Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation D
et attestation de conformité

Tous les autres commerçants et prestataires de services admissibles QAÉ

Version 2.0

Octobre 2010

Modifications apportées au document

Date	Version	Description
1er octobre 2008	1.2	Harmonisation du contenu avec les nouvelles normes PCI DSS v1.2 et mise en œuvre des changements mineurs notés depuis la v1.1 d'origine.
28 octobre 2010	2.0	Harmonisation du contenu avec les nouvelles exigences PCI DSS v2.0 et procédures de test.

Table des matières

Normes de sécurité des données du PCI : Documents connexes

Les documents suivants ont été conçus de manière à aider les commerçants et les prestataires de services à comprendre les normes PCI DSS et le QAÉ relatif à ces normes.

Document	Public
Normes de sécurité des données du PCI : Conditions et procédures d'évaluation de sécurité	Tous les commerçants et les prestataires de services
Parcourir les PCI DSS : Comprendre l'objectif des exigences	Tous les commerçants et les prestataires de services
Normes de sécurité des données du PCI : Instructions et directives concernant l'auto-évaluation	Tous les commerçants et les prestataires de services
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation A et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation B et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation C-VT et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation C et attestation	Commerçants admissibles[1]
Normes de sécurité des données du PCI : Questionnaire d'auto-évaluation D et attestation	prestataires de services et commerçants admissibles[1]
Normes de sécurité des données du PCI et Normes de sécurité des données de l'application de paiement : Glossaire, abréviations et acronymes	Tous les commerçants et les prestataires de services

[1] Pour définir le questionnaire d'auto-évaluation approprié, consulter le document *Normes de sécurité des données du PCI : Instructions et directives concernant l'auto-évaluation*, « Sélection du questionnaire d'auto-évaluation et de l'attestation les plus appropriés pour l'organisation ».

Avant de commencer

Compléter le questionnaire d'auto-évaluation

Le QAÉ D a été conçu pour tous les prestataires de services pouvant remplir un questionnaire d'auto-évaluation et pour tous les commerçants ne répondant pas aux descriptions des QAÉ A à C indiquées dans le tableau ci-dessous et, de façon plus approfondie, dans les *instructions et directives concernant le questionnaire d'auto-évaluation PCI DSS*.

QAÉ	Description
A	Commerçants carte absente (commerce électronique ou commande par courrier/téléphone), sous-traitance de toutes les fonctions de données de titulaire de carte. *Ne peut s'appliquer aux commerçants en face-à-face.*
B	Commerçants avec dispositifs d'impression uniquement ou commerçants avec terminal par ligne commutée autonome sans stockage électronique de données de titulaire de carte.
C-VT	Commerçants utilisant uniquement des terminaux virtuels basés sur le Web, sans stockage électronique de données de titulaire de carte.
C	Commerçants ayant des systèmes d'application de paiement connectés à Internet, sans stockage électronique de données de titulaire de carte.
D	Tous les autres commerçants (non compris dans les descriptions des QAÉ A à C ci-dessus) et **tous** les **prestataires de services** définis comme admissibles à remplir un QAÉ par une marque de carte de paiement.

Le QAÉ D s'applique aux commerçants admissibles QAÉ ne répondant pas aux critères des QAÉ A à C ci-dessus, et à tous les prestataires de services définis comme admissibles à remplir un QAÉ par une marque de carte de paiement. Les prestataires de services et les commerçants QAÉ D valident leur conformité en remplissant le QAÉ D et l'attestation de conformité associée.
Si la plupart des organisations qui remplissent le QAÉ D doivent obtenir une attestation de conformité pour toutes les exigences des PCI DSS, certaines présentant des modèles commerciaux spécifiques ne sont pas visées par l'ensemble des exigences. Par exemple, une société qui n'utilise pas la technologie sans fil ne se voit pas contrainte d'obtenir une attestation de conformité pour les sections des PCI DSS relatives à la technologie sans fil. Consulter les directives qui suivent pour plus de renseignements sur l'exclusion de la technologie sans fil et d'autres exigences spécifiques.

Chaque section du questionnaire est consacrée à un thème de sécurité spécifique, selon les exigences des normes PCI DSS.

