptions de la manière dont une activité est exécutée et si le personnel a des connaissances ou une compréhension particulière.

Les méthodes de test sont destinées à permettre au commerçant de démontrer comment il a satisfait à une exigence. Les éléments spécifiques à examiner ou à observer et le personnel à interroger doivent être adaptés à la fois à l'exigence évaluée et à la mise en œuvre particulière du commerçant.

Les détails complets des procédures de test pour chaque exigence sont disponibles dans le standard PCI DSS.

Réponses aux Exigences

Pour chaque élément d'une exigence, il existe un choix de réponses pour indiquer le statut du commerçant par rapport à cette exigence. ***Seule une réponse doit être sélectionnée pour chaque élément de l'exigence.***

Une description de la signification de chaque réponse est fournie dans le tableau ci-dessous :

Réponse	Quand utiliser cette réponse :
En Place	Les tests prévus ont été effectués et tous les éléments de l'exigence ont été satisfaits comme indiqué.
En Place avec CCW (Feuille de Travail des Mesures de Sécurité Compensatoires)	Les tests prévus ont été effectués et l'exigence a été satisfaite avec l'aide d'une mesure de sécurité compensatoire. Toutes les réponses dans cette colonne nécessitent de remplir une Feuille de Travail des Mesures de Sécurité Compensatoires (CCW) à l'Annexe B de ce SAQ. Des informations sur l'utilisation des mesures compensatoires et des conseils sur la façon de remplir la feuille de travail sont fournies dans les Annexes A et B du standard PCI DSS.
Non Applicable	L'exigence ne s'applique pas à l'environnement du commerçant. (Voir « Directives pour les Exigences Non Applicables » ci-dessous pour des exemples.) Toutes les réponses dans cette colonne nécessitent une explication justificative dans l'Annexe C de ce SAQ.
Non Testé	L'exigence n'a pas été prise en considération dans l'évaluation et n'a été testée d'aucune façon. (Voir « Comprendre la différence entre Non Applicable et Non Testé » ci-dessous pour des exemples d'utilisation de cette option.) Toutes les réponses dans cette colonne nécessitent une explication justificative dans l'Annexe D de ce SAQ.
Pas en Place	Certains ou tous les éléments de l'exigence n'ont pas été satisfaits, ou sont en cours de mise en œuvre, ou nécessitent des tests supplémentaires avant que le commerçant puisse confirmer qu'ils sont En Place. Les réponses dans cette colonne peuvent nécessiter de remplir la partie 4, à la demande de l'entité à laquelle ce SAQ sera soumis. Cette réponse est également utilisée si une exigence ne peut être satisfaite en raison d'une restriction légale. (Voir « Exception Légale » ci-dessous pour plus d'informations).

Directives pour les Exigences Non Applicables

Alors que de nombreux commerçants remplissant le SAQ D devront valider la conformité à toutes les exigences du standard PCI DSS, certaines entités avec des modèles commerciaux très spécifiques peuvent constater que certaines exigences ne s'appliquent pas. Par exemple, les entités qui n'utilisent pas la technologie sans fil à quelque titre que ce soit ne sont pas tenues de se conformer aux exigences du standard PCI DSS spécifiques à la gestion de la technologie sans fil. De même, les entités qui ne stockent aucune donnée de compte par voie électronique à tout moment ne sont pas tenues de se conformer aux exigences du standard PCI DSS relatives au stockage sécurisé des données de compte (par exemple, l'exigence 3.5.1). Un autre exemple est les exigences spécifiques au développement d'applications et au codage sécurisé (par exemple, les exigences 6.2.1 à 6.2.4), qui s'appliquent uniquement à une entité avec un logiciel sur mesure (développé pour l'entité par un tiers conformément aux spécifications de l'entité) ou un logiciel personnalisé (développé par l'entité pour son propre usage).

Pour chaque réponse où l'option Non Applicable est sélectionnée dans ce SAQ, remplir l'Annexe C : *Explication des Exigences Indiquées comme Non Applicables.*

Comprendre la Différence entre Non Applicable et Non Testé

Les exigences jugées Non Applicables à un environnement doivent être vérifiées comme telles. En utilisant l'exemple de technologie sans fil ci-dessus, pour qu'un commerçant sélectionne « Non Applicable » pour les exigences 1.3.3, 2.3.1, 2.3.2 et 4.2.1.2, le commerçant doit d'abord confirmer qu'aucune technologie sans fil n'est utilisée dans son
environnement de données de titulaires de cartes (CDE) ou qui se connectent à son CDE. Une fois que cela a été confirmé, le commerçant peut sélectionner « Non Applicable » pour ces exigences spécifiques.

Si une exigence est complètement exclue de l'examen sans aucune considération quant à savoir si elle *pourrait* s'appliquer, l'option « Non Testé » doit être sélectionnée. Voici des exemples de situations où cela pourrait se produire :

- Un commerçant est invité par son acquéreur à valider un sous-ensemble d'exigences, par exemple, en utilisant l'approche prioritaire du standard PCI DSS pour valider uniquement certains jalons.
- Un commerçant confirme une nouvelle mesure de sécurité qui n'affecte qu'un sous-ensemble d'exigences, par exemple, la mise en œuvre d'une nouvelle méthodologie de chiffrement qui nécessite uniquement l'évaluation des exigences du standard PCI DSS 2, 3 et 4.

Dans ces scénarios, l'évaluation du commerçant ne comprend que certaines Exigences du standard PCI DSS même si d'autres exigences peuvent également s'appliquer à son environnement.

Si des exigences sont complètement exclues de l'auto-évaluation du commerçant, sélectionner Non Testé pour cette exigence spécifique et remplir l'Annexe D : Explication des exigences Non Testées pour chaque entrée « Non Testée ». Une évaluation avec des réponses Non Testées est une évaluation « partielle » du standard PCI DSS et sera notée comme telle par le commerçant dans l'Attestation de Conformité de la section 3, partie 3 de ce SAQ.

Directives pour répondre aux exigences futures

Dans la section 2 ci-dessous, chaque exigence ou note du PCI DSS avec une période de mise en œuvre prolongée comprend la note suivante : « Cette exigence [ou note] est une meilleure pratique jusqu'au 31 mars 2025, après quoi elle sera requise et doit être pleinement prise en compte lors d'une évaluation PCI DSS. »

Ces nouvelles exigences ne sont pas requises dans une évaluation PCI DSS tant que la date future n'est pas passée. Avant cette date future, toute exigence avec une date de mise en œuvre prolongée qui n'a pas été mise en œuvre par le commerçant peut être marquée comme non applicable et documentée à l'*annexe C : Explication des exigences notées comme non applicables.*

Exception Légale

Si votre organisation est soumise à une restriction légale qui l'empêche de répondre à une exigence du standard PCI DSS, sélectionner l'option Pas en Place pour cette exigence et remplir l'attestation pertinente dans la section 3, partie 3 de ce SAQ.

Remarque : *Une exception à une restriction légale est une restriction légale due à une loi, une réglementation ou une exigence réglementaire locale ou régionale, dans laquelle le respect d'une exigence PCI DSS violerait cette loi, cette réglementation ou cette exigence réglementaire.*

Les obligations contractuelles ou les conseils juridiques ne sont pas des restrictions légales.

Utilisation de l'Approche Personnalisée

L'utilisation de l'Approche Personnalisée n'est pas prise en charge dans les SAQ.

Les SAQ ne peuvent pas être utilisés pour documenter l'utilisation de l'Approche Personnalisée pour répondre aux exigences du standard PCI DSS. Pour cette raison, les objectifs de l'Approche Personnalisée ne sont pas inclus dans les SAQ. Les entités souhaitant valider à l'aide de l'Approche Personnalisée peuvent utiliser le modèle de Rapport de Conformité (ROC) au standard PCI DSS pour documenter les résultats de leur évaluation.

L'utilisation de l'Approche Personnalisée peut être réglementée par les organisations qui gèrent les programmes de conformité telles que, les marques de paiement et les acquéreurs. Les questions concernant l'utilisation d'une Approche Personnalisée doivent toujours être adressées à ces organisations. Cela inclut si une entité éligible à un SAQ peut plutôt remplir un ROC pour utiliser une Approche Personnalisée, et si une entité est tenue d'utiliser un QSA, ou peut utiliser une ISA, pour effectuer une évaluation utilisant l'Approche Personnalisée. Des informations concernant l'utilisation de l'Approche Personnalisée sont disponibles dans les Annexes D et E du standard PCI DSS.

Ressources Supplémentaires du PCI SSC

Des ressources supplémentaires qui fournissent des conseils sur les exigences du standard PCI DSS et sur la façon de remplir le Questionnaire d'Auto-Évaluation ont été fournies ci-dessous pour faciliter le processus d'évaluation.

Resource	Comporte :
Les Exigences et Procédures de Test du PCI Standard de Sécurité des Données (PCI DSS)	▪ Directives sur la Délimitation ▪ Directives sur l'intention de toutes les Exigences du Standard PCI DSS ▪ Détails des procédures de test ▪ Directives sur les Mesures Compensatoires ▪ Annexe G : Glossaire des Termes, Abréviations et Acronymes
Instructions et Directives concernant le SAQ	▪ Informations sur tous les SAQ et leurs critères d'éligibilité ▪ Comment déterminer le SAQ qui convient à votre organisation
Questions Fréquemment Posées (FAQ)	▪ Directives et informations concernant les SAQ.
Glossaire en ligne du standard PCI DSS	▪ Termes, Abréviations et Acronymes du Standard PCI DSS
Compléments d'Information et Directives	▪ Directives sur une variété de sujets liés au standard PCI DSS, notamment : – *Comprendre la Délimitation du Standard PCI DSS et la Segmentation du Réseau.* – *Assurance de Sécurité de Tiers* – *Directives Concernant l'Authentification à Plusieurs Facteurs* – *Meilleures Pratiques pour Maintenir la Conformité au Standard PCI DSS*
Guide de Démarrage avec la PCI	▪ Ressources pour les petits commerçants, notamment : – *Guide pour des Paiements Sécurisés* – *Systèmes de Paiement Courants* – *Questions à Poser à Vos Fournisseurs* – *Glossaire des Termes Relatifs au Paiement et à la Sécurité des Informations* – *Principes de base du pare-feu PCI* – *Guide de Ressources ASV*

Ces ressources et d'autres sont disponibles sur le site Web du PCI SSC *(www.pcisecuritystandards.org).*

Les organisations sont encouragées à consulter le standard PCI DSS et d'autres documents justificatifs avant de commencer une évaluation.

Section 1 : Informations Concernant l'Évaluation

Instructions Concernant la Soumission

Ce document doit être rempli comme déclaration des résultats de l'auto-évaluation du commerçant par rapport aux *exigences et aux procédures de test du Payment Card Industry Standard de Sécurité des Données (PCI DSS).* Remplir toutes les sections. Le commerçant est responsable de s'assurer que chaque section est remplie par les parties pertinentes, le cas échéant. Contacter l'entité ou les entités auxquelles l'Attestation de Conformité (AOC) sera soumise pour les procédures de rapport et de soumission.

Partie 1. Coordonnées	
Partie 1a. Commerçant Évalué	
Nom de l'Entreprise :	
DBA (exerçant ses activités sous le nom de) :	
Adresse postale de l'entreprise :	
Site principal de l'entreprise :	
Nom du Contact de l'Entreprise :	
Titre du contact de l'entreprise :	
Numéro de téléphone du contact :	
Adresse e-mail du contact :	
Partie 1b. Auditeur	
Fournir les informations suivantes pour tous les auditeurs impliqués dans l'évaluation. S'il n'y avait aucun auditeur pour un type d'auditeur donné, saisir Non Applicable.	
Auditeur(s) de Sécurité Interne du PCI SSC	
Nom(s) du ou des ISA :	
Auditeur de Sécurité Qualifié	
Nom de l'Entreprise :	
Adresse postale de l'entreprise :	
Site web de l'entreprise :	
Nom de l'Auditeur Principal :	
Numéro de téléphone de l'auditeur :	
Adresse e-mail de l'auditeur :	
Numéro de certificat de l'auditeur :	

Partie 2. Sommaire Exécutif

Partie 2a. Canaux de Paiement de l'Entreprise du Commerçant (sélectionner toutes les options qui s'appliquent) :

Indiquer tous les canaux de paiement utilisés par l'entreprise qui sont inclus dans cette évaluation.

☐ Commande par correspondance/par téléphone (MOTO)

☐ E-Commerce

☐ Avec carte

Y a-t-il des canaux de paiement non inclus dans cette évaluation ? Si oui, indiquer le ou les canaux qui ne sont pas inclus dans l'évaluation et expliquer brièvement pourquoi le canal a été exclu.	☐ Oui ☐ Non

Remarque : *Si l'organisation dispose d'un canal de paiement qui n'est pas couvert par ce SAQ, consulter la ou les entités auxquelles cet AOC sera soumis concernant la validation pour les autres canaux.*

Partie 2b. Description du Rôle avec les Cartes de Paiement

Pour chaque canal de paiement inclus dans cette évaluation et sélectionné dans la partie 2a ci-dessus, décrire la manière dont l'entreprise stocke, traite et/ou transmet les données de compte.

Canal	Comment l'Entreprise Stocke, Traite et/ou Transmet les Données de Compte

Partie 2c. Description de l'Environnement des Cartes de Paiement

Fournir une description de ***haut niveau*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions vers et depuis l'environnement de données de titulaire de carte (CDE).* • *Composants système critiques au sein du CDE, tels que les dispositifs POI, les bases de données, les serveurs Web, etc., et tout autre composant de paiement nécessaire, le cas échéant.* • *Composants système susceptibles d'avoir une incidence sur la sécurité des données de compte.*	
Indiquer si l'environnement inclut une segmentation pour réduire le périmètre de l'évaluation. *(Se reporter à la section « Segmentation » du standard PCI DSS afin d'obtenir des directives sur la segmentation.)*	☐ Oui ☐ Non

Partie 2. Sommaire Exécutif *(suite)*

Partie 2d. Emplacements/Installations dans le Périmètre

Énumérer tous les types d'emplacements/d'installations physiques (par exemple, les points de vente, les bureaux de l'entreprise, les centres de données, les centres d'appels et les salles de courrier) dans le périmètre de l'évaluation du standard PCI DSS.

Type d'Installation	**Nombre total d'emplacements** (Combien d'emplacements de ce type sont dans le périmètre)	**Emplacement(s) de l'installation (ville, pays)**
Par exemple : Centre de données	*3*	*Boston, MA, USA*

Partie 2e. Produits et Solutions Validés par le PCI SSC

Le commerçant utilise-t-il un élément identifié sur une liste du PCI SSC de produits et de solutions validés♦?

☐ Oui ☐ Non

Fournir les informations suivantes concernant chaque élément utilisé par le commerçant à partir des listes du PCI SSC de produits et de solutions validés.

Nom du Produit ou de la Solution validés par le PCI SSC	**Version du Produit ou de la Solution**	**Standard du PCI SSC selon lequel le produit ou la solution ont été validés**	**Numéro de référence de la liste du PCI SSC**	**Date d'expiration de la liste** (JJ-MM-AAAA)
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA
				JJ-MM-AAAA

♦ Aux fins de ce document, la « Listes de produits et solutions validés » désigne les listes de produits, solutions et/ou composants validés figurant sur le site Web du PCI SSC (www.pcisecuritystandards.org) par exemple, kits de développement logiciel 3DS, appareils PTS approuvés, logiciels de paiement validés, solutions de chiffrement point à point (P2PE), logiciels Entrée PIN sur les produits COTS (SPoC) et Paiements sans contact sur les solutions COTS (CPoC), et Paiements mobiles sur COTS (MPoC).

Partie 2. Sommaire Exécutif *(suite)*

Partie 2f. Prestataires de Services Tiers

L'entité entretient-elle des relations avec un ou plusieurs prestataires de services tiers qui :

• Stockent, traitent ou transmettent les données de compte au nom de l'entité (par exemple, les passerelles de paiement, les processeurs de paiement, les prestataires de services de paiement (PSP) et le stockage hors site).	☐ Oui ☐ Non
• Gèrent les composants système inclus dans le périmètre de l'évaluation de PCI DSS de l'entité– par exemple, via les services de mesures de sécurité du réseau, les services anti-malware, la gestion des incidents et des événements liés à la sécurité (SIEM), les centres de contact et d'appel, les services d'hébergement Web et les Fournisseurs de cloud IaaS, PaaS, SaaS et FaaS.	☐ Oui ☐ Non
• Pourraient avoir une incidence sur la sécurité du CDE de l'entité (par exemple, les prestataires fournissant une assistance via un accès à distance et/ou les développeurs de logiciels sur mesure)	☐ Oui ☐ Non

Si oui :

Nom du prestataire de services :	**Description du ou des services fournis :**

Remarque : *L'exigence 12.8 s'applique à toutes les entités dans cette liste.*

Partie 2. Sommaire Exécutif *(suite)*

Partie 2g. Synthèse de l'Évaluation

(SAQ - Section 2 et Annexes associées)

Indiquer ci-dessous toutes les réponses qui ont été sélectionnées pour chaque exigence du standard PCI DSS.

Exigence de PCI DSS*	Réponses aux Exigences *Plusieurs réponses peuvent être sélectionnées pour une exigence donnée. Indique toutes les réponses qui s'appliquent.*				
	En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
Exigence 1 :	☐	☐	☐	☐	☐
Exigence 2 :	☐	☐	☐	☐	☐
Exigence 3 :	☐	☐	☐	☐	☐
Exigence 4 :	☐	☐	☐	☐	☐
Exigence 5 :	☐	☐	☐	☐	☐
Exigence 6 :	☐	☐	☐	☐	☐
Exigence 7 :	☐	☐	☐	☐	☐
Exigence 8 :	☐	☐	☐	☐	☐
Exigence 9 :	☐	☐	☐	☐	☐
Exigence 10 :	☐	☐	☐	☐	☐
Exigence 11 :	☐	☐	☐	☐	☐
Exigence 12 :	☐	☐	☐	☐	☐
Annexe A2 :	☐	☐	☐	☐	☐

Section 2 : Questionnaire d'Auto-Évaluation D pour les Commerçants

Remarque : *Les exigences suivantes reflètent les exigences du document* Exigences et Procédures de Test du Standard PCI DSS.

Date d'achèvement de l'auto-évaluation : JJ-MM-AAAA

Créer et Maintenir un Réseau et des Systèmes Sécurisés

Exigence 1 : Installer et Maintenir des Mesures de Sécurité du Réseau

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.1 Les processus et mécanismes d'installation et de maintenance des mesures de sécurité du réseau sont définis et compris.							
1.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 1 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
1.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 1 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
1.2 Les mesures de sécurité réseau (NSC) sont configurés et maintenus.							
1.2.1	Les standards de configuration pour les ensembles de règles NSC sont : • Définis. • Mis en œuvre. • Maintenue.	• Examiner les standards de configuration. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.2.2	Toutes les modifications apportées aux connexions réseau et aux configurations des NSC sont approuvées et gérées conformément au processus de contrôle des modifications défini dans l'exigence 6.5.1.	• Examiner les procédures documentées. • Examiner les configurations du réseau. • Examiner les documents de contrôle des modifications. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité						
	Les modifications apportées aux connexions réseau comprennent l'ajout, la suppression ou la modification d'une connexion. Les modifications apportées aux configurations NSC comprennent celles liées au composant lui-même ainsi que celles affectant la manière dont il exécute sa fonction de sécurité.						
1.2.3	Un ou des schémas de réseau précis sont maintenus, montrant toutes les connexions entre le CDE et d'autres réseaux, y compris les réseaux sans fil.	• Examiner les schémas de réseau. • Examiner les configurations du réseau. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité						
	Un ou des schémas de réseau actuels ou une autre solution technique ou topologique qui identifie les connexions réseau et les périphériques peuvent être utilisés pour satisfaire à cette exigence.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.2.4	Un ou des diagrammes de flux de données précis sont maintenus et répondent aux critères suivants : • Affiche tous les flux de données de compte dans tous les systèmes et les réseaux. • Mis à jour au besoin lors de modifications apportées à l'environnement.	• Examiner les diagrammes de flux de données. • Observer les configurations du réseau. • Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Un ou des diagrammes de flux de données ou une autre solution technique ou topologique qui identifie les flux de données de compte à travers les systèmes et les réseaux peuvent être utilisés pour répondre à la présente exigence.						
1.2.5	Tous les services, protocoles et ports autorisés sont identifiés, approuvés et ont un besoin commercial défini.	• Examiner la documentation. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
1.2.6	Les fonctionnalités de sécurité sont définies et mises en œuvre pour tous les services, protocoles et ports utilisés et considérés comme non sécurisés, de sorte que le risque soit atténué.	• Examiner la documentation. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
1.2.7	Les configurations des NSC sont évaluées au moins une fois tous les six mois pour confirmer qu'elles sont pertinentes et efficaces.	• Examiner les procédures documentées. • Examiner la documentation des examens effectués. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.2.8	Les fichiers de configuration des NSC sont comme suit : • Sécurisés contre les accès non autorisés. • Maintenus cohérents avec les configurations de réseau actives.	• Examiner les fichiers de configuration des NSC.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Tout fichier ou paramètre utilisé pour configurer ou synchroniser les NSC est considéré « fichier de configuration ». Cela inclut les fichiers, les mesures automatisés et les mesures de sécurité basée sur le système, les scripts, les paramètres, l'infrastructure en tant que code ou d'autres paramètres qui sont sauvegardés, archivés ou stockés à distance.						
1.3 L'accès au réseau vers et depuis l'environnement de données du titulaire de carte est restreint.							
1.3.1	Le trafic entrant vers le CDE est limité comme suit : • Seul le trafic qui est nécessaire, • Tout autre trafic est spécifiquement refusé.	• Examiner les standards de configuration des NSC. • Examiner les configurations des NSC.	☐	☐	☐	☐	☐
1.3.2	Le trafic sortant du CDE est limité comme suit : • Seul le trafic qui est nécessaire. • Tout autre trafic est spécifiquement refusé.	• Examiner les standards de configuration des NSC. • Examiner les configurations des NSC.	☐	☐	☐	☐	☐
1.3.3	Les NSC sont installés entre tous les réseaux sans fil et le CDE, que le réseau sans fil soit ou non un CDE, de sorte que : • Tout le trafic sans fil allant des réseaux sans fil vers le CDE est refusé par défaut. • Seul le trafic sans fil à des fins commerciales autorisées est permis d'accéder au CDE.	• Examiner les paramètres de configuration. • Examiner les schémas de réseau	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.4 Les connexions réseau entre les réseaux de confiance et les réseaux non fiables sont contrôlées.							
1.4.1	Les NSC sont mis en œuvre entre les réseaux approuvés et les réseaux non fiables.	• Examiner les standards de configuration des NSC. • Examiner les schémas de réseau actuels • Examiner les configurations du réseau.	☐	☐	☐	☐	☐
1.4.2	Le trafic entrant des réseaux non fiables vers les réseaux de confiance est limité : • Aux communications avec des composants systèmes autorisés à fournir des services, des protocoles et des ports accessibles au public. • Aux réponses avec état aux communications initiées par les composants système dans un réseau de confiance. • Tout autre trafic est refusé.	• Examiner la documentation des NSC. • Examiner les configurations des NSC.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Le but de cette exigence est de traiter des sessions de communication entre les réseaux de confiance et les réseaux non fiables, plutôt que les spécificités des protocoles. Cette exigence ne limite pas l'utilisation du protocole UDP ou d'autres protocoles réseau en mode non connecté si l'état est maintenu par le NSC.						
1.4.3	Des mesures de détection d'usurpation sont mises en œuvre afin de détecter et empêcher les adresses IP sources falsifiées d'entrer dans le réseau de confiance.	• Examiner la documentation des NSC. • Examiner les configurations des NSC.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.4.4	Les composants système qui stockent les données des titulaires de cartes ne sont pas directement accessibles à partir de réseaux non fiables.	• Examiner le diagramme de flux de données et le schéma de réseau. • Examiner les configurations des NSC.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à être appliquée au stockage des données de compte dans la mémoire volatile, mais à être appliquée lorsque la mémoire est traitée comme un stockage persistant (par exemple, un disque virtuel). Les données de compte peuvent être stockées dans la mémoire volatile uniquement le temps nécessaire pour prendre en charge le processus commercial associé (par exemple, jusqu'à la fin de la transaction par carte de paiement associée).						
1.4.5	La divulgation des adresses IP internes et des informations de routage est limitée aux seules parties autorisées.	• Examiner les configurations des NSC. • Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
1.5 Les risques pour le CDE provenant d'appareils informatiques capables de se connecter à la fois à des réseaux non fiables et au CDE sont atténués.							
1.5.1	Des mesures de sécurité sont mises en œuvre sur tous les appareils informatiques, y compris les appareils appartenant à l'entreprise et aux employés, qui se connectent à la fois aux réseaux non fiables (y compris Internet) et au CDE, de la manière suivante. • Des paramètres de configuration spécifiques sont définis afin d'empêcher l'introduction de menaces dans le réseau de l'entité. • Les mesures de sécurité sont activées et en cours d'exécution. • Les mesures de sécurité ne sont pas modifiables par les utilisateurs des appareils informatiques, à moins qu'elles ne soient spécifiquement documentées et autorisées par la direction au cas par cas pour une période limitée.	• Examiner les politiques et les standards de configuration. • Examiner les paramètres de configuration des appareils.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Ces mesures de sécurité ne peuvent être temporairement désactivés que s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si ces mesures de sécurité doivent être désactivés dans un but précis, cette décision doit être formellement autorisée. Des mesures de sécurité supplémentaires peuvent également devoir être mises en œuvre pour la période pendant laquelle ces contrôles de sécurité ne sont pas actifs. Cette exigence s'applique aux appareils informatiques appartenant aux employés et à l'entreprise. Les systèmes qui ne peuvent pas être gérés par la politique de l'entreprise introduisent des faiblesses et offrent des opportunités que des individus malveillants peuvent exploiter.						

Exigence 2 : Appliquer des Configurations Sécurisées à Tous les Composants Système

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
2.1 Les processus et mécanismes d'application de configurations sécurisées à tous les composants système sont définis et compris.							
2.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 2 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
2.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 2 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
2.2 Les composants système sont configurés et gérés en toute sécurité.							
2.2.1	Les normes de configuration sont élaborées, mises en œuvre et maintenues pour : • Couvrir tous les composants système. • Corriger toutes les vulnérabilités de sécurité connues. • Se conformer aux normes relatives à la sécurité renforcée des systèmes agréés par l'industrie ou aux recommandations pour une sécurité renforcée des fournisseurs. • Être mises à jour à mesure que de nouveaux problèmes de vulnérabilité sont identifiés, comme défini dans l'exigence 6.3.1. • Être appliquées lorsque de nouveaux systèmes sont configurés et vérifiés comme étant En Place avant ou immédiatement après la connexion d'un composant système à un environnement de production.	• Examiner les standards relatifs à la configuration du système. • Examiner les normes de durcissement acceptées par l'industrie. • Examiner les paramètres de configuration. • Interroger le personnel.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
2.2.2	Les comptes par défaut du fournisseur sont gérés comme suit : • Si le ou les comptes par défaut du fournisseur sont utilisés, le mot de passe par défaut est modifié conformément à l'exigence 8.3.6. • Si le ou les comptes par défaut du fournisseur ne sont pas utilisés, le compte est supprimé ou désactivé.	• Examiner les standards relatifs à la configuration du système. • Examiner la documentation du fournisseur. • Observer un administrateur système se connectant à l'aide des comptes par défaut du fournisseur. • Examiner les fichiers de configuration. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cela s'applique à TOUS les comptes et mots de passe par défaut des fournisseurs, y compris, sans toutefois s'y limiter, ceux utilisés avec des valeurs par défaut par les systèmes d'exploitation, les logiciels qui fournissent des services de sécurité, les comptes d'application et système, les terminaux de point de vente (POS), les applications de paiement et le Protocole simplifié de gestion de réseau (SNMP). Cette exigence s'applique également lorsqu'un composant système n'est pas installé dans l'environnement d'une entité ; par exemple, des logiciels et des applications qui font partie du CDE et qui sont accessibles via un service d'abonnement cloud.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
2.2.3	Les fonctions principales nécessitant différents niveaux de sécurité sont gérées de la manière suivante : • Une seule fonction principale existe sur un composant système, **OU** • Les fonctions principales avec des niveaux de sécurité différents qui existent sur le même composant système sont isolées les unes des autres, **OU** • Les fonctions principales avec des niveaux de sécurité différents sur le même composant système sont toutes sécurisées au niveau exigé par la fonction ayant le besoin de sécurité le plus élevé.	• Examiner les standards relatifs à la configuration du système. • Examiner les configurations du système.	☐	☐	☐	☐	☐
2.2.4	Seuls les services, protocoles, démons et fonctions nécessaires sont activés et toutes les fonctionnalités inutiles sont supprimées ou désactivées.	• Examiner les standards relatifs à la configuration du système. • Examiner les configurations du système.	☐	☐	☐	☐	☐
2.2.5	Si des services, protocoles ou démons non sécurisés sont présents : • La justification commerciale est documentée. • Des fonctionnalités de sécurité supplémentaires sont documentées et mises en œuvre afin de réduire le risque d'utilisation de services, de protocoles ou de démons non sécurisés.	• Examiner les standards relatifs à la configuration. • Interroger le personnel. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
2.2.6	Les paramètres de sécurité du système sont configurés afin d'éviter toute utilisation abusive.	• Examiner les standards relatifs à la configuration du système. • Interroger le personnel. • Examiner les configurations du système.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
2.2.7	Tous les accès administratifs non-console sont cryptés à l'aide d'une cryptographie robuste.	• Examiner les standards relatifs à la configuration du système. • Observer le processus de connexion d'un administrateur. • Examiner les configurations du système. • Examiner la documentation du fournisseur. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité						
	Cela inclut l'accès administratif via des interfaces basées sur un navigateur et des interfaces de programmation d'applications (API).						
2.3 Les environnements sans fil sont configurés et gérés en toute sécurité.							
2.3.1	Pour les environnements sans fil connectés au CDE ou transmettant des données de compte, toutes les valeurs par défaut du fournisseur sans fil sont modifiées lors de l'installation ou sont confirmées comme étant sécurisées, y compris, sans toutefois s'y limiter : • Clés cryptographiques sans fil par défaut. • Mots de passe sur des points d'accès sans fil. • Valeurs SNMP par défaut. • Toute autre valeur par défaut du fournisseur sans fil liée à la sécurité.	• Examiner les politiques et les procédures. • Examiner la documentation du fournisseur. • Examiner les paramètres de configuration du réseau sans fil. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité						
	Cela inclut, sans toutefois s'y limiter, les clés cryptographiques sans fil par défaut, les mots de passe sur les points d'accès sans fil, les valeurs SNMP par défaut et toute autre valeur par défaut du fournisseur sans fil liée à la sécurité.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
2.3.2	Pour les environnements sans fil connectés au CDE ou transmettant des données de compte, les clés cryptographiques sans fil sont modifiées comme suit : • Chaque fois que le personnel connaissant la clé quitte l'entreprise ou le rôle pour lequel la connaissance de la clé était nécessaire. • Chaque fois qu'une clé est soupçonnée ou avérée être compromise.	• Examiner la documentation de la gestion des clés. • Interroger le personnel.	☐	☐	☐	☐	☐

Protéger les Données de Compte

Exigence 3 : Protéger les Données de Compte Stockées

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.1 Les processus et mécanismes de protection des données de compte stockées sont définis et compris.							
3.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 3 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
3.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 3 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.2 Le stockage des données de compte est réduit au minimum.							
3.2.1	Le stockage des données de compte est réduit au minimum grâce à la mise en œuvre de politiques, procédures et processus de conservation et d'élimination des données qui incluent au moins les éléments suivants : • Couverture de tous les emplacements des données de compte stockées. • Couverture de toutes les données d'authentification sensibles (SAD) stockées avant la fin de l'autorisation. *Ce point est une bonne pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes d'Applicabilité ci-dessous pour plus de détails.* • Limiter la quantité de stockage des données et la durée de conservation à ce qui est requis pour les exigences légales ou réglementaires et/ou commerciales. • Des exigences de rétention spécifiques pour les données de compte stockées qui définissent la durée de la période de conservation et incluent une justification commerciale documentée. • Des processus de suppression sécurisée ou rendre des données de compte irrécupérables lorsqu'elles ne sont plus nécessaires conformément à la politique de conservation. • Un processus pour vérifier, au moins une fois tous les trois mois, que les données de compte stockées dépassant la période de conservation définie ont été supprimées en toute sécurité ou rendues irrécupérables. *(suite)*	• Examiner les politiques, procédures et processus de rétention et de suppression des données. • Interroger le personnel. • Examiner les fichiers et les enregistrements système sur les composants système où les données de compte sont stockées. • Observer les mécanismes utilisés pour rendre les données de compte irrécupérables.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Lorsque les données de compte sont stockées par un TPSP (par exemple, dans un environnement cloud), les entités sont tenues de collaborer avec leurs prestataires de services afin de comprendre comment le TPSP satisfait à cette exigence pour l'entité. Les considérations incluent de s'assurer que toutes les instances géographiques d'un élément de données sont supprimées en toute sécurité. *La puce ci-dessus (concernant la couverture des SAD stockées avant l'achèvement de l'autorisation) est une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera requise dans le cadre de l'exigence 3.2.1 et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
3.3 Les données d'authentification sensibles (SAD) ne sont pas stockées après autorisation.							
3.3.1	Les SAD ne sont pas stockés après autorisation, même si elles sont cryptées. Toutes les données d'authentification sensibles reçues sont rendues irrécupérables à la fin du processus d'autorisation.	• Examiner les politiques et les procédures documentées. • Examiner les configurations du système. • Observer les processus sécurisés de suppression des données.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Une partie de cette note d'applicabilité a été supprimée intentionnellement pour ce SAQ, car elle ne s'applique pas aux évaluations des commerçants*. Les données d'authentification sensibles incluent les données citées dans les exigences 3.3.1.1 à 3.3.1.3.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.3.1.1	Le contenu complet d'une piste n'est pas stocké à la fin du processus d'autorisation.	• Examiner les sources de données.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Dans le cours normal des activités, les éléments de données suivants de la piste peuvent devoir être conservés : • Le Nom du Titulaire de Carte. • Le Numéro de Compte Primaire (PAN). • La Date d'Expiration. • Code de Service. Pour minimiser les risques, ne stocker en toute sécurité que ces éléments de données nécessaires à l'activité.						
3.3.1.2	Le code de vérification de la carte n'est pas stocké à la fin du processus d'autorisation.	• Examiner les sources de données.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Le code de vérification de la carte est le numéro à trois ou quatre chiffres imprimés au recto ou au verso d'une carte de paiement utilisée pour vérifier les transactions sans carte présente.						
3.3.1.3	Le numéro d'identification personnel (PIN) et le bloc PIN ne sont pas stockés à la fin du processus d'autorisation.	• Examiner les sources de données.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les blocs PIN sont cryptés au cours du déroulement naturel des processus de transaction ; cependant, même si une entité crypte à nouveau le bloc PIN, il n'est toujours pas autorisé à être stocké après l'achèvement du processus d'autorisation.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.3.2	Les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation sont cryptées à l'aide d'une cryptographie robuste.	• Examiner les entrepôts de données et les configurations système. • Examiner la documentation du fournisseur.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Que les SAD soient permises d'être stockées avant l'autorisation est déterminée par les entreprises qui gèrent les programmes de conformité (par exemple, les marques de paiement et les acquéreurs). Contacter ces entreprises pour tout critère supplémentaire. Cette exigence s'applique à tous les stockages de SAD, même si aucun PAN n'est présent dans l'environnement. Se reporter à l'exigence 3.2.1 pour une exigence supplémentaire qui s'applique si les SAD sont stockées avant l'achèvement de l'autorisation. *Une partie de cette note d'applicabilité a été supprimée intentionnellement pour ce SAQ, car elle ne s'applique pas aux évaluations des commerçants*. Cette exigence ne remplace pas la façon dont les blocs PIN doivent être gérés, ni ne signifie qu'un bloc PIN correctement crypté doit être à nouveau crypté. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
3.3.3	***Exigences supplémentaires pour les émetteurs et les entreprises qui prennent en charge les services d'émission et stockent les données d'authentification sensibles***						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.4 L'accès aux affichages du PAN complet et la possibilité de copier le PAN sont limités.							
3.4.1	Le PAN est masqué lorsqu'il est affiché (le BIN et les quatre derniers chiffres **sont le nombre maximum** de chiffres à afficher), de sorte que seul le personnel ayant un besoin métier légitime peut voir **plus que** le BIN et les quatre derniers chiffres du PAN.	• Examiner les politiques et les procédures documentées. • Examiner les configurations du système. • Examiner la liste documentée des rôles qui ont besoin d'accéder à plus que le BIN et les quatre derniers chiffres du PAN (y compris le PAN complet). • Examiner les affichages du PAN (par exemple, à l'écran, sur les reçus papier).	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence ne remplace pas les exigences plus strictes En Place pour l'affichage des données des titulaires de carte ; par exemple, les exigences légales ou de marques de paiement pour les reçus des points de vente (POS). Cette exigence concerne la protection du PAN lorsqu'il est affiché sur les écrans, les reçus papier, les impressions, etc., et ne doit pas être confondu avec l'exigence 3.5.1 pour la protection du PAN lorsqu'il est stocké, traité, ou transmis.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.4.2	Lors de l'utilisation de technologies d'accès à distance, les mesures techniques empêchent la copie et/ou la relocalisation du PAN pour tout le personnel, à l'exception de ceux disposant d'une autorisation explicite documentée et d'un besoin commercial légitime et défini.	• Examiner les politiques et procédures documentées et les preuves documentées des mesures techniques. • Examiner les configurations des technologies d'accès à distance. • Observer les processus. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Que le stockage ou le déplacement du PAN sur des disques durs locaux, des supports électroniques amovibles et d'autres périphériques de stockage permet à ces périphériques d'être dans le périmètre du standard PCI DSS. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.5 Le Numéro de Compte Primaire (PAN) est sécurisé partout où il est stocké.							
3.5.1	Le PAN est rendu illisible partout où il est stocké en utilisant l'une des approches suivantes : • Hachages à sens unique basés sur une cryptographie robuste de l'intégralité du PAN. • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN). – Si des versions hachées et tronquées du même PAN, ou des formats de troncature différents du même PAN, sont présentes dans un environnement, des mesures supplémentaires sont En Place afin que les différentes versions ne puissent pas être corrélées pour reconstruire le PAN d'origine • Tokens d'index. • Cryptographie robuste avec processus et procédures de gestion des clés associés.	• Examiner la documentation sur le système utilisé pour rendre le PAN illisible. • Examiner les référentiels de données. • Examiner les journaux d'audit, y compris les journaux d'applications de paiement. • Examiner les mesures de sécurité afin de vérifier que les PAN hachés et tronqués ne peuvent pas être corrélés pour reconstruire le PAN d'origine.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique aux PAN stockés dans le stockage principal (bases de données ou fichiers plats tels que des feuilles de calcul en fichiers texte) ainsi que le stockage non principal (sauvegarde, journaux d'audit, journaux des exceptions ou de dépannage). Cette exigence n'exclut pas l'utilisation de fichiers temporaires contenant un PAN en texte clair lors du cryptage et du décryptage du PAN.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.5.1.1	Les hachages utilisés pour rendre le PAN illisible (selon la première puce de l'exigence 3.5.1) sont des hachages cryptographiques de l'ensemble du PAN, avec les processus et procédures de gestion des clés associés conformément aux exigences 3.6 et 3.7.	• Examiner la documentation sur la méthode de hachage utilisée. • Examiner la documentation sur les procédures et processus de gestion des clés. • Examiner les référentiels de données. • Examiner les journaux d'audit, y compris les journaux d'applications de paiement.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Toutes les Note d'Applicabilité pour l'exigence 3.5.1 s'applique également à cette exigence. Les processus et procédures de gestion des clés (Exigences 3.6 et 3.7) ne s'appliquent pas aux composants systèmes utilisés pour générer des hachages à clé individuels d'un PAN pour comparer avec un autre système si : • Les composants système ont accès uniquement à une seule valeur de hachage à la fois (les valeurs de hachage ne sont pas stockées sur le système) **ET** • Il n'y a aucune autre donnée stockée sur le système sous forme de hachages. *Cette exigence est considérée une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS. Cette exigence remplacera la note de l'exigence 3.5.1 pour les hachages unidirectionnels une fois sa date d'entrée en vigueur atteinte.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.5.1.2	Si le chiffrement au niveau du disque ou au niveau de la partition (plutôt que le chiffrement de la base de données au niveau des fichiers, des colonnes ou des champs) est utilisé pour rendre le PAN illisible, il est mis en œuvre uniquement de la manière suivante : • Sur des supports électroniques amovibles. **OU** • S'il est utilisé sur des supports électroniques non amovibles, le PAN est également rendu illisible via un autre mécanisme qui satisfait à l'exigence 3.5.1.	• Observer les processus de chiffrement. • Examiner les configurations et/ou la documentation du fournisseur. • Observer les processus de chiffrement.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique à toutes les méthodes de chiffrement qui fournissent le PAN en teste clair automatiquement lorsqu'un système est exécuté, même si un utilisateur autorisé n'a pas spécifiquement demandé ces données. Bien que le chiffrement de disque ou de partition puisse toujours être présent sur ces types de périphériques, il ne peut pas être la seule méthode utilisée pour protéger le PAN stocké sur ces systèmes. Tout PAN stocké doit également être rendu illisible conformément à l'exigence 3.5.1 ; par exemple, via une troncature ou un mécanisme de chiffrement au niveau des données. Le chiffrement complet du disque aide à protéger les données en cas de perte physique d'un disque et, par conséquent, son utilisation n'est appropriée que pour les périphériques de stockage électroniques amovibles. Les supports faisant partie d'une architecture de centre de données (par exemple, les lecteurs remplaçables à chaud, les sauvegardes sur bande en masse) sont considérés comme des supports électroniques non amovibles auxquels l'exigence 3.5.1 s'applique. Les mises en œuvre de chiffrement de disques ou de partitions doivent également répondre à toutes les autres exigences de chiffrement et de gestion des clés du standard PCI DSS. *Une partie de cette Note d'Applicabilité a été intentionnellement supprimée pour ce SAQ car elle ne s'applique pas aux évaluations des commerçants.* *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.5.1.3	Si le chiffrement au niveau du disque ou au niveau de la partition est utilisé (plutôt que le chiffrement au niveau de la base de données, des fichiers, des colonnes ou des champs) afin de rendre le PAN illisible, il est géré de la manière suivante : • L'accès logique est géré séparément et indépendamment de l'authentification du système d'exploitation natif et des mécanismes de contrôle d'accès. • Les clés de déchiffrement ne sont pas associées aux comptes utilisateur. • Les facteurs d'authentification (mots de passe, phrases secrètes ou clés cryptographiques) qui permettent l'accès aux données non chiffrées sont stockés en toute sécurité.	• Examiner les configurations du système. • Observer le processus d'authentification. • Examiner les fichiers contenant les facteurs d'authentification. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les mises en œuvre de chiffrement de disques ou de partitions doivent également répondre à toutes les autres exigences de chiffrement et de gestion des clés du standard PCI DSS.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.6 Les clés cryptographiques utilisées pour protéger les données de compte stockées sont sécurisées.							
3.6.1	Des procédures sont définies et mises en œuvre afin de protéger les clés cryptographiques utilisées pour protéger les données de compte stockées contre la divulgation et l'utilisation abusive, notamment : • L'accès aux clés est limité au plus petit nombre d'opérateurs nécessaire. • Les clés de chiffrement des clés sont au moins aussi robustes que les clés cryptographiques des données qu'elles protègent. • Les clés de chiffrement des clés sont stockées séparément des clés cryptographiques de données. • Les clés sont stockées en toute sécurité dans le moins d'emplacements et de formes possibles.	• Examiner les politiques et les procédures documentées de la gestion des clés.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique aux clés utilisées pour protéger les données de compte stockées et aux clés de chiffrement utilisées pour protéger les clés cryptographiques des données. L'exigence de protéger les clés utilisées pour protéger les données de compte stockées contre la divulgation et l'utilisation abusive s'applique à la fois aux clés cryptographiques des données et aux clés de chiffrement des clés. Étant donné qu'une clé de chiffrement de clé peut accorder l'accès à de nombreuses clés cryptographiques de données, les clés de chiffrement de clés nécessitent des mesures de protection strictes.						
3.6.1.1	*Exigences supplémentaires pour les prestataires de services uniquement*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.6.1.2	Les clés secrètes et privées utilisées pour protéger les données de compte stockées sont conservées sous l'une (ou plusieurs) des formes suivantes à tout moment : • Chiffrée avec une clé de chiffrement de clé qui est au moins aussi robuste que la clé cryptographique des données, et qui est stockée séparément de la clé cryptographique des données. • Dans un dispositif cryptographique sécurisé (SCD), tel qu'un module de sécurité matérielle (HSM) ou un dispositif de point d'interaction approuvé PTS. • Sous forme d'au moins deux composants de clé ou de partages de clé de pleine longueur, conformément à une méthode acceptée par l'industrie.	• Examiner les procédures documentées. • Examiner les configurations système et les emplacements de stockage des clés, y compris les clés de déchiffrement des clés.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes. Les clés cryptographiques stockées dans le cadre d'un système de gestion des clés (KMS) qui utilise des SCD sont acceptables. Une clé cryptographique divisée en deux parties ne répond pas à cette exigence. Les clés secrètes ou privées stockées en tant que composants de clé ou partages de clé doivent être générées via l'une des méthodes suivantes : • À l'aide d'un générateur de chiffres aléatoires approuvé et au sein d'un SCD, **OU** • Selon ISO 19592 ou une norme industrielle équivalente pour la génération de partages de clés secrètes.						
3.6.1.3	L'accès aux composants de clé cryptographique en texte clair est limité au plus petit nombre d'opérateurs nécessaire.	• Examiner les listes d'accès des utilisateurs.	☐	☐	☐	☐	☐
3.6.1.4	Les clés cryptographiques sont stockées dans le moins d'emplacements possibles.	• Examiner les emplacements de stockage des clés. • Observer les processus.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.7 Lorsque la cryptographie est utilisée pour protéger les données de compte stockées, des processus et procédures de gestion des clés couvrant tous les aspects du cycle de vie des clés sont définis et mis en œuvre.							
3.7.1	Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la génération de clés cryptographiques robustes utilisées pour protéger les données de compte stockées.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Observer la méthode de génération des clés.	☐	☐	☐	☐	☐
3.7.2	Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la distribution de clés cryptographiques utilisées pour protéger les données de compte stockées.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Observer la méthode de distribution des clés.	☐	☐	☐	☐	☐
3.7.3	Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure le stockage de clés cryptographiques utilisées pour protéger les données de compte stockées.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Observer la méthode de stockage des clés.	☐	☐	☐	☐	☐
3.7.4	Les politiques et procédures de gestion des clés sont mises en œuvre pour les changements de clés cryptographiques pour les clés qui ont atteint la fin de leur cryptopériode, telles que définies par le fournisseur d'applications associé ou le propriétaire de la clé, et basées sur les meilleures pratiques et directives de l'industrie, y compris ce qui suit : • Une cryptopériode définie pour chaque type de clé utilisé. • Un processus pour les changements de clé à la fin de la cryptopériode définie.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Interroger le personnel. • Observer les emplacements de stockage des clés.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
3.7.5	Les procédures et politiques de gestion des clés sont mises en œuvre pour inclure le retrait, le remplacement ou la destruction des clés utilisées pour protéger les données de compte stockées, comme jugé nécessaire lorsque : • La clé a atteint la fin de sa cryptopériode définie. • L'intégrité de la clé a été affaiblie, notamment lorsque le personnel connaissant un composant de clé en texte clair quitte l'entreprise ou le rôle pour lequel le composant de clé était connu. • La clé est soupçonnée ou avérée être compromise. Les clés retirées ou remplacées ne sont pas utilisées pour les opérations de chiffrement.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Si des clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, à l'aide d'une clé de chiffrement de clé).						
3.7.6	Lorsque les opérations manuelles de gestion des clés cryptographiques en texte clair sont effectuées par le personnel, les politiques et procédures de gestion des clés sont mises en œuvre, notamment la gestion de ces opérations à l'aide du fractionnement des connaissances et du double contrôle. *(suite)*	• Examiner les politiques et les procédures documentées de la gestion des clés. • Interroger le personnel. • Observer les processus.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Cette mesure de sécurité s'applique aux opérations manuelles de gestion des clés. Une clé cryptographique simplement divisée en deux parties ne répond pas à cette exigence. Les clés secrètes ou privées stockées en tant que composants de clé ou partages de clé doivent être générées via l'une des méthodes suivantes : • L'utilisation d'un générateur de chiffres aléatoires approuvé et dans un dispositif cryptographique sécurisé (SCD), tel qu'un module de sécurité matérielle (HSM) ou un dispositif de point d'interaction approuvé PTS **OU** • Selon ISO 19592 ou une norme industrielle équivalente pour la génération de partages de clés secrètes.						
3.7.7	Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la prévention de la substitution non autorisée de clés cryptographiques.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Interroger le personnel. • Observer les processus.	☐	☐	☐	☐	☐
3.7.8	Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure que les opérateurs de clés cryptographiques reconnaissent formellement (par écrit ou par voie électronique) qu'ils comprennent et acceptent leurs responsabilités d'opérateurs de clés.	• Examiner les politiques et les procédures documentées de la gestion des clés. • Examiner la documentation ou d'autres justificatifs des confirmations des opérateurs des clés.	☐	☐	☐	☐	☐
3.7.9	*Exigences supplémentaires pour les prestataires de services uniquement*						

Exigence 4 : Protéger les Données des Titulaires de Cartes grâce à une Cryptographie Robuste lors de la Transmission sur des Réseaux Publics Ouverts

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
4.1 Des processus et des mécanismes de protection des données des titulaires de carte avec une cryptographie robuste lors de la transmission sur des réseaux publics ouverts, sont définis et compris.							
4.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 4 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
4.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 4 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
4.2 Le PAN est protégé par une cryptographie robuste pendant la transmission.							
4.2.1	Des protocoles de chiffrement et de sécurité robustes sont mis en œuvre comme suit afin de protéger le PAN pendant la transmission sur des réseaux publics ouverts :						
	• Seuls les clés et certificats de confiance sont acceptés.	• Examiner les politiques et les procédures documentées. • Interroger le personnel. • Examiner les configurations du système. • Examiner les transmissions des données de titulaire de carte. • Examiner les clés et les certificats.	☐	☐	☐	☐	☐
	• Les certificats utilisés pour protéger le PAN lors de la transmission sur des réseaux publics ouverts sont confirmés comme valides et ne sont ni expirés ni révoqués. *Ce point est une bonne pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes d'Applicabilité ci-dessous pour plus de détails.* *(suite)*		☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	• Le protocole utilisé ne prend en charge que les versions ou configurations sécurisées et ne prend pas en charge le basculement ou l'utilisation de versions, d'algorithmes, de tailles de clé ou de mises en œuvre non sécurisés.		☐	☐	☐	☐	☐
	• La force du chiffrement est adéquate pour la méthodologie de chiffrement utilisée.		☐	☐	☐	☐	☐
	Notes d'Applicabilité Un certificat auto-signé peut également être acceptable si le certificat est émis par une autorité de certification interne au sein de l'entreprise, que l'auteur du certificat est confirmé et que le certificat est vérifié (par exemple, par hachage ou signature) et qu'il n'a pas expiré. *La puce ci-dessus (pour confirmer que les certificats utilisés pour protéger le PAN pendant la transmission sur des réseaux publics ouverts sont valides et n'ont pas expiré ni été révoqués) est une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera requise dans le cadre de l'exigence 4.2.1. et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
4.2.1.1	Un inventaire des clés et des certificats approuvés de l'entité utilisés pour protéger le PAN pendant la transmission, est maintenu.	• Examiner les politiques et les procédures documentées. • Examiner l'inventaire des clés et des certificats fiables.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
4.2.1.2	Les réseaux sans fil transmettant le PAN ou connectés au CDE utilisent les meilleures pratiques de l'industrie pour mettre en œuvre une cryptographie robuste pour l'authentification et la transmission.	• Examiner les configurations du système.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
4.2.2	Le PAN est sécurisé avec une cryptographie robuste chaque fois qu'il est envoyé via les technologies de messagerie des utilisateurs finaux.	• Examiner les politiques et les procédures documentées. • Examiner les configurations du système et la documentation du fournisseur.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique également si un client, ou un autre tiers, demande que le PAN lui soit envoyé via les technologies de messagerie des utilisateurs finaux. Il peut arriver qu'une entité reçoive des données non sollicitées de titulaires de cartes via un canal de communication non sécurisé qui n'était pas destiné aux fins de recevoir des données sensibles. Dans cette situation, l'entité peut choisir soit d'inclure le canal dans le périmètre de son CDE et de le sécuriser conformément au standard PCI DSS, soit de supprimer les données du titulaire de carte et mettre en œuvre des mesures afin d'empêcher l'utilisation du canal pour les données de titulaires de cartes.						

Maintenir un Programme de Gestion des Vulnérabilités

Exigence 5 : Protéger Tous les Systèmes et Réseaux Contre les Logiciels Malveillants

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
5.1 Les processus et mécanismes de protection de tous les systèmes et réseaux contre les logiciels malveillants sont définis et compris.							
5.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 5 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
5.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 5 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
5.2 Les logiciels malveillants (malware) sont empêchés ou détectés et traités.							
5.2.1	Une ou plusieurs solutions anti-programmes malveillants sont déployées sur tous les composants système, à l'exception des composants systèmes identifiés dans les évaluations périodiques conformément à l'exigence 5.2.3 qui conclut que les composants système ne sont pas à risque de logiciels malveillants.	• Examiner les composants système. • Examiner les évaluations périodiques.	☐	☐	☐	☐	☐
5.2.2	La ou les solutions anti-programmes malveillants déployées : • Détecte tous les types connus de logiciels malveillants. • Supprime, bloque ou contient tous les types connus de logiciels malveillants.	• Examiner la documentation du fournisseur. • Examiner les configurations du système.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
5.2.3	Tous les composants système qui ne présentent pas de risque de logiciels malveillants sont évalués périodiquement pour inclure les éléments suivants : • Une liste documentée de tous les composants système ne présentant pas de risque de logiciels malveillants. • Identification et évaluation des menaces de logiciels malveillants en évolution pour ces composants système. • Confirmation indiquant si ces composants système continuent de ne pas nécessiter de protection anti-programmes malveillants.	• Examiner les politiques et les procédures documentées. • Interroger le personnel. • Examiner la liste des composants systèmes non exposés aux logiciels malveillants et les comparer aux composants système sans solution anti-programmes malveillants déployée.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les composants systèmes couverts par cette exigence sont ceux pour lesquels aucune solution anti-programmes malveillants n'est déployée conformément à l'exigence 5.2.1.						
5.2.3.1	La fréquence des évaluations périodiques des composants systèmes identifiés comme ne présentant pas de risque de logiciels malveillants est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1.	• Examiner l'analyse des risques ciblée. • Examiner les résultats documentés des évaluations périodiques. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
5.3 Les mécanismes et processus anti-programmes malveillants sont actifs, maintenus et surveillés.							
5.3.1	La ou les solutions anti-programmes malveillants sont tenues à jour via des mises à jour automatiques.	• Examiner les configurations de la ou des solutions anti-programmes malveillants, y compris toute installation originale. • Examiner les composants système et les journaux	☐	☐	☐	☐	☐
5.3.2	La ou les solutions anti-programmes malveillants : • Effectue des analyses périodiques et des analyses actives ou en temps réel. **OU** • Effectue une analyse comportementale continue des systèmes ou des processus.	• Examiner les configurations de la ou des solutions anti-programmes malveillants, y compris toute installation originale. • Examiner les composants système • Examiner les journaux et les résultats des analyses.	☐	☐	☐	☐	☐
5.3.2.1	Si des analyses périodiques de logiciels malveillants sont effectuées pour répondre à l'exigence 5.3.2, la fréquence des analyses est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.	• Examiner l'analyse des risques ciblée. • Examiner les résultats documentés analyses périodiques des logiciels malveillants. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique aux entités effectuant des analyses périodiques des logiciels malveillants pour satisfaire à l'exigence 5.3.2. Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
5.3.3	Pour les supports électroniques amovibles, la ou les solutions anti-programmes malveillants : • Effectue des analyses automatiques lorsque le support est inséré, connecté ou monté logiquement, **OU** • Effectue une analyse comportementale continue des systèmes ou des processus lorsque le support est inséré, connecté ou monté logiquement.	• Examiner les configurations de la ou des solutions anti-programmes malveillants. • Examiner les composants système avec des supports électroniques amovibles. • Examiner les journaux et les résultats des analyses.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
5.3.4	Les journaux d'audit pour la ou les solutions anti-programmes malveillants sont activés et conservés conformément à l'exigence 10.5.1.	• Examiner les configurations de la ou des solutions anti-programmes malveillants.	☐	☐	☐	☐	☐
5.3.5	Les mécanismes Anti-programmes malveillants ne peuvent pas être désactivés ou modifiés par les utilisateurs, à moins qu'ils ne soient spécifiquement documentés et autorisés par la direction au cas par cas pour une durée limitée dans le temps.	• Examiner les configurations anti-programmes malveillants. • Observer les processus. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les solutions anti-programmes malveillants ne peuvent être temporairement désactivés que s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la solution anti-programmes malveillants doit être désactivée dans un but précis, cette décision doit être formellement autorisée. Des mesures de sécurité supplémentaires peuvent également devoir être mises en œuvre pendant la période pendant laquelle la protection anti-programmes malveillants n'est pas active.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
5.4 Les mécanismes anti-hameçonnage protègent les utilisateurs contre les attaques par hameçonnage.							
5.4.1	Des processus et des mécanismes automatisés sont En Place pour détecter et protéger le personnel contre les attaques d'hameçonnage.	• Observer les processus mis en place. • Examiner les mécanismes.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'objectif de cette exigence est de protéger le personnel ayant accès aux composants système dans le périmètre du standard PCI DSS. Répondre à cette exigence de mesures techniques et automatisés pour détecter et protéger le personnel contre l'hameçonnage n'est pas la même chose que l'exigence 12.6.3.1 pour la formation de sensibilisation à la sécurité. Répondre à cette exigence ne répond pas non plus à l'exigence de fournir au personnel une formation de sensibilisation à la sécurité, et vice versa. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence 6 : Développer et Maintenir des Systèmes et des Logiciels Sécurisés

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.1 Les processus et mécanismes de développement et de maintenance de systèmes et de logiciels sécurisés sont définis et compris.							
6.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 6 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
6.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 6 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
6.2 Les logiciels sur mesure et personnalisés sont développés de manière sécurisée.							
6.2.1	Les logiciels sur mesure et personnalisés sont développés de manière sécurisée comme suit : • Sur la base des standards de l'industrie et/ou des meilleures pratiques pour un développement sécurisé. • Conformément au standard PCI DSS (par exemple, authentification et journalisation sécurisées). • Intégration de la prise en compte des problèmes de sécurité de l'information à chaque étape du cycle de vie du développement logiciel.	• Examiner les procédures documentées de développement de logiciels.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cela s'applique à tous les logiciels développés pour ou par l'entité pour son propre usage. Cela inclut des logiciels à la fois sur mesure et personnalisés. Ceci ne s'applique pas aux logiciels tiers.						

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.2.2	Le personnel développeur de logiciels travaillant sur des logiciels sur mesure et personnalisés est formé au moins une fois tous les 12 mois comme suit : • Sur la sécurité des logiciels en rapport avec leur fonction et leurs langages de développement. • Inclure la conception de logiciels sécurisés et les techniques de codage sécurisé. • Inclure, si des outils de test de sécurité sont utilisés, la manière d'utiliser les outils pour détecter les vulnérabilités dans les logiciels.	• Examiner les procédures documentées de développement de logiciels. • Examiner les dossiers de formation. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Le personnel développeur de logiciels reste informé des pratiques de développement sécurisé ; de la sécurité des logiciels ; et des attaques contre les langages, les frameworks ou les applications qu'ils développent. Le personnel peut accéder à une assistance et à des conseils en cas de besoin.						
6.2.3	Les logiciels sur mesure et personnalisés sont examinés avant d'être mis en production ou envoyés aux clients, afin d'identifier et de corriger les vulnérabilités de codage potentielles, comme suit : • Les examens de code garantissent que le code est développé conformément aux directives de codage sécurisé. • Les examens de code recherchent les vulnérabilités logicielles existantes et émergentes. • Des corrections appropriées sont mises en œuvre avant la publication. (suite)	• Examiner les procédures documentées de développement de logiciels. • Interroger le personnel responsable. • Examiner les preuves de modifications apportées aux logiciels sur mesure et personnalisés.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Cette exigence d'examen de code s'applique à tous les logiciels sur mesure et personnalisés (à la fois internes et publics), dans le cadre du cycle de vie du développement système. Les applications Web accessibles au public sont également soumises à des mesures supplémentaires, afin de faire face aux menaces et vulnérabilités en cours après la mise en œuvre, comme défini dans l'exigence 6.4 du standard PCI DSS. Les examens de code peuvent être effectués à l'aide de processus manuels ou automatisés, ou d'une combinaison des deux.						
6.2.3.1	Si des examens manuels du code sont effectués sur des logiciels sur mesure et personnalisés avant la mise en production, les modifications de code sont : • Examinées par des personnes autres que l'auteur du code d'origine, et qui connaissent les techniques d'examen du code et les pratiques de codage sécurisé. • Examinées et approuvées par la direction avant la publication.	• Examiner les procédures documentées de développement de logiciels. • Interroger le personnel responsable. • Examiner les preuves de modifications apportées aux logiciels sur mesure et personnalisés.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les examens manuels du code peuvent être effectués par du personnel interne compétent ou par du personnel tiers compétent. Un utilisateur à qui la responsabilité du contrôle des versions a été officiellement confiée et qui n'est ni l'auteur du code d'origine ni l'examinateur du code remplit les critères de gestion.						
6.2.4	Des techniques d'ingénierie logicielle ou d'autres méthodes sont définies et utilisées par le personnel de développement de logiciels afin de prévenir ou d'atténuer les attaques logicielles courantes et les vulnérabilités associées dans les logiciels sur mesure et personnalisés, y compris, sans toutefois s'y limiter :						
	• Attaques par injection, y compris SQL, LDAP, XPath ou d'autres failles de type commande, paramètre, objet, erreur ou injection. *(suite)*	• Examiner les procédures documentées.	☐	☐	☐	☐	☐

Exigence de PCI DSS	Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
		En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
• Attaques ciblant les données et les structures de données, y compris les tentatives de manipulation de tampons, de pointeurs, de données d'entrée ou de données partagées.	• Interroger le personnel responsable du développement logiciel.	☐	☐	☐	☐	☐
• Attaques ciblant l'utilisation de la cryptographie, y compris les tentatives d'exploitation d'implémentations cryptographiques, d'algorithmes, de suites de chiffrement ou de modes de fonctionnement faibles, non sécurisés ou inadéquats.		☐	☐	☐	☐	☐
• Attaques contre la logique métier, y compris les tentatives d'abus ou de contournement des caractéristiques et fonctionnalités des applications via la manipulation d'API, de protocoles et de canaux de communication, de fonctionnalités côté client ou d'autres fonctions et ressources du système ou de l'application. Cela comprend les scripts de site à site (XSS) et les altérations de requêtes de site à site (CSRF).		☐	☐	☐	☐	☐
• Attaques contre les mécanismes de contrôle d'accès, y compris les tentatives de contourner ou d'abuser de l'identification, de l'authentification ou des mécanismes d'autorisation, ou des tentatives d'exploiter les faiblesses de la mise en œuvre de ces mécanismes.		☐	☐	☐	☐	☐
• Attaques via toutes les vulnérabilités « à haut risque » identifiées dans le processus d'identification des vulnérabilités, telles qu'elles sont définies dans l'exigence 6.3.1.		☐	☐	☐	☐	☐
Notes d'Applicabilité						
Cela s'applique à tous les logiciels développés pour ou par l'entité pour son propre usage. Cela inclut des logiciels à la fois sur mesure et personnalisés. Ceci ne s'applique pas aux logiciels tiers.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.3 Les vulnérabilités de sécurité sont identifiées et corrigées.							
6.3.1	Les vulnérabilités de sécurité sont identifiées et gérées de la manière suivante : • Les nouvelles vulnérabilités de sécurité sont identifiées à l'aide de sources reconnues par l'industrie pour les informations sur les vulnérabilités de sécurité, y compris les alertes des équipes internationales et nationales d'intervention en cas d'urgence informatique (CERT). • Les vulnérabilités se voient attribuer un classement de risques basé sur les meilleures pratiques de l'industrie et la prise en compte de l'incidence potentielle. • Les classements des risques identifient, au minimum, toutes les vulnérabilités considérées comme à haut risque ou critiques pour l'environnement. • Les vulnérabilités des logiciels sur mesure et personnalisés et des logiciels de tiers (par exemple les systèmes d'exploitation et les bases de données) sont couvertes.	• Examiner les politiques et les procédures. • Interroger le personnel responsable. • Examiner la documentation. • Observer les processus.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas satisfaite par, et s'ajoute à l'exécution des analyses des vulnérabilités conformément aux exigences 11.3.1 et 11.3.2. Cette exigence vise un processus visant la surveillance active des sources de l'industrie pour les informations sur les vulnérabilités et pour que l'entité détermine la catégorisation des risques à associer à chaque vulnérabilité.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.3.2	Un inventaire des logiciels sur mesure et personnalisés et des composants logiciels tiers intégrés dans des logiciels sur mesure et personnalisés est conservé afin de faciliter la gestion des vulnérabilités et des correctifs.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
6.3.3	Tous les composants système sont protégés contre les vulnérabilités connues en installant les correctifs/mises à jour de sécurité applicables comme suit : • Les correctifs/mises à jour pour des vulnérabilités critiques (identifiés selon le processus de classement des risques énoncé à l'exigence 6.3.1) sont installés dans le mois suivant leur publication. • Tous les autres correctifs/mises à jour de sécurité applicables sont installés dans un délai approprié déterminé par l'évaluation par l'entité de la criticité du risque à l'environnement tel qu'identifié selon le processus de classification des risques dans l'Exigence 6.3.1.	• Examiner les politiques et les procédures. • Examiner les composants système et les logiciels connexes. • Comparer la liste des correctifs de sécurité installés aux listes de correctifs récents des fournisseurs.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.4 Les applications Web destinées au public sont protégées contre les attaques.							
6.4.1	Pour les applications Web destinées au public, les nouvelles menaces et vulnérabilités sont traitées en permanence, et ces applications sont protégées contre les attaques connues comme suit : • Examiner les applications Web accessibles au public grâce à des outils ou des méthodes manuels ou automatisés d'évaluation des vulnérabilités des applications, comme suit : – Au moins une fois tous les 12 mois et après des modifications importantes. – Par une entité spécialisée dans la sécurité des applications. – Y compris, au minimum, toutes les attaques logicielles courantes énoncées dans l'exigence 6.2.4. – Toutes les vulnérabilités sont classées conformément à l'exigence 6.3.1. – Toutes les vulnérabilités sont corrigées. – L'application est réévaluée après les corrections **OU** • L'installation d'une ou plusieurs solutions techniques automatisées qui détectent et empêchent en permanence les attaques basées sur le Web, comme suit : – Installé devant les applications Web destinées au public afin de détecter et empêcher les attaques Web. – En exécution active et à jour, le cas échéant. – Génération de journaux d'audit. – Configurée pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée. *(suite)*	• Examiner les processus documentés. • Interroger le personnel. • Examiner les enregistrements des évaluations de la sécurité des applications • Examiner les paramètres de configuration du système et les journaux d'audit.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Cette évaluation n'est pas la même que les analyses de vulnérabilité effectuées pour les exigences 11.3.1 et 11.3.2. Cette exigence sera remplacée par l'exigence 6.4.2 après le 31 mars 2025 lorsque l'exigence 6.4.2 entrera en vigueur.						
6.4.2	Pour les applications Web destinées au public, une solution technique automatisée est déployée qui détecte et empêche en permanence les attaques Web, avec au moins les éléments suivants : • Est installée devant les applications Web destinées au public et configurée afin de détecter et empêcher les attaques Web. • En exécution active et à jour, le cas échéant. • Génération de journaux d'audit. • Configurée pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée.	• Examiner les paramètres de la configuration du système. • Examiner les journaux d'audit. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette nouvelle exigence remplacera l'exigence 6.4.1 une fois sa date d'entrée en vigueur atteinte. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.4.3	Tous les scripts de la page de paiement qui sont chargés et exécutés dans le navigateur du client sont gérés comme suit :						
	• Une méthode est mise en œuvre pour confirmer que chaque script est autorisé.	• Examiner les politiques et les procédures. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	• Une méthode est mise en œuvre pour assurer l'intégrité de chaque script.		☐	☐	☐	☐	☐
	• Un inventaire de tous les scripts est maintenu avec une justification commerciale ou technique écrite expliquant pourquoi chacun est nécessaire.	• Examiner les registres d'inventaire. • Examiner les configurations du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique à tous les scripts chargés à partir de l'environnement de l'entité et aux scripts chargés à partir de tiers et de quatrièmes parties. Cette exigence s'applique également aux scripts présents dans la ou les pages Web de l'entité qui incluent la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un ou plusieurs cadres en ligne ou iframes). Cette exigence ne s'applique pas à une entité pour les scripts dans la page/formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, une ou plusieurs iframes), lorsque l'entité inclut la page/formulaire de paiement d'un TPSP/processeur de paiement sur sa page Web. Il incombe au TPSP/processeur de paiement de gérer les scripts dans la page/le formulaire de paiement intégré du TPSP/processeur de paiement conformément à cette exigence. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.5 Les modifications apportées à tous les composants système sont gérées de manière sécurisée.							
6.5.1	Les modifications apportées à tous les composants système dans l'environnement de production sont effectuées conformément aux procédures établies qui comportent : • Raison et description du changement. • Documentation de l'impact sur la sécurité. • Approbation des changements documentée par les parties autorisées. • Tests pour vérifier que le changement n'a pas d'incidence négative sur la sécurité du système. • Pour les changements apportés aux logiciels sur mesure et personnalisés, toutes les mises à jour sont testées afin de vérifier leur conformité à l'exigence 6.2.4 avant d'être déployées en production. • Procédures pour la résolution des défaillances et le retour à un état sécurisé.	• Examiner les procédures documentées de contrôle des modifications. • Examiner les modifications récentes apportées aux composants système et retracer les modifications jusqu'à la documentation de contrôle des modifications. • Examiner les documents de contrôle des modifications.	☐	☐	☐	☐	☐
6.5.2	À la fin de modifications importantes, toutes les exigences applicables du standard PCI DSS sont confirmées être En Place sur tous les systèmes et réseaux nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant.	• Examiner la documentation pour les modifications importantes. • Interroger le personnel. • Observer les systèmes/réseaux touchés.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Ces modifications importantes doivent également être capturées et reflétées dans l'activité annuelle de confirmation du périmètre du standard PCI DSS de l'entité conformément à l'exigence 12.5.2.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.5.3	Les environnements de pré-production sont séparés des environnements de production et la séparation est appliquée avec des contrôles d'accès.	• Examiner les politiques et les procédures. • Examiner la documentation du réseau et les configurations des mesures de sécurité du réseau. • Examiner les paramètres de contrôle d'accès.	☐	☐	☐	☐	☐
6.5.4	Les rôles et les fonctions sont séparés entre les environnements de production et de pré-production afin d'assurer la responsabilité de sorte que seules les modifications examinées et approuvées soient déployées.	• Examiner les politiques et les procédures. • Observer les processus. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Dans les environnements avec un personnel limité où les individus remplissent plusieurs rôles ou fonctions, ce même objectif peut être atteint avec des mesures procéduraux supplémentaires qui garantissent la responsabilité. Par exemple, un développeur peut également être un administrateur qui utilise un compte de niveau administrateur avec des privilèges élevés dans l'environnement de développement ; et, pour son rôle de développeur, il utilise un compte distinct avec un accès de niveau utilisateur dans l'environnement de production.						
6.5.5	Les PAN actifs ne sont pas utilisés dans les environnements de pré-production, sauf lorsque ces environnements sont inclus dans le CDE et protégés conformément à toutes les exigences applicables du standard PCI DSS.	• Examiner les politiques et les procédures. • Observer les processus de test. • Interroger le personnel. • Examiner les données des tests de pré-production.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
6.5.6	Les données de test et les comptes de test sont supprimés des composants système avant que le système ne passe en production.	• Examiner les politiques et les procédures. • Observer les processus de test pour les logiciels prêts à l'emploi et les applications internes. • Interroger le personnel. • Examiner les données et les comptes des logiciels et des applications internes récemment installés ou mis à jour.	☐	☐	☐	☐	☐

Mettre en Œuvre des Mesures Robustes de Contrôle d'Accès

Exigence 7 : Limiter l'Accès aux Composants Système et aux Données des Titulaires de Cartes en Fonction des Besoins de l'Entreprise

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
7.1 Les processus et les mécanismes de restriction de l'accès aux composants système et aux données des titulaires de cartes par l'entreprise doivent être définis et compris.							
7.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 7 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
7.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 7 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
7.2 L'accès aux composants système et aux données du système est défini et attribué de manière adéquate.							
7.2.1	Un modèle de contrôle d'accès est défini et inclut l'octroi d'accès comme suit : • Accès approprié en fonction de l'activité de l'entité et des besoins d'accès. • Accès aux composants système et aux ressources de données en fonction de la classification et des fonctions des utilisateurs. • Les moindres privilèges requis (par exemple, utilisateur, administrateur) pour exécuter une fonction.	• Examiner les politiques et les procédures documentées. • Interroger le personnel. • Examiner les paramètres de contrôle d'accès.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
7.2.2	L'accès est attribué aux utilisateurs, y compris les utilisateurs privilégiés, selon : • La classification du poste et de la fonction. • Les moindres privilèges nécessaires pour exercer les responsabilités du poste.	• Examiner les politiques et les procédures. • Examiner les paramètres d'accès des utilisateurs, y compris pour les utilisateurs privilégiés. • Interroger le personnel de direction responsable. • Interroger le personnel responsable de l'attribution de l'accès.	☐	☐	☐	☐	☐
7.2.3	Les privilèges requis sont approuvés par un personnel autorisé.	• Examiner les politiques et les procédures. • Examiner les identifiants des utilisateurs et les privilèges qui leur sont attribués. • Examiner les approbations documentées.	☐	☐	☐	☐	☐
7.2.4	Tous les comptes et les privilèges d'accès associés, y compris les comptes tiers/fournisseurs, sont examinés comme suit : • Au moins une fois tous les six mois. • Pour garantir que les comptes d'utilisateurs et l'accès restent appropriés selon la fonction du poste. • Tout accès inapproprié est traité. • La direction reconnaît que l'accès demeure approprié. *(suite)*	• Examiner les politiques et les procédures. • Interroger le personnel responsable. • Examiner les résultats documentés des examens périodiques des comptes d'utilisateurs.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Cette exigence s'applique à tous les comptes d'utilisateurs et les privilèges associés, y compris ceux utilisés par le personnel et les tiers/fournisseurs, et les comptes utilisés pour accéder aux services cloud de tiers. Voir les exigences 7.2.5 et 7.2.5.1 et 8.6.1 à 8.6.3 pour les mesures de sécurité des comptes d'application et système. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
7.2.5	Tous les comptes d'applications et système et les privilèges d'accès associés sont attribués et gérés comme suit : • Basés sur les moindres privilèges nécessaires à l'opérabilité du système ou de l'application. • L'accès est limité aux systèmes, applications ou processus qui nécessitent spécifiquement leur utilisation.	• Examiner les politiques et les procédures. • Examiner les privilèges associés aux comptes système et d'applications. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
7.2.5.1	Tous les accès par comptes d'applications et système et les privilèges d'accès associés sont examinés comme suit : • Périodiquement, (à la fréquence définie dans l'analyse des risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1). • L'accès à l'application ou au système reste approprié pour la fonction exécutée. • Tout accès inapproprié est traité. • La direction reconnaît que l'accès demeure approprié.	• Examiner les politiques et les procédures. • Examiner l'analyse des risques ciblée. • Interroger le personnel responsable. • Examiner les résultats documentés des examens périodiques des comptes système et d'application et des privilèges associés.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
7.2.6	Tout accès utilisateur pour envoyer aux référentiels des requêtes de données de titulaires de cartes stockées est limité comme suit : • Via des applications ou d'autres méthodes de programmation, avec accès et actions autorisées en fonction des rôles d'utilisateur et des moindres privilèges. • Seuls les administrateurs responsables peuvent accéder directement ou envoyer des requêtes aux référentiels de CHD stockés.	• Examiner les politiques et les procédures. • Interroger le personnel. • Examiner les paramètres de configuration pour interroger les référentiels de données de titulaires de cartes stockées.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique aux contrôles d'accès des utilisateurs aux référentiels de requêtes de données de titulaires de cartes stockées. Voir les exigences 7.2.5 et 7.2.5.1 et 8.6.1 à 8.6.3 pour les mesures de sécurité des comptes d'application et système.						

Exigence de PCI DSS		Tests Prévus	Réponse♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
7.3 L'accès aux composants système et aux données est géré via un ou plusieurs systèmes de contrôle d'accès.							
7.3.1	Un ou plusieurs systèmes de contrôle d'accès sont En Place qui limitent l'accès en fonction du besoin de connaître de l'utilisateur et couvrent tous les composants système.	• Examiner la documentation du fournisseur. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
7.3.2	Le ou les systèmes de contrôle d'accès sont configurés pour appliquer les autorisations attribuées aux personnes, aux applications et aux systèmes sur la base de la classification et la fonction des tâches.	• Examiner la documentation du fournisseur. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐
7.3.3	Le ou les systèmes de contrôle d'accès sont définis par défaut pour « refuser tout le monde ».	• Examiner la documentation du fournisseur. • Examiner les paramètres de configuration.	☐	☐	☐	☐	☐

Exigence 8 : Identifier les Utilisateurs et Authentifier l'Accès aux Composants Système

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.1 Les processus et mécanismes d'identification des utilisateurs et d'authentification de l'accès aux composants système sont définis et compris.							
8.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 8 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
8.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 8 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
8.2 L'identification des utilisateurs et les comptes associés pour les utilisateurs et les administrateurs sont strictement gérés tout au long du cycle de vie d'un compte.							
8.2.1	Tous les utilisateurs reçoivent un identifiant unique avant que l'accès aux composants système ou aux données des titulaires de cartes ne soit autorisé.	• Interroger le personnel responsable. • Examiner les journaux d'audit et autres preuves.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction.						

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.2.2	Les identifiants de groupe, partagés ou génériques, ou d'autres « credentials d'authentification » partagés ne sont utilisés que si nécessaire sur une base exceptionnelle et sont gérés comme suit : • L'utilisation des identifiants est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles. • L'utilisation est limitée au temps nécessaire à la circonstance exceptionnelle. • La justification commerciale de l'utilisation est documentée. • L'utilisation est explicitement approuvée par la direction. • L'identité de l'utilisateur individuel est confirmée avant que l'accès à un compte ne soit accordé. • Chaque action entreprise est attribuable à un seul utilisateur.	• Examiner les listes des comptes d'utilisateurs sur les composants système et la documentation applicable. • Examiner les politiques et procédures d'authentification. • Interroger les administrateurs système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction.						
8.2.3	***Exigences supplémentaires pour les prestataires de services uniquement***						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.2.4	L'ajout, la suppression et la modification des identifiants utilisateur, des facteurs d'authentification et d'autres objets identifiants sont gérés comme suit : • Autorisés avec l'approbation appropriée. • Mis en œuvre avec uniquement les privilèges spécifiés sur l'approbation documentée.	• Examiner les autorisations documentées à travers les différentes phases du cycle de vie du compte (ajouts, modifications et suppressions). • Examiner les paramètres système	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique à tous les comptes d'utilisateurs, y compris les employés, les sous-traitants, les consultants, les travailleurs temporaires et les fournisseurs tiers.						
8.2.5	L'accès des utilisateurs dont le contrat a été résilié est immédiatement révoqué.	• Examiner les sources d'informations pour les utilisateurs dont le contrat a été résilié. • Examiner les listes d'accès des utilisateurs actuels. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
8.2.6	Les comptes utilisateur inactifs sont supprimés ou désactivés dans les 90 jours suivant l'inactivité.	• Examiner les comptes d'utilisateurs et les dernières informations de connexion. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
8.2.7	Les comptes utilisés par des tiers pour accéder, prendre en charge ou maintenir des composants système via un accès à distance sont gérés comme suit : • Activés uniquement pendant la période nécessaire et désactivés lorsqu'ils ne sont pas utilisés. • L'utilisation est surveillée pour détecter toute activité imprévue.	• Interroger le personnel responsable. • Examiner la documentation pour la gestion des comptes. • Examiner les justificatifs.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.2.8	Si une session utilisateur est inactive pendant plus de 15 minutes, l'utilisateur doit s'authentifier à nouveau pour réactiver le terminal ou la session.	• Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction. Cette exigence n'est pas destinée à empêcher l'exécution d'activités légitimes lorsque la console ou l'ordinateur est sans surveillance.						
8.3 Une authentification robuste pour les utilisateurs et les administrateurs est établie et gérée.							
8.3.1	Tous les accès d'utilisateurs aux composants système pour les utilisateurs et les administrateurs sont authentifiés via au moins l'un des facteurs d'authentification suivants : • Quelque chose que vous connaissez, comme un mot de passe ou une phrase secrète. • Un objet que vous possédez, tel qu'un dispositif à token ou une carte à puce. • Quelque chose que vous êtes, comme un élément biométrique.	• Examiner la documentation décrivant le ou les facteurs d'authentification utilisés. • Pour chaque type de facteur d'authentification utilisé avec chaque type de composant système, observer le processus d'authentification.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction. Cette exigence ne remplace pas les exigences d'authentification à plusieurs facteurs (MFA), mais s'applique aux systèmes dans le périmètre qui ne sont pas autrement soumis aux exigences de la MFA. Un certificat numérique est une option valide pour « quelque chose que vous avez » s'il est unique pour un utilisateur particulier.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.3.2	Une cryptographie robuste est utilisée pour rendre tous les facteurs d'authentification illisibles pendant la transmission et le stockage sur tous les composants système.	• Examiner la documentation du fournisseur. • Examiner les paramètres de la configuration du système. • Examiner les référentiels de facteurs d'authentification. • Examiner les transmissions des données.	☐	☐	☐	☐	☐
8.3.3	L'identité de l'utilisateur est vérifiée avant de modifier tout facteur d'authentification.	• Examiner les procédures de modification des facteurs d'authentification. • Observer le personnel chargé de la sécurité.	☐	☐	☐	☐	☐
8.3.4	Les tentatives d'authentification non valides sont limitées par : • Le verrouillage de l'identifiant utilisateur après pas plus de 10 tentatives. • Le réglage de la durée de verrouillage sur un minimum de 30 minutes ou jusqu'à ce que l'identité de l'utilisateur soit confirmée.	• Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction.						
8.3.5	Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils sont définis et réinitialisés pour chaque utilisateur comme suit : • Réglés sur une valeur unique pour la première utilisation et lors de la réinitialisation. • Doivent être modifiés immédiatement après la première utilisation.	• Examiner les procédures de définition et de réinitialisation des mots de passe/phrases secrètes. • Observer le personnel chargé de la sécurité.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.3.6	Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils devront répondre au niveau de complexité minimum suivant : • Une longueur minimale de 12 caractères (ou SI le système ne prend pas en charge 12 caractères, une longueur minimale de huit caractères). • Contenir à la fois des caractères numériques et alphabétiques.	• Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer : • Aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction. • Aux comptes d'applications ou système, qui sont régis par les exigences de la section 8.6. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.* Jusqu'au 31 mars 2025, les mots de passe doivent avoir une longueur minimale de sept caractères conformément à l'exigence 8.2.3 du standard PCI DSS v3.2.1.						
8.3.7	Les personnes ne sont pas autorisées à soumettre un nouveau mot de passe/phrase secrète qui soient les mêmes que ceux des quatre derniers mots de passe/phrase secrètes utilisés.	• Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.3.8	Les politiques et procédures d'authentification sont documentées et communiquées à tous les utilisateurs, notamment : • Des conseils sur le choix de facteurs d'authentification robustes. • Des conseils sur la façon dont les utilisateurs doivent protéger leurs facteurs d'authentification. • Des instructions pour ne pas réutiliser les mots de passe/phrases secrètes précédemment utilisés. • Des instructions pour modifier les mots de passe/phrases secrètes en cas de soupçon ou de connaissance que les mots de passe/phrases secrètes ont été compromis et comment signaler l'incident.	• Examiner les procédures. • Interroger le personnel. • Examiner les stratégies et les procédures d'authentification qui sont distribuées aux utilisateurs. • Interroger les utilisateurs.	☐	☐	☐	☐	☐
8.3.9	Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès utilisateur (c'est-à-dire dans toute mise en œuvre d'authentification à un seul facteur), alors soit : • Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours, **OU** • La posture de sécurité des comptes est analysée de manière dynamique et l'accès en temps réel aux ressources est automatiquement déterminé en conséquence. *(suite)*	• Inspecter les paramètres de la configuration du système.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Cette exigence ne s'applique pas aux composants système dans le périmètre. Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction. Cette exigence ne s'applique pas aux comptes clients des prestataires de services mais s'applique aux comptes du personnel des prestataires de services.						
8.3.10	***Exigences supplémentaires pour les prestataires de services uniquement***						
8.3.10.1	***Exigences supplémentaires pour les prestataires de services uniquement***						
8.3.11	Lorsque des facteurs d'authentification tels que des jetons de sécurité physiques ou logiques, des cartes à puce ou des certificats sont utilisés : • Les facteurs sont attribués à un utilisateur individuel et ne sont pas partagés entre plusieurs utilisateurs. • Les mesures de sécurité physiques et/ou logiques garantissent que seul l'utilisateur prévu peut utiliser ce facteur pour obtenir l'accès.	• Examiner les politiques et procédures d'authentification. • Interroger le personnel chargé de la sécurité. • Examiner les paramètres de configuration du système et/ou observer les mesures de sécurité physiques, le cas échéant.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.4 L'authentification à plusieurs facteurs (MFA) est mise en œuvre pour sécuriser l'accès au CDE.							
8.4.1	La MFA est mis en œuvre pour tous les accès non-console dans le CDE pour le personnel avec accès administratif.	• Examiner les configurations réseau et/ou système. • Observer le personnel administrateur se connecter au CDE.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'exigence de la MFA pour l'accès administratif non-console s'applique à tout le personnel avec des privilèges élevés ou accrus accédant au CDE via une connexion non-console, c'est-à-dire via un accès logique survenant sur une interface réseau plutôt que via une connexion physique directe.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.4.2	L'authentification MFA est mise en œuvre pour tous les accès hors console au CDE.	• Examiner les configurations réseau et/ou système. • Observer le personnel se connecter au CDE. • Examiner les justificatifs.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence ne s'applique pas : • Aux comptes d'application ou système exécutant des fonctions automatisées. • Aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction. • Aux comptes utilisateur qui uniquement authentifiés via des facteurs d'authentification résistant à l'hameçonnage. L'authentification MFA est requise pour les deux types d'accès spécifiés dans les exigences 8.4.2 et 8.4.3. Par conséquent, l'application de l'authentification MFA à un type d'accès ne remplace pas la nécessité d'appliquer une autre instance de l'authentification MFA à l'autre type d'accès. Si un utilisateur se connecte d'abord au réseau de l'entité via un accès à distance, puis initie ultérieurement une connexion au CDE à partir du réseau, conformément à cette exigence, ladite personne s'authentifiera à l'aide d'une authentification MFA deux fois, une fois lors de la connexion via un accès à distance au réseau de l'entité et une fois lors de la connexion du réseau de l'entité au CDE. Les exigences de l'authentification MFA s'appliquent à tous les types de composants système, y compris le cloud, les systèmes hébergés et les applications sur site, les dispositifs de sécurité réseau, les postes de travail, les serveurs et les points de terminaison, et comportent l'accès direct aux réseaux ou systèmes d'une entité ainsi qu'un accès Web à une application ou à une fonction. L'authentification MFA pour l'accès au CDE peut être mise en œuvre au niveau du réseau ou du système/application ; elle n'a pas à être appliquée aux deux niveaux. Par exemple, si l'authentification MFA est utilisée lorsqu'un utilisateur se connecte au réseau CDE, il n'est pas nécessaire de l'utiliser lorsque l'utilisateur se connecte à chaque système ou application au sein du CDE. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.4.3	L'authentification MFA est mise en œuvre pour tous les accès distants provenant de l'extérieur du réseau de l'entité qui pourraient accéder ou avoir une incidence sur le CDE.	• Examiner les configurations réseau et/ou système pour les serveurs et systèmes d'accès à distance. • Observer le personnel (par exemple, les utilisateurs et les administrateurs) et les tiers se connectant à distance au réseau.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'exigence de l'authentification MFA pour l'accès à distance provenant de l'extérieur du réseau de l'entité s'applique à tous les comptes d'utilisateur pouvant accéder au réseau à distance, lorsque cet accès à distance conduit ou pourrait conduire à l'accès au CDE. Cela inclut tous les accès à distance par le personnel (utilisateurs et administrateurs) et par des tiers (y compris, sans toutefois s'y limiter, les vendeurs, les fournisseurs, les prestataires de services et les clients). Si l'accès à distance concerne une partie du réseau de l'entité qui est correctement segmentée du CDE, de sorte que les utilisateurs distants ne peuvent pas accéder ou avoir un impact sur le CDE, l'authentification MFA pour l'accès à distance à cette partie du réseau n'est pas requise. Cependant, l'authentification MFA est requis pour tout accès distant aux réseaux ayant accès au CDE et est recommandée pour tous les accès distants aux réseaux de l'entité. Les exigences de l'authentification MFA s'appliquent à tous les types de composants système, y compris le cloud, les systèmes hébergés et les applications sur site, les dispositifs de sécurité réseau, les postes de travail, les serveurs et les points de terminaison, et comportent l'accès direct aux réseaux ou systèmes d'une entité ainsi qu'un accès Web à une application ou à une fonction.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.5 Les systèmes d'authentification à plusieurs facteurs (MFA) sont configurés pour éviter les abus.							
8.5.1	Les systèmes MFA sont mis en œuvre comme suit : • Le système MFA n'est pas sensible aux attaques par réinsertion. • Les systèmes MFA ne peuvent être contournés par aucun utilisateur, y compris les utilisateurs administratifs, à moins que cela ne soit spécifiquement documenté et autorisé par la direction à titre exceptionnel, pour une période limitée. • Au moins deux types différents de facteurs d'authentification sont utilisés. • La réussite de tous les facteurs d'authentification est obligatoire avant que l'accès ne soit accordé.	• Examiner la documentation du système du fournisseur. • Examiner les configurations système pour l'implémentation de la MFA. • Interroger le personnel responsable et observer les processus. • Observer le personnel se connectant aux composants système dans le CDE. • Observer le personnel se connectant à distance depuis l'extérieur du réseau de l'entité.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.6 L'utilisation des comptes d'applications et système et des facteurs d'authentification associés est strictement gérée.							
8.6.1	Si les comptes utilisés par les systèmes ou les applications peuvent être utilisés pour la connexion interactive, ils sont gérés comme suit : • L'utilisation interactive est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles. • L'utilisation interactive est limitée au temps nécessaire à la circonstance exceptionnelle. • La justification commerciale de l'utilisation interactive est documentée. • L'utilisation interactive est explicitement approuvée par la direction. • L'identité de l'utilisateur individuel est confirmée avant que l'accès au compte ne soit accordé. • Chaque action entreprise est attribuable à un seul utilisateur.	• Examiner les comptes d'application et système qui peuvent être utilisés et les connexions interactives. • Interroger le personnel administratif.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.6.2	Les mots de passe/phrases secrètes pour tous les comptes d'applications et système qui peuvent être utilisés pour la connexion interactive ne sont pas codés en dur dans les scripts, les fichiers de configuration/de propriété ou le code source sur mesure et personnalisé.	• Interroger le personnel. • Examiner les procédures de développement du système. • Examiner les scripts, les fichiers de configuration/de propriété et le code source sur mesure et personnalisé pour les comptes d'applications et système pouvant être utilisés pour une connexion interactive.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les mots de passe/phrases secrètes stockés doivent être cryptés conformément à l'exigence 8.3.2 du standard PCI DSS. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
8.6.3	Les mots de passe/phrases secrètes pour tous les comptes d'applications et système sont protégés contre les abus comme suit : • Les mots de passe/phrases secrètes sont modifiés périodiquement (à la fréquence définie dans l'analyse des risques ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1) et en cas de soupçon ou de confirmation de compromission. • Les mots de passe/phrases secrètes sont construits avec une complexité suffisante adaptée à la fréquence à laquelle l'entité modifie les mots de passe/phrases secrètes.	• Examiner les politiques et les procédures. • Examiner l'analyse des risques ciblée. • Interroger le personnel responsable. • Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence 9 : Limiter l'accès physique aux données des titulaires de cartes

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.1 Les processus et mécanismes de restriction de l'accès physique aux données des titulaires de cartes sont définis et compris.							
9.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 9 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
9.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 9 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
9.2 Les mesures de sécurité d'accès physiques gèrent l'entrée dans les installations et les systèmes contenant les données des titulaires de cartes.							
9.2.1	Des mesures de sécurité d'accès aux installations appropriés sont En Place pour limiter l'accès physique aux systèmes du CDE.	• Observer les mesures de sécurité d'entrée physiques. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence ne s'applique pas aux emplacements accessibles au public par les consommateurs (titulaires de cartes).						

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.2.1.1	L'accès physique individuel aux zones sensibles au sein du CDE est surveillé à l'aide de caméras vidéo ou de mécanismes de contrôle d'accès physique (ou les deux), des manières suivantes : • Les points d'entrée et de sortie des zones sensibles du CDE sont surveillés. • Les dispositifs ou mécanismes de surveillance sont protégés contre l'altération ou la désactivation. • Les données recueillies sont examinées et corrélées avec d'autres entrées. • Les données recueillies sont conservées pendant au moins trois mois, sauf restriction légale contraire.	• Observer les emplacements où se produit l'accès physique individuel aux zones sensibles au sein du CDE. • Observer les mécanismes de contrôle d'accès physique et/ou examiner les caméras vidéo. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
9.2.2	Des mesures de sécurité physiques et/ou logiques sont mis en œuvre pour limiter l'utilisation des prises réseaux accessibles au public au sein de l'installation.	• Interroger le personnel responsable. • Observer les emplacements des prises réseaux accessibles au public.	☐	☐	☐	☐	☐
9.2.3	L'accès physique aux points d'accès sans fil, aux passerelles, au matériel de mise en réseau/de communication et aux lignes de télécommunication au sein de l'installation est limité.	• Interroger le personnel responsable. • Observer les emplacements du matériel et des lignes.	☐	☐	☐	☐	☐
9.2.4	L'accès aux consoles dans les zones sensibles est limité par verrouillage lorsqu'elles ne sont pas utilisées.	• Observer la tentative d'un administrateur système de se connecter à des consoles dans des zones sensibles.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.3 L'accès physique du personnel et des visiteurs est autorisé et géré.							
9.3.1	Des procédures sont mises en œuvre pour autoriser et gérer l'accès physique du personnel au CDE, notamment : • Identification du personnel. • Gérer les modifications des exigences d'accès physique d'un utilisateur. • Révoquer ou mettre fin à l'identification du personnel. • Limiter l'accès au processus ou au système d'identification au personnel autorisé.	• Examiner les procédures documentées. • Observer les méthodes d'identification, telles que les badges d'identification. • Observer les processus.	☐	☐	☐	☐	☐
9.3.1.1	L'accès physique aux zones sensibles au sein du CDE pour le personnel est contrôlé comme suit : • L'accès est autorisé et basé sur la fonction du poste individuel. • L'accès est révoqué immédiatement après la résiliation du contrat de travail. • Tous les mécanismes d'accès physiques, tels que les clés, les cartes d'accès, etc., sont retournés ou désactivés lors de la résiliation du contrat.	• Observer le personnel dans les zones sensibles dans le CDE. • Interroger le personnel responsable. • Examiner les listes de contrôle d'accès physique. • Observer les processus.	☐	☐	☐	☐	☐
9.3.2	Des procédures sont mises en œuvre afin d'autoriser et gérer l'accès des visiteurs au CDE, notamment : • Les visiteurs sont autorisés avant d'entrer. • Les visiteurs sont escortés en tout temps. • Les visiteurs sont clairement identifiés et reçoivent un badge ou autre pièce d'identité qui a un délai d'expiration. • Les badges de visiteur ou autre identification distinguent visiblement les visiteurs du personnel.	• Examiner les procédures documentées. • Observer les processus lorsque des visiteurs sont présents dans le CDE. • Interroger le personnel. • Observer l'utilisation des badges de visiteur ou d'autres identifications.	☐	☐	☐	☐	☐
9.3.3	Les badges ou les pièces d'identité des visiteurs sont remis ou désactivés avant que les visiteurs ne quittent l'établissement ou à la date d'expiration.	• Observer les visiteurs quittant l'établissement • Interroger le personnel.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.3.4	Les journaux de visiteurs sont utilisés pour conserver un enregistrement physique de l'activité des visiteurs à la fois au sein de l'installation et dans les zones sensibles, y compris : • Le nom du visiteur et l'organisation représentée. • La date et l'heure de la visite. • Le nom du personnel autorisant l'accès physique. • Conserver le journal pendant au moins trois mois, sauf restriction légale contraire.	• Examiner les journaux des visiteurs. • Interroger le personnel responsable. • Examiner les emplacements de stockage des journaux des visiteurs.	☐	☐	☐	☐	☐
9.4 Les supports contenant les données des titulaires de carte sont stockés, consultés, distribués et détruits de manière sécurisée.							
9.4.1	Tous les supports contenant des données de titulaire de carte sont physiquement sécurisés.	• Examiner la documentation.	☐	☐	☐	☐	☐
9.4.1.1	Les sauvegardes sur des supports hors ligne avec les données des titulaires de cartes sont stockées dans un emplacement sécurisé.	• Examiner les procédures documentées. • Examiner les journaux ou d'autres documents. • Interroger le personnel responsable au(x) lieu(x) de stockage.	☐	☐	☐	☐	☐
9.4.1.2	La sécurité des emplacements des supports de sauvegarde hors ligne contenant les données des titulaires de cartes est examinée au moins une fois tous les 12 mois.	• Examiner les procédures documentées, les journaux ou toute autre documentation. • Interroger le personnel responsable au(x) lieu(x) de stockage.	☐	☐	☐	☐	☐
9.4.2	Tous les supports contenant des données de titulaires de cartes sont classés en fonction de la sensibilité des données.	• Examiner les procédures documentées. • Examiner les journaux des supports ou autres documents.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.4.3	Les supports avec les données des titulaires de cartes envoyées à l'extérieur de l'installation sont sécurisés comme suit : • Les supports envoyés à l'extérieur de l'installation sont enregistrés. • Les supports sont envoyés par courrier sécurisé ou par un autre mode de livraison pouvant être suivi avec précision. • Les journaux de suivi hors site incluent des détails sur l'emplacement des supports.	• Examiner les procédures documentées. • Interroger le personnel. • Examiner les enregistrements. • Examiner les journaux de suivi hors site pour tous les supports.	☐	☐	☐	☐	☐
9.4.4	La direction approuve tous les supports avec des données de titulaires de cartes qui sont déplacés hors de l'installation (y compris lorsque les supports sont distribués à des personnes individuelles).	• Examiner les procédures documentées. • Examiner les journaux de suivi des supports hors site. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Les personnes qui approuvent les mouvements des supports devraient avoir le niveau approprié d'autorité de gestion pour accorder cette approbation. Cependant, il n'est pas spécifiquement exigé que ces personnes aient l'indication « responsable » dans leur titre.						
9.4.5	Les journaux d'inventaire de tous les supports électroniques contenant les données des titulaires de cartes sont conservés.	• Examiner les procédures documentées. • Examiner les journaux d'inventaire des supports électroniques. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.4.5.1	Les inventaires des supports électroniques avec les données des titulaires de cartes sont réalisés au moins une fois tous les 12 mois.	• Examiner les procédures documentées. • Examiner les journaux d'inventaire des supports électroniques. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
9.4.6	Les documents papier contenant les données des titulaires de cartes sont détruits lorsqu'ils ne sont plus nécessaires pour des raisons commerciales ou juridiques, comme suit : • Les documents sont déchiquetés, incinérés ou réduits en pâte afin que les données des titulaires de cartes ne puissent pas être reconstituées. • Les documents sont stockés dans des conteneurs de stockage sécurisés avant destruction.	• Examiner la politique de destruction des supports. • Observer les processus. • Interroger le personnel. • Observer les conteneurs de stockage.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Ces exigences relatives à la destruction du support lorsque ce support n'est plus nécessaire pour des raisons commerciales ou juridiques sont distinctes de l'exigence 3.2.1 du standard PCI DSS, qui vise à supprimer en toute sécurité les données des titulaires de cartes lorsque celles-ci ne sont plus nécessaires conformément aux politiques de conservation des données des titulaires de carte de l'entité.						
9.4.7	Les supports électroniques contenant les données de titulaires de cartes sont détruits lorsqu'ils ne sont plus nécessaires pour des raisons commerciales ou juridiques via l'un des éléments suivants : • Les supports électroniques sont détruits. • Les données des titulaires de cartes sont rendues irrécupérables de sorte qu'elles ne peuvent pas être reconstituées. *(suite)*	• Examiner la politique de destruction des supports. • Observer le processus de destruction des supports. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Ces exigences relatives à la destruction du support lorsque ce support n'est plus nécessaire pour des raisons commerciales ou juridiques sont distinctes de l'exigence 3.2.1 du standard PCI DSS, qui vise à supprimer en toute sécurité les données des titulaires de cartes lorsque celles-ci ne sont plus nécessaires conformément aux politiques de conservation des données des titulaires de carte de l'entité.						
9.5 Les dispositifs de point d'interaction (POI) sont protégés contre l'altération et la substitution non autorisée.							
9.5.1	Les appareils POI qui capturent les données de la carte de paiement via une interaction physique directe avec le facteur de forme de la carte de paiement sont protégés contre l'altération et la substitution non autorisée, notamment : • Maintenir une liste des périphériques POI. • Inspecter périodiquement les appareils POI pour rechercher des altérations ou des substitutions non autorisées. • Former le personnel à être conscient des comportements suspects et à signaler toute altération ou substitution non autorisée d'appareils.	• Examiner les politiques et les procédures documentées.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Ces exigences s'appliquent aux appareils POI déployés utilisés dans les transactions par carte (c'est-à-dire un facteur de forme de carte de paiement tel qu'une carte qui est glissée, tapée ou insérée). Ces exigences ne s'appliquent pas aux : • Composants utilisés uniquement pour la saisie manuelle des clés PAN. • Appareils commerciaux disponibles sur le marché (COTS) (par exemple, les smartphones ou les tablettes), qui sont des appareils mobiles appartenant à des commerçants conçus pour la distribution sur le marché de masse.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.5.1.1	Une liste à jour des appareils POI est maintenue, y compris : • La marque et le modèle de l'appareil. • L'emplacement de l'appareil. • Numéro de série de l'appareil ou autres méthodes d'identification uniques.	• Examiner la liste des périphériques POI. • Observer les périphériques POI et les emplacements des périphériques. • Interroger le personnel.	☐	☐	☐	☐	☐
9.5.1.2	Les surfaces des appareils POI sont inspectées périodiquement afin de détecter les altérations et les substitutions non autorisées.	• Examiner les procédures documentées. • Interroger le personnel responsable. • Observer les processus d'inspection.	☐	☐	☐	☐	☐
9.5.1.2.1	La fréquence des inspections périodiques des appareils POI et le type d'inspections effectuées sont définis dans l'analyse de risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1.	• Examiner l'analyse des risques ciblée. • Examiner les résultats documentés d'inspections périodiques des appareils. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
9.5.1.3	Une formation est dispensée au personnel des environnements POI pour qu'il soit au courant des tentatives d'altération ou de remplacement des appareils POI, et comprend : • Vérifier l'identité de toute personne tierce prétendant être du personnel de réparation ou de maintenance, avant de leur accorder l'accès pour modifier ou dépanner les appareils. • Des procédures pour garantir que les appareils ne sont pas installés, remplacés ou retournés sans vérification. • Être conscient des comportements suspects entourant les appareils. • Signaler les comportements suspects et les indications d'altération ou de substitution de l'appareil au personnel approprié.	• Examiner les supports de formation pour le personnel dans les environnements POI. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

Surveiller et Tester Régulièrement les Réseaux

Exigence 10 : Enregistrer et Surveiller Tous les Accès aux Composants Système et aux Données des Titulaires de Cartes

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.1 Les processus et mécanismes d'enregistrement et de surveillance de tous les accès aux composants système et aux données des titulaires de cartes sont définis et compris.							
10.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 10 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
10.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 10 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
10.2 Les journaux d'audit sont mis en œuvre pour prendre en charge la détection des anomalies et des activités suspectes, ainsi que l'analyse criminelle des événements.							
10.2.1	Les journaux d'audit sont activés et actifs pour tous les composants système et les données des titulaires de cartes.	• Interroger les administrateurs système. • Examiner les configurations du système.	☐	☐	☐	☐	☐
10.2.1.1	Les journaux d'audit capturent tous les accès des utilisateurs individuels aux données des titulaires de cartes.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.2.1.2	Les journaux d'audit capturent toutes les actions effectuées par tout utilisateur disposant d'un accès administratif, y compris toute utilisation interactive des comptes d'applications ou système.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.2.1.3	Les journaux d'audit capturent tous les accès aux journaux d'audit.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.2.1.4	Les journaux d'audit capturent toutes les tentatives d'accès logique non valides.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.2.1.5	Les journaux d'audit capturent toutes les modifications apportées à l'identification et aux « credentials », y compris, sans toutefois s'y limiter : • La création de nouveaux comptes. • L'élévation des privilèges. • Toutes les modifications, ajouts ou suppressions de comptes avec accès administrateur.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.2.1.6	Les journaux d'audit capturent les éléments suivants : • Toutes les initialisations des nouveaux journaux d'audit, et • Tous les démarrages, arrêts ou pauses des journaux d'audit existants.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.2.1.7	Les journaux d'audit capturent toutes les créations et suppressions d'objets au niveau du système.	• Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.2.2	Les journaux d'audit enregistrent les détails suivants pour chaque événement auditable : • Identification de l'utilisateur. • Type d'événement. • Date et heure. • Indication de réussite et d'échec. • Origine de l'événement. • Identité ou nom des données, composant système, ressource ou service touchés (par exemple, nom et protocole).	• Interroger le personnel responsable. • Examiner les configurations des journaux d'audit. • Examiner les données des journaux d'audit.	☐	☐	☐	☐	☐
10.3 Les journaux d'audit sont protégés contre la destruction et les modifications non autorisées.							
10.3.1	L'accès en lecture aux fichiers journaux d'audit est limité aux personnes ayant un besoin lié au travail.	• Interroger les administrateurs système. • Examiner les configurations du système et les privilèges.	☐	☐	☐	☐	☐
10.3.2	Les fichiers Journaux d'audit sont protégés pour empêcher les modifications par des utilisateurs.	• Examiner les configurations du système et les privilèges. • Interroger les administrateurs système.	☐	☐	☐	☐	☐
10.3.3	Les fichiers Journaux d'audit, y compris ceux des technologies externes, sont rapidement sauvegardés sur un ou des serveurs de journaux internes sécurisés et centraux ou sur d'autres supports difficiles à modifier.	• Examiner les configurations ou les fichiers journaux de sauvegarde.	☐	☐	☐	☐	☐
10.3.4	Des mécanismes de surveillance de l'intégrité des fichiers ou de détection des modifications sont utilisés sur les journaux d'audit afin de garantir que les données de journalisation existantes ne peuvent pas être modifiées sans générer d'alertes.	• Examiner les paramètres système. • Examiner les fichiers surveillés. • Examiner les résultats des activités de surveillance.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.4 Les journaux d'audit sont examinés pour identifier les anomalies ou les activités suspectes.							
10.4.1	Les journaux d'audit suivants sont examinés au moins une fois par jour : • Tous les événements de sécurité. • Les journaux de tous les composants système qui stockent, traitent ou transmettent des CHD et/ou des SAD. • Les journaux de tous les composants système critiques. • Les journaux de tous les serveurs et composants système qui exécutent des fonctions de sécurité (par exemple, mesures de sécurité réseau, systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), serveurs d'authentification).	• Examiner les politiques et les procédures de sécurité. • Observer les processus. • Interroger le personnel.	☐	☐	☐	☐	☐
10.4.1.1	Des mécanismes automatisés sont utilisés pour effectuer des examens des journaux d'audit.	• Examiner les mécanismes d'examen des journaux. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
10.4.2	Les journaux de tous les autres composants système (ceux non spécifiés dans l'exigence 10.4.1) sont examinés périodiquement.	• Examiner les politiques et les procédures de sécurité. • Examiner les résultats documentés des examens des journaux. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique à tous les autres composants système dans le périmètre non inclus dans l'exigence 10.4.1.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.4.2.1	La fréquence des examens périodiques des journaux pour tous les autres composants système (non définis dans l'exigence 10.4.1) est définie dans l'analyse de risques ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1.	• Examiner l'analyse des risques ciblée. • Examiner les résultats documentés des examens périodiques des journaux. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
10.4.3	Les exceptions et anomalies identifiées au cours du processus d'examen sont traitées.	• Examiner les politiques et les procédures de sécurité. • Observer les processus. • Interroger le personnel.	☐	☐	☐	☐	☐
10.5 L'historique des journaux d'audit est conservé et disponible pour analyse.							
10.5.1	Conserver l'historique des journaux d'audit pendant au moins 12 mois, avec au moins les trois mois les plus récents immédiatement disponibles pour analyse.	• Examiner les politiques et les procédures documentées de conservation des journaux d'audit. • Examiner les configurations de l'historique des journaux d'audit. • Examiner les journaux d'audit. • Interroger le personnel. • Observer les processus.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.6 Les mécanismes de synchronisation temporelle prennent en charge des paramètres de temps cohérents sur tous les systèmes.							
10.6.1	Les horloges système et l'heure sont synchronisées à l'aide de la technologie de synchronisation date/heure. **Notes d'Applicabilité** Le maintien à jour de la technologie de synchronisation date/heure comporte la gestion des vulnérabilités et la mise à jour de la technologie conformément aux exigences 6.3.1 et 6.3.3 du standard PCI DSS.	• Examiner les paramètres de la configuration du système.	☐	☐	☐	☐	☐
10.6.2	Les systèmes sont configurés pour l'heure correcte et cohérente comme suit : • Un ou plusieurs serveurs de temps désignés utilisés. • Seul le ou seuls les serveurs de temps centraux désignés reçoit l'heure de sources externes. • L'heure reçue de sources externes est basée sur le temps atomique international ou le temps universel coordonné (UTC). • Le ou les serveurs de temps désignés n'acceptent les mises à jour de la date/heure que de sources externes spécifiques acceptées par l'industrie. • Lorsqu'il y a plus d'un serveur de temps désigné, les serveurs de temps s'échangent les uns avec les autres pour garder l'heure exacte. • Les systèmes internes ne reçoivent des informations de date/heure que du ou des serveurs de temps centraux désignés.	• Examiner les paramètres de configuration du système pour acquérir, distribuer et stocker l'heure correcte.	☐	☐	☐	☐	☐
10.6.3	Les paramètres et les données de synchronisation date/heure sont protégés comme suit : • L'accès aux données date/heure est limité au personnel ayant un besoin professionnel. • Toute modification des paramètres horaires sur les systèmes critiques est enregistrée, surveillée et examinée.	• Examiner les configurations système et les paramètres et journaux de synchronisation de l'heure. • Observer les processus.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.7 Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement.							
10.7.1	***Exigences supplémentaires pour les prestataires de services uniquement***						
10.7.2	Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances des systèmes de mesures de sécurité critiques suivants : • Mesures de sécurité réseau. • IDS/IPS. • Les mécanismes de détection des modifications. • Les solutions anti-programmes malveillants. • Les contrôles d'accès physiques • Les contrôles d'accès logiques • Les mécanismes de journalisation des audits. • Des mesures de sécurité de segmentation (le cas échéant). • Les mécanismes d'examen des Journaux d'audit. • Des outils automatisés de test de la sécurité (le cas échéant).	• Examiner les processus documentés. • Observer les processus de détection et d'alerte. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique à toutes les entités, y compris les prestataires de services, et remplacera l'exigence 10.7.1 à compter du 31 mars 2025. Elle comprend deux systèmes supplémentaires de mesures de sécurité critiques qui ne figurent pas dans l'exigence 10.7.1. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
10.7.3	Les défaillances de tout système de mesures de sécurité critique sont traitées rapidement, y compris, sans toutefois s'y limiter : • Restauration des fonctions de sécurité. • Identifier et documenter la durée (date et heure du début à la fin) de la défaillance de sécurité. • Identifier et documenter la ou les causes de la défaillance et documenter les mesures correctives nécessaires. • Identifier et résoudre tous les problèmes de sécurité survenus lors de la défaillance. • Déterminer si d'autres mesures est nécessaires à la suite de la défaillance de la sécurité. • Mettre en œuvre des mesures afin d'éviter que la cause de la défaillance ne se reproduise. • Reprendre la surveillance des mesures de sécurité.	• Examiner les processus documentés. • Interroger le personnel. • Examiner les enregistrements liés aux défaillances critiques des systèmes de mesures de sécurité.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence s'applique uniquement lorsque l'entité évaluée est un prestataire de services, jusqu'au 31 mars 2025, après quoi cette exigence s'appliquera à toutes les entités. *Il s'agit d'une exigence actuelle v3.2.1 qui s'applique uniquement aux prestataires de services. Cependant, cette exigence est une bonne pratique pour toutes les autres entités jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence 11 : Tester Régulièrement la Sécurité des Systèmes et des Réseaux

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.1 Les processus et mécanismes pour tester régulièrement la sécurité des systèmes et des réseaux sont définis et compris.							
11.1.1	Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 11 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
11.1.2	Les rôles et les responsabilités liés aux activités de l'exigence 11 sont documentés, attribués et compris.	• Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.2 Les points d'accès sans fil sont identifiés et surveillés, et les points d'accès sans fil non autorisés sont traités.							
11.2.1	Les points d'accès sans fil autorisés et non autorisés sont gérés de la manière suivante : • La présence de points d'accès sans fil (Wi-Fi) est testée. • Tous les points d'accès sans fil autorisés et non autorisés sont détectés et identifiés. • Les tests, la détection et l'identification sont effectués au moins une fois tous les trois mois. • Si une surveillance automatisée est utilisée, le personnel doit être averti via des alertes générées.	• Examiner les politiques et les procédures. • Examiner la ou les méthodologies utilisées et la documentation qui en résulte. • Interroger le personnel. • Examiner les résultats de l'évaluation sans fil. • Examiner les paramètres de configuration.	☐	☐.	☐	☐	☐
	Notes d'Applicabilité L'exigence s'applique même lorsqu'il existe une politique interdisant l'utilisation de la technologie sans fil. Les méthodes utilisées pour satisfaire à cette exigence doivent être suffisantes pour détecter et identifier à la fois les appareils autorisés et non autorisés, y compris les appareils non autorisés qui se connectent à des appareils eux-mêmes autorisés.						
11.2.2	Un inventaire des points d'accès sans fil autorisés est conservé, y compris une justification commerciale documentée.	• Examiner la documentation.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.3 Les vulnérabilités externes et internes sont régulièrement identifiées, priorisées et traitées.							
11.3.1	Les analyses de vulnérabilités internes sont effectuées comme suit : • Au moins une fois tous les trois mois. • Les vulnérabilités qui sont soit à haut risque soit critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues. • De rescans sont effectués pour confirmer que toutes les vulnérabilités à haut risque et critiques, comme indiqué ci-dessus, ont été résolues. • L'outil d'analyse est tenu à jour avec les dernières informations sur les vulnérabilités. • Les analyses sont effectuées par du personnel qualifié et l'indépendance organisationnelle du testeur existe.	• Examiner les résultats du rapport d'analyse interne. • Examiner les configurations des outils d'analyse. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Il n'est pas nécessaire d'utiliser un QSA ou un ASV pour effectuer des analyses de vulnérabilité internes. Les analyses de vulnérabilités internes peuvent être effectuées par du personnel interne qualifié qui est raisonnablement indépendant du ou des composants système analysés (par exemple, un administrateur réseau ne devrait pas être responsable de l'analyse du réseau), ou une entité peut choisir d'avoir des analyses de vulnérabilités internes effectuées par une firme spécialisée dans l'analyse des vulnérabilités.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.3.1.1	Toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme vulnérabilités à haut risque ou vulnérabilité critiques (conformément aux classements de risque de vulnérabilité de l'entité définis à l'exigence 6.3.1) sont gérées comme suit : • Traitées sur la base du risque défini dans l'analyse de risque ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1. • De nouvelles analyses sont effectuées au besoin.	• Examiner l'analyse des risques ciblée. • Interroger le personnel responsable. • Examiner les résultats du rapport d'analyse interne ou autre documentation.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Le délai pour traiter les vulnérabilités à faible risque est soumis aux résultats d'une analyse des risques conformément à l'exigence 12.3.1 qui comprend (au minimum) l'identification des actifs protégés, des menaces et de la probabilité et/ou de l'impact d'une menace réalisée. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
11.3.1.2	Les analyses de vulnérabilité internes sont effectuées via une analyse authentifiée comme suit :						
	• Les systèmes qui ne peuvent pas accepter les « credentials » pour l'analyse authentifiée sont documentés.	• Examiner la documentation. • Examiner les configurations des outils d'analyse. • Examiner les résultats du rapport d'analyse. • Interroger le personnel. • Examiner les comptes utilisés pour l'analyse authentifiée.	☐	☐	☐	☐	☐
	• Des privilèges suffisants sont utilisés pour les systèmes qui acceptent les « credentials » pour l'analyse.		☐	☐	☐	☐	☐
	• Si les comptes utilisés pour l'analyse authentifiée peuvent être utilisés pour la connexion interactive, ils sont gérés conformément à l'exigence 8.2.2. *(suite)*		☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Les outils d'analyse authentifiée peuvent être basés sur l'hôte ou sur le réseau. Les privilèges « suffisants » sont ceux qui sont nécessaires pour accéder aux ressources système afin qu'une analyse approfondie puisse être effectuée pour détecter les vulnérabilités connues. Cette exigence ne s'applique pas aux composants système qui ne peuvent pas accepter les « credentials » pour l'analyse. Des exemples de systèmes qui peuvent ne pas accepter les « credentials » pour l'analyse comportent certains appareils réseau et de sécurité, les serveurs principaux et les conteneurs. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
11.3.1.3	Les analyses internes des vulnérabilités sont effectuées après toute modification importante comme suit : • Les vulnérabilités qui sont soit à haut risque, soit critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues. • De nouvelles analyses sont effectuées au besoin. • Les analyses sont effectuées par du personnel qualifié et l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	• Examiner les documents de contrôle des modifications. • Interroger le personnel. • Examiner le rapport d'analyse interne et de nouvelles analyses, le cas échéant. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'analyse authentifiée des vulnérabilités internes conformément à l'exigence 11.3.1.2 n'est pas nécessaire pour les analyses effectuées après des modifications importantes.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.3.2	Les analyses de vulnérabilités externes sont effectuées comme suit : • Au moins une fois tous les trois mois. • Par un fournisseur d'analyse agréé par le PCI SSC (ASV). • Les vulnérabilités sont résolues et les exigences du G*uide du Programme* de l'ASV pour une analyse réussie sont respectées. • Des réanalyses sont effectuées au besoin pour confirmer que les vulnérabilités sont résolues conformément aux exigences du *Guide du Programme* de l'ASV pour une analyse réussie.	• Examiner les rapports d'analyse de l'ASV.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Pour l'évaluation initiale au standard PCI DSS pour cette exigence, il n'est pas nécessaire que quatre scans réussis soient effectués dans les 12 mois si l'auditeur vérifie que : 1) le résultat de l'analyse le plus récent était une analyse réussie, 2) l'entité a documenté des politiques et des procédures exigeant une analyse au moins une fois tous les trois mois, et 3) les vulnérabilités notées dans les résultats de l'analyse ont été corrigées comme indiqué dans une ou plusieurs nouvelles analyses. Cependant, pour les années suivantes après l'évaluation initiale du standard PCI DSS, des analyses réussies au moins tous les trois mois doivent avoir eu lieu. Les outils d'analyse de l'ASV peuvent analyser une vaste gamme de types de réseaux et de topologies. Tous les détails concernant l'environnement cible (par exemple, les équilibreurs de charge, les fournisseurs tiers, les ISP, les configurations spécifiques, les protocoles utilisés, les interférences d'analyse) doivent être réglés entre l'ASV et le client de l'analyse. Se reporter au G*uide du Programme de l'ASV* publié sur le site Web du PCI SSC afin de connaître les responsabilités du client de l'analyse, la préparation de l'analyse, etc.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.3.2.1	Les analyses externes des vulnérabilités sont effectuées après toute modification importante comme suit : • Les vulnérabilités notées 4,0 ou plus par le CVSS sont résolues. • De nouvelles analyses sont effectuées au besoin. • Les analyses sont effectuées par du personnel qualifié et l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	• Examiner les documents de contrôle des modifications. • Interroger le personnel. • Examiner les rapports d'analyse externe et, le cas échéant, des nouvelles analyses.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.4 Des tests d'intrusion externes et internes sont effectués régulièrement, et les vulnérabilités exploitables et les faiblesses de sécurité sont corrigées.							
11.4.1	Une méthodologie de test d'intrusion est définie, documentée et mise en œuvre par l'entité, et comprend : • Des approches de test d'intrusion acceptées par l'industrie. • Une couverture de l'ensemble du périmètre du CDE et des systèmes critiques. • Des tests à la fois à l'intérieur et à l'extérieur du réseau. • Des tests pour valider les mesures de segmentation et de réduction du périmètre. • Des tests d'intrusion de la couche application pour identifier, au minimum, les vulnérabilités répertoriées dans l'exigence 6.2.4. • Des tests d'intrusion de la couche réseau qui englobent tous les composants prenant en charge les fonctions réseau ainsi que les systèmes d'exploitation. • L'examen et la prise en compte des menaces et des vulnérabilités rencontrées au cours des 12 derniers mois. • Une approche documentée pour évaluer et traiter le risque posé par les vulnérabilités exploitables et les faiblesses de sécurité détectées lors des tests d'intrusion. • La conservation des résultats des tests d'intrusion et des activités de correction pendant au moins 12 mois. *(suite)*	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité Les tests à l'intérieur du réseau (ou « tests d'intrusion internes ») signifient des tests à la fois à l'intérieur du CDE et vers le CDE à partir de réseaux internes fiables et non fiables. Les tests depuis l'extérieur du réseau (ou test d'intrusion « externe ») » signifie tester le périmètre externe exposé des réseaux de confiance et des systèmes critiques connectés ou accessibles aux infrastructures de réseau public.						
11.4.2	Un test d'intrusion interne est effectué : • Selon la méthodologie définie par l'entité. • Au moins une fois tous les 12 mois. • Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application. • Par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	• Examiner le périmètre de travail. • Examiner les résultats du test d'intrusion externe le plus récent. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
11.4.3	Un test d'intrusion externe est effectué : • Selon la méthodologie définie par l'entité. • Au moins une fois tous les 12 mois. • Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application. • Par une ressource interne qualifiée ou un tiers externe qualifié. • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	• Examiner le périmètre de travail. • Examiner les résultats du test d'intrusion externe le plus récent. • Interroger le personnel responsable.					
11.4.4	Les vulnérabilités exploitables et les faiblesses de sécurité détectées lors des tests d'intrusion sont corrigées comme suit : • Conformément à l'évaluation par l'entité du risque posé par le problème de sécurité tel que défini dans l'exigence 6.3.1. • Les tests d'intrusion sont répétés pour vérifier les corrections.	• Examiner les résultats des tests d'intrusion.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.4.5	Si la segmentation est utilisée pour isoler le CDE des autres réseaux, des tests d'intrusion sont effectués sur les mesures de sécurité de segmentation comme suit : • Au moins une fois tous les 12 mois et après toute modification des mesures ou méthodes de segmentation • Couvrir toutes les mesures de sécurité ou méthodes de segmentation utilisée. • Conformément à la méthodologie des tests d'intrusion définie par l'entité. • Confirmer que les mesures ou méthodes de segmentation sont opérationnels et efficaces, et isoler le CDE de tous les systèmes hors du périmètre. • Confirmer l'efficacité de toute utilisation de l'isolement pour séparer les systèmes avec des niveaux de sécurité différents (voir l'exigence 2.2.3). • Effectués par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	• Examiner les mesures de segmentation. • Examiner la méthodologie des tests d'intrusion. • Examiner les résultats du test d'intrusion le plus récent. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
11.4.6	***Exigences supplémentaires pour les prestataires de services uniquement.***						
11.4.7	***Exigences supplémentaires uniquement pour les prestataires de services mutualisés.***						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
11.5 Les intrusions réseau et les modifications imprévues de fichiers sont détectées et traitées.							
11.5.1	Les techniques de détection des intrusions et/ou de prévention des intrusions sont utilisées pour détecter et/ou empêcher les intrusions dans le réseau comme suit : • Tout le trafic est surveillé sur le périmètre du CDE. • Tout le trafic est surveillé aux points critiques du CDE. • Le personnel est alerté des compromissions soupçonnées. • Tous les moteurs de détection et de prévention des intrusions, les lignes de base et les signatures sont tenus à jour.	• Examiner les configurations du système et les schémas de réseau. • Examiner les configurations du système. • Interroger le personnel responsable. • Examiner la documentation du fournisseur.	☐	☐	☐	☐	☐
11.5.1.1	***Exigences supplémentaires pour les prestataires de services uniquement.***						
11.5.2	Un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) est déployé de la façon suivante : • Pour alerter le personnel de modifications non autorisées (y compris les modifications, les ajouts et les suppressions) de fichiers critiques. • Pour effectuer des comparaisons de fichiers critiques au moins une fois par semaine. *(suite)*	• Examiner les paramètres système pour le mécanisme de détection des modifications. • Examiner les fichiers surveillés. • Examiner les résultats des activités de surveillance.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité À des fins de détection des modifications, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une compromission ou un risque de compromission du système. Les mécanismes de détection des modifications, tels que les outils de surveillance de l'intégrité des fichiers, sont généralement préconfigurés avec des fichiers critiques pour le système d'exploitation associé. D'autres fichiers critiques, tels que ceux des applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).						
11.6 Les modifications non autorisées sur les pages de paiement sont détectées et traitées.							
11.6.1	Un mécanisme de détection des modifications et des altérations est déployé de la manière suivante :						
	• Alerter le personnel des modifications non autorisées (y compris les indicateurs de compromission, de changements, d'ajouts et de suppressions) de la sécurité impactant les en-têtes HTTP et du contenu des scripts des pages de paiement comme reçus par le navigateur du consommateur.	• Examiner les paramètres système et les paramètres de configuration du mécanisme. • Examiner les pages de paiement surveillées. • Examiner les résultats des activités de surveillance. • Examiner les paramètres de configuration du mécanisme. • Examiner les paramètres de configuration. • Interroger le personnel responsable. • Le cas échéant, examiner l'analyse des risques ciblée.	☐	☐	☐	☐	☐
	• Le mécanisme est configuré pour évaluer les en-têtes HTTP et les pages de paiement reçus.		☐	☐	☐	☐	☐
	• Les fonctions du mécanisme sont exécutées comme suit : – Au moins une fois toutes les semaines. **OU** – Périodiquement, (à la fréquence définie dans l'analyse des risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1). *(suite)*		☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
	Notes d'Applicabilité						
	Cette exigence s'applique également aux entités disposant d'une ou plusieurs pages Web qui incluent la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un ou plusieurs cadres en ligne ou iframes.) Cette exigence ne s'applique pas à une entité pour les scripts dans la page/formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, une ou plusieurs iframes), lorsque l'entité inclut la page/formulaire de paiement d'un TPSP/processeur de paiement sur sa page Web. Il incombe au TPSP/processeur de paiement de gérer les scripts dans la page/le formulaire de paiement intégré du TPSP/processeur de paiement conformément à cette exigence. L'intention de cette exigence n'est pas qu'une entité soit obligée d'installer un logiciel dans les systèmes ou les navigateurs de ses consommateurs, mais plutôt qu'elle utilise des techniques telles que celles décrites dans les exemples ci-dessus afin d'empêcher et de détecter des activités de script imprévues. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Maintenir une Politique de Sécurité des Informations

Exigence 12 : Appuyer la Sécurité des Informations avec des Politiques et des Programmes Organisationnels

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.1 Une politique complète de sécurité de l'information qui régit et fournit une orientation pour la protection des actifs informationnels de l'entité est connue et à jour.							
12.1.1	Une politique globale de sécurité des informations est : • Établie. • Publiée. • Maintenue. • Diffusé à tout le personnel concerné, ainsi qu'aux fournisseurs et partenaires commerciaux concernés.	• Examiner la politique de sécurité des informations. • Interroger le personnel.	☐	☐	☐	☐	☐
12.1.2	La politique de sécurité des informations est : • Examinée au moins une fois tous les 12 mois. • Mise à jour au besoin pour refléter les modifications apportées aux objectifs professionnels ou les risques pour l'environnement.	• Examiner la politique de sécurité des informations. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.1.3	La politique de sécurité définit clairement les rôles et les responsabilités en matière de sécurité des informations pour tout le personnel, et tout le personnel est conscient et reconnaît ses responsabilités en matière de sécurité desdites informations.	• Examiner la politique de sécurité des informations. • Interroger le personnel responsable. • Examiner les preuves documentées.	☐	☐	☐	☐	☐
12.1.4	La responsabilité de la sécurité de l'information est officiellement attribuée à un responsable de la sécurité de l'information ou à un autre membre de la direction compétent en matière de sécurité de l'information.	• Examiner la politique de sécurité des informations.	☐	☐	☐	☐	☐

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.2 Des politiques d'une utilisation acceptable pour les technologies de l'utilisateur final sont définies et mises en œuvre.							
12.2.1	Des politiques d'utilisation acceptable pour les technologies d'utilisateur final sont documentées et mises en œuvre, notamment : • Une approbation expresse par les parties autorisées. • Des utilisations acceptables de la technologie. • Une liste de produits approuvée par l'entreprise pour une utilisation par les employés, y compris le matériel et les logiciels.	• Examiner les politiques d'utilisation acceptable. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Des exemples de technologies d'utilisateur final pour lesquelles des politiques d'utilisation acceptables sont prévues comptent, sans toutefois s'y limiter, les technologies d'accès à distance et sans fil, les ordinateurs portables, les tablettes, les téléphones portables et les supports électroniques amovibles, l'utilisation de la messagerie électronique et l'utilisation d'Internet.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.3 Les risques pour l'environnement des données des titulaires de cartes sont formellement identifiés, évalués et gérés.							
12.3.1	Pour chaque exigence du standard PCI DSS qui spécifie l'accomplissement d'une analyse de risque ciblée, l'analyse est documentée et comprend : • L'identification des actifs à protéger. • L'identification de la ou des menaces contre lesquelles l'exigence protège. • L'identification des facteurs qui contribuent à la probabilité et/ou à l'impact d'une menace. • L'analyse résultante qui détermine et inclut la justification de la manière dont la fréquence et les processus définis par l'entité pour satisfaire à l'exigence minimisent la probabilité et/ou l'impact de la menace qui se matérialise. • L'examen de chaque analyse ciblée de risque au moins une fois tous les 12 mois afin de déterminer si les résultats sont toujours valides ou si une analyse de risque mise à jour est nécessaire • La réalisation d'analyses de risques mises à jour au besoin, tel que déterminé par l'examen annuel.	• Examiner les politiques et les procédures documentées.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
12.3.2	***Cette exigence est spécifique à l'Approche Personnalisée et ne s'applique pas aux entités remplissant un Questionnaire d'Auto-Évaluation.***						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.3.3	Les suites de chiffrement cryptographiques et les protocoles utilisés sont documentés et examinés au moins une fois tous les 12 mois, y compris au moins les éléments suivants : • Un inventaire tenu à jour de toutes les suites et protocoles de chiffrement cryptographiques utilisés, y compris le but et le lieu d'utilisation. • Une surveillance active des tendances de l'industrie concernant la viabilité continue de toutes les suites et protocoles de chiffrement cryptographiques utilisés. • Une documentation d'un plan pour répondre aux changements anticipés des vulnérabilités cryptographiques.	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'exigence s'applique à toutes les suites et protocoles cryptographiques chiffrements utilisés pour répondre aux exigences du standard PCI DSS, y compris, sans toutefois s'y limiter, ceux utilisés pour rendre les PAN illisibles lors du stockage et de la transmission, pour protéger les mots de passe et dans le cadre de l'authentification de l'accès. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.3.4	Les technologies matérielles et logicielles utilisées sont examinées au moins une fois tous les 12 mois, y compris au moins les éléments suivants : • Une analyse selon laquelle les technologies continuent de recevoir rapidement des correctifs de sécurité des fournisseurs. • Une analyse selon laquelle les technologies continuent de prendre en charge (et n'empêchent pas) la conformité au standard PCI DSS de l'entité. • Une documentation de toute annonce ou tendance de l'industrie liée à une technologie ; par exemple, lorsqu'un fournisseur annonce des plans de « fin de vie » pour une technologie. • Une documentation d'un plan, approuvé par la haute direction, afin d'appliquer des correctifs aux technologies obsolètes, y compris celles pour lesquelles les fournisseurs ont annoncé des plans de « fin de vie ».	• Examiner la documentation. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS*						
12.4 La conformité au standard PCI DSS est gérée.							
12.4.1	***Exigences supplémentaires pour les prestataires de services uniquement.***						
12.4.2	***Exigences supplémentaires pour les prestataires de services uniquement.***						
12.4.2.1	***Exigences supplémentaires pour les prestataires de services uniquement.***						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.5 Le périmètre du standard PCI DSS est documenté et validé.							
12.5.1	Un inventaire des composants système qui sont dans le périmètre du standard PCI DSS, y compris une description de la fonction ou de l'utilisation, est maintenu et tenu à jour.	• Examiner l'inventaire. • Interroger le personnel.	☐	☐	☐	☐	☐
12.5.2	Le périmètre du standard PCI DSS est documentée et confirmée par l'entité au moins une fois tous les 12 mois et en cas de modification importante de l'environnement dans le périmètre.	• Examiner les résultats documentés des examens des périmètres. • Interroger le personnel.	☐	☐	☐	☐	☐
	Au minimum, la validation du périmètre comprend :						
	• Identifier tous les flux de données pour les différentes étapes de paiement (par exemple, l'autorisation, la capture des règlements, les rétro facturations et les remboursements) et les canaux d'acceptation (par exemple, la carte présente, la carte non présente et le commerce électronique).	• Examiner les résultats documentés des examens des périmètres.	☐	☐	☐	☐	☐
	• Mettre à jour tous les diagrammes de flux de données conformément à l'exigence 1.2.4.		☐	☐	☐	☐	☐
	• Identifier tous les emplacements où les données de compte sont stockées, traitées et transmises, y compris, sans toutefois s'y limiter : 1) tous les emplacements en dehors du CDE actuellement défini, 2) les applications qui traitent les CHD, 3) les transmissions entre les systèmes et les réseaux, et 4) les sauvegardes de fichiers.		☐	☐	☐	☐	☐
	• Identifier tous les composants système dans le CDE, connectés au CDE, ou qui pourraient avoir une incidence sur la sécurité du CDE.		☐	☐	☐	☐	☐
	• Identifier toutes les mesures de segmentation utilisée et le ou les environnements à partir desquels le CDE est segmenté, y compris la justification des environnements hors du périmètre. *(suite)*		☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.5.2 *(suite)*	• Identifier toutes les connexions d'entités tierces ayant accès au CDE.		☐	☐	☐	☐	☐
	• Confirmer que tous les flux de données identifiés, les données de compte, les composants système, les mesures de segmentation et les connexions de tiers ayant accès au CDE sont inclus dans le périmètre.		☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette confirmation annuelle du périmètre du standard PCI DSS est une activité qui doit être effectuée par l'entité évaluée, et n'est pas la même que la confirmation du périmètre effectuée par l'évaluateur de l'entité lors de l'évaluation annuelle, et elle n'est pas destinée à être remplacée par celle-ci.						
12.5.2.1	***Exigences supplémentaires pour les prestataires de services uniquement.***						
12.5.3	***Exigences supplémentaires pour les prestataires de services uniquement.***						
12.6 La sensibilisation à la sécurité est une activité continue.							
12.6.1	Un programme formel de sensibilisation à la sécurité est mis en œuvre pour informer tout le personnel de la politique et des procédures de sécurité des informations de l'entité, ainsi que de son rôle dans la protection des données des titulaires de cartes.	• Examiner le programme de sensibilisation à la sécurité.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.6.2	Le programme de sensibilisation à la sécurité est : • Examiné au moins une fois tous les 12 mois. • Mis à jour si nécessaire pour prendre en compte toute nouvelle menace et vulnérabilité susceptible d'avoir une incidence sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles de l'entité, ou les informations fournies au personnel concernant son rôle dans la protection des données des porteurs de cartes.	• Examiner le contenu du programme de sensibilisation à la sécurité. • Examiner les preuves d'examens. • Interroger le personnel.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
12.6.3	Le personnel reçoit une formation de sensibilisation à la sécurité comme suit : • À l'embauche et au moins une fois tous les 12 mois. • Plusieurs modes de communication sont utilisés. • Le personnel confirme au moins une fois tous les 12 mois avoir lu et compris la politique et les procédures de sécurité des informations.	• Examiner les dossiers du programme de sensibilisation à la sécurité. • Interroger le personnel concerné. • Examiner les supports du programme de sensibilisation à la sécurité. • Examiner les confirmations du personnel.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.6.3.1	La formation de sensibilisation à la sécurité comprend la sensibilisation aux menaces et aux vulnérabilités qui pourraient avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles, y compris, sans toutefois s'y limiter : • Hameçonnage et attaques associées. • Ingénierie sociale.	• Examiner le contenu de la formation de sensibilisation à la sécurité.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Voir l'exigence 5.4.1 dans le standard PCI DSS pour des conseils sur la différence entre les mesures de sécurité techniques et automatisés pour détecter et protéger les utilisateurs contre les attaques d'hameçonnage, et cette exigence pour fournir aux utilisateurs une formation de sensibilisation à la sécurité sur l'hameçonnage et l'ingénierie sociale. Ce sont deux exigences séparées et distinctes, et l'une n'est pas satisfaite par la mise en œuvre des mesures de sécurité requises par l'autre. *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
12.6.3.2	La formation de sensibilisation à la sécurité comporte la sensibilisation à l'utilisation acceptable des technologies de l'utilisateur final conformément à l'exigence 12.2.1.	• Examiner le contenu de la formation de sensibilisation à la sécurité.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.7 Le personnel est contrôlé afin de réduire les risques d'attaques internes.							
12.7.1	Le personnel potentiel qui aura accès au CDE est contrôlé, dans les limites des lois locales, avant l'embauche afin de minimiser le risque d'attaques provenant de sources internes.	• Interroger le personnel de gestion responsable du service des ressources humaines.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Pour le personnel potentiel à embaucher pour des postes tels que les caissiers de magasin, qui n'ont accès qu'à un seul numéro de carte à la fois lors de la facilitation d'une transaction, cette exigence n'est qu'une recommandation.						
12.8 Le risque pour les fonds documentaires associés aux relations avec les prestataires de services tiers (TPSP) est géré.							
12.8.1	Une liste de tous les prestataires de services tiers (TPSP) avec lesquels les données de compte sont partagées ou qui pourraient affecter la sécurité des données de compte, est conservée, y compris une description pour chacun des services fournis.	• Examiner les politiques et les procédures. • Examiner la liste des TPSP.	☐	☐	☐	☐	☐
	Notes d'Applicabilité L'utilisation d'un TPSP conforme au standard PCI DSS ne rend pas une entité conforme au standard PCI DSS, ni ne supprime la responsabilité de l'entité quant à sa propre conformité au standard PCI DSS.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.8.2	Les accords écrits avec les TPSP sont maintenus comme suit : • Des accords écrits sont maintenus avec tous les TPSP avec lesquels les données de compte sont partagées ou qui pourraient avoir une incidence sur la sécurité du CDE. • Les accords écrits comprennent des reconnaissances des TPSP que les TPSP sont responsables de la sécurité des données de carte que les TPSP possèdent ou autrement stockent, traitent ou transmettent au nom de l'entité, ou dans la mesure où les TPSP pourraient avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles de l'entité.	• Examiner les politiques et les procédures. • Examiner les accords écrits avec les TPSP.	☐	☐	☐	☐	☐
	Notes d'Applicabilité La formulation exacte d'un accord dépendra des détails du service fourni et des responsabilités attribuées à chaque partie. L'accord n'a pas à inclure la formulation exacte fournie dans cette exigence. La reconnaissance écrite du TPSP est une confirmation qui déclare que le TPSP est responsable de la sécurité des données de carte qu'il peut stocker, traiter ou transmettre au nom du client ou dans la mesure où le TPSP peut avoir un impact sur la sécurité des données du titulaire de carte d'un client et/ ou des données d'authentification sensibles. La preuve qu'un TPSP respecte les exigences du standard PCI DSS n'est pas la même chose qu'une reconnaissance écrite spécifiée dans cette exigence. Par exemple, une attestation de conformité PCI DSS (AOC), une déclaration sur le site Web d'une entreprise, une déclaration de politique, une matrice de responsabilité ou toute autre preuve non incluse dans un accord écrit ne constitue pas une reconnaissance écrite.						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.8.3	Un processus établi est mis en œuvre pour engager les TPSP, y compris une diligence raisonnable appropriée avant l'engagement.	• Examiner les politiques et les procédures. • Examiner les justificatifs. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.8.4	Un programme est mis en œuvre pour surveiller l'état de conformité au standard PCI DSS des TPSP au moins une fois tous les 12 mois.	• Examiner les politiques et les procédures. • Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Lorsqu'une entité passe un accord avec un TPSP pour satisfaire aux exigences du standard PCI DSS au nom de l'entité (par exemple, via un service de pare-feu), l'entité doit collaborer avec le TPSP pour s'assurer que les exigences applicables du standard PCI DSS sont satisfaites. Si le TPSP ne satisfait pas aux exigences applicables du standard PCI DSS, ces exigences ne sont pas non plus « En Place » chez l'entité.						
12.8.5	Des informations sont conservées sur les exigences du standard PCI DSS qui sont gérées par chaque TPSP, celles qui sont gérées par l'entité et celles qui sont partagées entre le TPSP et l'entité.	• Examiner les politiques et les procédures. • Examiner la documentation. • Interroger le personnel responsable.	☐	☐	☐	☐	☐
12.9 Les prestataires de services tiers (TPSP) prennent en charge la conformité du standard PCI DSS de leurs clients.							
12.9.1	***Exigences supplémentaires pour les prestataires de services uniquement.***						
12.9.2	***Exigences supplémentaires pour les prestataires de services uniquement.***						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.10 Les incidents de sécurité soupçonnés et confirmés qui pourraient avoir un impact sur le CDE sont traités immédiatement.							
12.10.1	Un plan de réponse aux incidents existe et est prêt à être activé en cas d'incident de sécurité soupçonné ou avéré. Le plan comprend, mais n'est pas limité à : • Les rôles, responsabilités et stratégies de communication et de contact en cas d'incident de sécurité soupçonné ou avéré, y compris la notification des marques de paiement et des acquéreurs, au minimum. • Les procédures de réponse aux incidents avec des activités de confinement et d'atténuation spécifiques pour différents types d'incidents. • Les procédures de reprise et de continuité de l'activité. • Les processus de sauvegarde des données. • L'analyse des exigences légales en matière de signalement des compromissions. • La couverture et les réponses de tous les composants système critiques. • La référence ou l'inclusion des procédures de réponse aux incidents des marques de paiement.	• Examiner le plan de réponse aux incidents. • Interroger le personnel. • Examiner la documentation des incidents précédemment signalés.	☐	☐	☐	☐	☐
12.10.2	Au moins une fois tous les 12 mois, le plan de réponse aux incidents de sécurité est : • Examinées et le contenu est mis à jour au besoin. • Testé, y compris tous les éléments énumérés à l'exigence 12.10.1.	• Interroger le personnel. • Examiner la documentation.	☐	☐	☐	☐	☐
12.10.3	Un personnel spécifique est désigné pour être disponible 24h/24 et 7j/7 pour répondre aux incidents de sécurité soupçonnés ou avérés.	• Interroger le personnel responsable. • Examiner la documentation.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.10.4	Le personnel chargé de répondre aux incidents de sécurité soupçonnés et avérés est formé de manière appropriée et périodique sur ses responsabilités en matière de réponse aux incidents.	• Interroger le personnel chargé des réponses aux incidents. • Examiner la documentation de formation.	☐	☐	☐	☐	☐
12.10.4.1	La fréquence des formations périodiques pour le personnel d'intervention en cas d'incident est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.	• Examiner l'analyse des risques ciblée.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Exigence de PCI DSS		Tests Prévus	Réponse ♦ (Cocher une réponse pour chaque exigence)				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.10.5	Le plan de réponse aux incidents de sécurité comprend la surveillance et la réponse aux alertes des systèmes de surveillance de la sécurité, y compris, sans toutefois s'y limiter : • Systèmes de détection et de prévention des intrusions. • Mesures de sécurité réseau. • Mécanismes de détection des modifications pour les fichiers critiques. • Mécanisme de détection des modifications et des altérations pour les pages de paiement. *Ce point est une bonne pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes d'Applicabilité ci-dessous pour plus de détails.* • Détection des points d'accès sans fil *non autorisés*.	• Examiner la documentation. • Observer les processus de réponse aux incidents.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *La puce ci-dessus (pour surveiller et répondre aux alertes d'un mécanisme de détection des modifications et des altérations pour les pages de paiement) est une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire dans le cadre de l'exigence 12.10.5 et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						
12.10.6	Le plan de réponse aux incidents de sécurité est modifié et mis à niveau en fonction des leçons apprises et pour intégrer les développements de l'industrie.	• Examiner les politiques et les procédures. • Examiner le plan de réponse aux incidents de sécurité. • Interroger le personnel responsable.	☐	☐	☐	☐	☐

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
12.10.7	Des procédures d'intervention en cas d'incident sont En Place, à déclencher dès la détection d'un PAN stocké là où il n'est pas prévu, et comprennent : • Déterminer ce qu'il faut faire si le PAN est découvert en dehors du CDE, y compris sa récupération, sa suppression sécurisée et/ou sa migration vers le CDE actuellement défini, selon le cas. • Identifier si des données d'authentification sensibles sont stockées avec le PAN. • Déterminer d'où proviennent les données de compte et comment elles se sont retrouvées là où elles n'étaient pas prévues. • Corriger les fuites de données ou les lacunes des processus qui ont fait que les données de compte se trouvaient là où elles n'étaient pas prévues.	• Examiner les procédures documentées de réponse aux incidents. • Interroger le personnel. • Examiner les enregistrements des actions de réponse.	☐	☐	☐	☐	☐
	Notes d'Applicabilité *Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.*						

Annexe A : Autres Exigences du Standard PCI DSS

Annexe A1 : Autres Exigences du Standard PCI DSS pour les Prestataires de Services Mutualisés

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

Annexe A2 : Autres Exigences du Standard PCI DSS pour les Entités Utilisant SSL/TLS Obsolète pour les Connexions de Terminaux POS POI avec Carte

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
A2.1 Les terminaux POI utilisant SSL et/ou TLS initial ne sont pas sensibles aux exploits SSL/TLS connus.							
A2.1.1	Lorsque les terminaux POS POI du commerçant ou du lieu d'acceptation des paiements utilisent SSL et/ou TLS initial, l'entité confirme que les appareils ne sont pas susceptibles à des exploits connus pour ces protocoles.	• Examiner la documentation (par exemple, la documentation du fournisseur, les détails de la configuration du système/du réseau) qui vérifie que les appareils ne sont pas sensibles à des exploits connus pour les protocoles SSL/TLS initial.	☐	☐	☐	☐	☐
	Notes d'Applicabilité Cette exigence est destinée à s'appliquer à l'entité disposant du terminal POS POI, telle qu'un commerçant. Cette exigence n'est pas destinée aux prestataires de services qui servent de point de terminaison ou de connexion à ces terminaux POS POI. Les exigences A2.1.2 et A2.1.3 s'appliquent aux prestataires de services POS POI. L'allocation pour les terminaux POS POI qui ne sont pas actuellement sensibles aux exploits est basée sur les risques actuellement connus. Si de nouveaux exploits sont introduits auxquels les terminaux POS POI sont sensibles, les terminaux POS POI devront être mis à jour immédiatement.						

♦ *Se reporter à la section « Réponses aux Exigences » (page vi) pour plus d'informations sur ces options de réponse.*

Exigence de PCI DSS		Tests Prévus	Réponse ♦ *(Cocher une réponse pour chaque exigence)*				
			En Place	En Place avec CCW	Non Applicable	Non Testé	Pas en Place
A2.1.2	***Exigences supplémentaires pour les prestataires de services uniquement.***						
A2.1.3	***Exigences supplémentaires pour les prestataires de services uniquement.***						

Annexe A3 : Validation Complémentaire des Entités Désignées (DESV)

Cette Annexe s'applique uniquement aux entités désignées par une ou des marques de paiement ou un acquéreur comme nécessitant une validation supplémentaire des exigences existantes du standard PCI DSS. Les entités tenues de valider cette Annexe doivent utiliser le modèle de rapport supplémentaire DESV et l'Attestation de Conformité supplémentaire pour les rapports, et consulter la marque de paiement et/ou l'acquéreur applicables pour les procédures de soumission.

Annexe B : Feuille de Travail des Mesures de Sécurité Compensatoires

Cette Annexe doit être remplie pour définir les mesures de sécurité compensatoires pour toute exigence dans laquelle l'option En Place avec CCW a été sélectionné.

***Remarque :** Seules les entités qui ont une contrainte technologique ou commerciale légitime et documentée peuvent envisager l'utilisation de mesures de sécurité compensatoires pour satisfaire à la conformité.*

Se reporter aux Annexes B et C du standard PCI DSS afin d'obtenir des informations sur les mesures de sécurité compensatoires et des conseils sur la façon de remplir cette feuille de travail.

Numéro et Définition de l'Exigence :

	Informations Requises	Explication
1. Contraintes	Documenter les contraintes techniques ou commerciales légitimes empêchant la conformité à l'exigence d'origine.	
2. Définition des Mesures Compensatoires	Définir les mesures de sécurité compensatoires : expliquer comment ils répondent aux objectifs du contrôle d'origine et au risque accru, le cas échéant.	
3. Objectif	Définir l'objectif de la mesure de sécurité d'origine.	
	Identifier l'objectif atteint par la mesure de sécurité compensatoire. ***Remarque :** Cela peut être, mais n'a pas besoin d'être, l'objectif de l'Approche Personnalisée indiqué pour cette exigence dans le standard PCI DSS.*	
4. Risque Identifié	Identifier tout risque supplémentaire posé par l'absence de la mesure de sécurité d'origine.	
5. Validation des Mesures de Sécurité Compensatoires	Définir la manière dont les mesures de sécurité compensatoires ont été validées et testées.	
6. Maintenance	Définir le ou les processus et les mesures de sécurité En Place pour maintenir les mesures de sécurité compensatoires.	

Annexe C : Explication des Exigences Indiquées comme Non Applicables

Cette Annexe doit être remplie pour chaque exigence pour laquelle l'option Non Applicable a été sélectionnée.

Exigence	Raison pour laquelle l'Exigence est Non Applicable
Par exemple :	
Exigence 3.5.1	*Les données de compte ne sont jamais stockées par voie électronique*

Annexe D : Explication des Exigences Indiquées comme Non Testées

Cette Annexe doit être remplie pour chaque exigence pour laquelle l'option Non Testée a été sélectionnée.

Exigence	Description de la ou les exigences Non Testées	Décrire pourquoi les exigences ont été exclues de l'évaluation
Exemples :		
Exigence 10	*Aucune exigence de l'Exigence 10 n'a été testée.*	*Cette évaluation ne couvre que les exigences de l'étape 1 de l'approche prioritaire.*
Exigences 1-8, 10-12	*Seule l'exigence 9 a été examinée pour cette évaluation. Toutes les autres exigences ont été exclues.*	*L'entreprise est un fournisseur d'hébergement physique (CO-LO), et seuls les mesures de sécurité physiques ont été pris en compte pour cette évaluation.*

Section 3 : Détails de la Validation et de l'Attestation

Partie 3. Validation du Standard PCI DSS

Cette AOC est basée sur les résultats notés dans le SAQ C (Section 2), en date du (Date d'achèvement de l'auto-évaluation *JJ-MM-AAAA*).

Indiquer ci-dessous si une évaluation complète ou partielle du standard PCI DSS a été effectuée :

☐ **Complète** – toutes les exigences ont été évaluées ; par conséquent, aucune exigence n'a été marquée comme Non Testée dans le SAQ.

☐ **Partielle** – Une ou plusieurs exigences n'ont pas été évaluées et ont donc été marquées comme Non Testées dans le SAQ. Toute exigence non évaluée est notée comme Non Testée dans la partie 2g ci-dessus.

Sur la base des résultats documentés dans le SAQ D indiqué ci-dessus, chaque signataire identifié dans l'une des parties 3b-3d, selon le cas, affirme le statut de conformité suivant pour le commerçant identifié dans la partie 2 de ce document.

Sélectionner une Option :

☐	**Conforme :** Toutes les sections du SAQ du standard PCI DSS sont complètes et toutes les exigences évaluées sont marquées comme étant soit 1) En Place, 2) En Place avec CCW, ou 3) Non Applicable, ce qui donne une note globale **CONFORME** ; ainsi (*Nom de l'Entreprise du Commerçant*) a démontré sa conformité à toutes les exigences du standard PCI DSS incluses dans ce SAQ, à l'exception de celles indiquées comme Non Testées ci-dessus.
☐	**Non Conforme :** Toutes les sections du SAQ du standard PCI DSS ne sont pas complètes, ou une ou plusieurs exigences sont marquées comme Pas en Place, ce qui entraîne une note globale **NON CONFORME** ; ainsi (*Nom de l'Entreprise du Commerçant*) n'a pas démontré sa conformité aux exigences du standard PCI DSS incluses dans ce SAQ **Date cible** pour la conformité : *JJ-MM-AAAA* Un commerçant soumettant ce formulaire avec un statut Non conforme peut être tenu de remplir le plan d'action de la partie 4 du présent document. Confirmer avec l'entité à laquelle cette AOC sera soumise *avant de remplir la partie 4.*
☐	**Conforme mais avec une exception Légale :** Une ou plusieurs exigences évaluées dans le PCI DSS sont marquées comme Pas en Place en raison d'une restriction légale qui empêche l'exigence d'être satisfaite, et toutes les autres exigences évaluées sont marquées comme étant soit 1) En Place, 2) En Place avec CCW, ou 3) Non Applicable, résultant en une note globale **CONFORME MAIS AVEC UNE EXCEPTION LÉGALE** ; ainsi (*Nom de l'Entreprise du Commerçant*) a démontré sa conformité à toutes les exigences du standard PCI DSS incluses dans ce SAQ à l'exception de celles marquées comme Non Testées ci-dessus ou Pas en Place en raison d'une restriction légale. Cette option nécessite un examen supplémentaire de la part de l'entité à laquelle cet AOC sera soumis. *Si l'option est sélectionnée, remplir ce qui suit :*

Exigence Touchée	Détails de la façon dont la contrainte légale empêche l'exigence d'être satisfaite

Partie 3a. Confirmation du Commerçant

Le ou les signataires confirment :

(Sélectionner toutes les options qui s'appliquent)

☐	Le Questionnaire d'Auto-Évaluation D du standard PCI DSS, version 4.0.1 a été rempli conformément aux instructions qui y figurent.
☐	Toutes les informations contenues dans le SAQ susmentionné et dans cette attestation représentent fidèlement les résultats de l'évaluation du commerçant à tous les égards importants.
☐	Les mesures de sécurité du standard PCI DSS seront maintenues à tout moment, selon l'environnement du commerçant.

Partie 3b. Attestation du Commerçant

Signature du Cadre Dirigeant du Commerçant ↑	*Date : JJ-MM-AAAA*
Nom du Cadre Dirigeant du Commerçant :	*Titre :*

Partie 3c. Confirmation de l'Auditeur de Sécurité Qualifié (QSA)

Si un QSA a participé ou contribué à cette évaluation, indiquer le rôle joué :	☐ Le QSA a effectué des procédures de test.
	☐ Le QSA a fourni une autre aide. Si l'option est sélectionnée, décrire tous les rôles joués :

Signature du QSA principal ↑	*Date : JJ-MM-AAAA*
Nom du QSA principal :	

Signature du Dirigeant Dûment Autorisé de l'Entreprise du QSA ↑	*Date : JJ-MM-AAAA*
Nom du Cadre Dirigeant Dûment Autorisé :	*Entreprise du QSA :*

Partie 3d. Participation de l'Auditeur de Sécurité Interne du PCI SSC

Si un ISA a participé ou contribué à cette évaluation, indiquer le rôle joué :	☐ L'ISA a effectué des procédures de test.
	☐ L'ISA a fourni une autre aide. Si l'option est sélectionnée, décrire tous les rôles joués :

Partie 4. Plan d'Action pour les Exigences Non Conformes

Ne remplir la partie 4 qu'à la demande de l'entité à laquelle cette AOC sera soumise, et seulement si l'évaluation a un statut Non conformes indiqués à la section 3.

Si invité à remplir cette section, sélectionner la réponse appropriée pour « Conforme aux exigences de PCI DSS » pour chaque exigence ci-dessous. Pour toute réponse « Non », indiquer la date à laquelle le commerçant s'attend à être conforme à l'exigence et une brève description des mesures prises pour satisfaire à l'exigence.

Exigence de PCI DSS	Description de l'Exigence	Conforme aux Exigences du Standard PCI DSS (Sélectionner une Option)		Date et Mesures de Correction (Si l'option « NON » est sélectionnée pour une exigence)
		OUI	NON	
1	Installer et maintenir des mesures de sécurité du réseau	☐	☐	
2	Appliquer des configurations sécurisées à tous les composants système	☐	☐	
3	Protéger les données de compte stockées	☐	☐	
4	Protéger les données des titulaires de cartes grâce à une cryptographie robuste lors de la transmission sur des réseaux publics ouverts	☐	☐	
5	Protéger tous les systèmes et réseaux contre les logiciels malveillants	☐	☐	
6	Développer et maintenir des systèmes et des logiciels sécurisés	☐	☐	
7	Limiter l'accès aux composants système et aux données des titulaires de cartes en fonction des besoins de l'entreprise	☐	☐	
8	Identifier les utilisateurs et authentifier l'accès aux composants système	☐	☐	
9	Limiter l'accès physique aux données des titulaires de cartes	☐	☐	
10	Enregistrer et surveiller tous les accès aux composants système et aux données des titulaires de cartes	☐	☐	
11	Tester Régulièrement la Sécurité des Systèmes et des Réseaux	☐	☐	
12	Appuyer la Sécurité des Informations avec des Politiques et des Programmes Organisationnels	☐	☐	
Annexe A2	Autres Exigences du Standard PCI DSS pour les entités utilisant SSL/TLS obsolète pour les Connexions de Terminaux POS POI avec carte	☐	☐	

Remarque : *Le PCI Security Standards Council est un organisme de standardisation mondial qui fournit des ressources aux professionnels de la sécurité des paiements, développées en collaboration avec notre communauté de parties prenantes. Nos documents sont acceptés dans de nombreux programmes de conformité à travers le monde. Veuillez vérifier auprès de votre organisme individuel acceptant la conformité pour vous assurer que ce formulaire est acceptable dans son programme. Pour plus d'informations sur le PCI SSC et notre communauté de parties prenantes, veuillez visiter : https://www.pcisecuritystandards.org/about_us/.*