Étapes de mise en conformité avec les normes PCI DSS

1. Évaluer la conformité d'un environnement aux normes PCI DSS.
2. Remplir le questionnaire d'auto-évaluation (QAÉ D) selon les instructions du document *Instructions et directives concernant le questionnaire d'auto-évaluation.*
3. Faire faire une analyse des vulnérabilités par un prestataire de services d'analyse agréé (ASV) par le PCI SSC et se procurer auprès de celui-ci un justificatif de l'exécution réussie de ces analyses.
4. Remplir l'attestation de conformité dans son intégralité.

5. Envoyer le questionnaire, le justificatif d’analyse réussie et l’attestation de conformité, avec tout autre document requis, à l'acquéreur (pour les commerçants) ou à la marque de carte de paiement ou à tout autre demandeur (pour les prestataires de services).

Directives sur la non-applicabilité de certaines exigences spécifiques

Exclusion : s'il est demandé de répondre au QAÉ D pour valider la conformité aux PCI DSS, il est nécessaire de considérer les exceptions suivantes. Se reporter à la section « Non applicabilité » ci-dessous pour la réponse QAÉ appropriée.

- Les questions spécifiques à la technologie sans fil concernent uniquement les organisations dont le réseau est équipé de la technologie sans fil (par exemple, exigences 1.2.3, 2.1.1 et 4.1.1). Il est nécessaire de répondre à l'exigence 11.1 (utilisation d'un processus pour identifier les points d'accès sans fil non autorisés) même si le réseau n'est pas doté de la technologie sans fil car le processus détecte les dispositifs non autorisés ou malveillants qui auraient pu être ajoutés sournoisement.
- Les questions portant sur le code et les applications personnalisés (exigences 6.3 et 6.5) s'adressent uniquement aux organisations développant leurs propres applications personnalisées.
- Les questions des exigences 9.1 à 9.4 concernent uniquement les installations avec des « zones sensibles », comme définies ici. « Zones sensibles », signifie un centre de données, une salle de serveurs ou une zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaire de carte. Cela exclut les zones où seuls des terminaux points de vente sont présents, comme les zones de caisse dans un magasin de vente au détail, mais comprend les salles de serveurs administratifs d'un magasin de vente au détail qui stockent des données de titulaire de carte, et les zones de stockage pour de grandes quantités de données de titulaire de carte.

Non applicabilité : ces exigences et toutes celles jugées non applicables à l'environnement doivent être définies comme telles par la mention « s.o. » dans la colonne « Spécial » du QAÉ. En conséquence, remplir la fiche « Explication de non applicabilité » dans l'annexe pour chaque entrée « s.o. ».

Attestation de conformité, QAÉ D – Version commerçant

Instructions de transmission

Le commerçant doit remplir cette attestation de conformité pour confirmer son statut de conformité avec le document *Normes de sécurité des données du secteur des cartes de paiement (PCI DSS) – Conditions et procédures d'évaluation de sécurité.* Il doit compléter toutes les sections applicables et se reporter aux instructions de transmission au niveau de « Étapes de mise en conformité avec les PCI DSS » dans ce document.

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

Partie 1a. Renseignements sur l'organisation du commerçant

Nom de la société :			DBA(s) :		
Nom du contact :			Poste occupé :		
Téléphone :			Courriel :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					

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

Nom de la société :			
Nom du principal contact QSA :		Poste occupé :	

Téléphone :			Courriel :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					

Partie 2 Type d'entreprise du commerçant (cocher toutes les cases concernées) :

☐ Détaillant ☐ Télécommunications ☐ Épiceries et supermarchés

☐ Pétrole ☐ Commerce électronique ☐ Vente par correspondance/téléphone

☐ Autres (préciser) :

Indiquer les installations et les sites compris dans l'examen PCI DSS :

Partie 2a. Relations

La société entretient-elle une relation avec un ou plusieurs prestataires de services tiers (par exemple, passerelles, sociétés d'hébergement sur le Web, tour opérateurs, agents de programmes de fidélité, etc.)?	☐ Oui ☐ Non
La société entretient-elle une relation avec plusieurs acquéreurs?	☐ Oui ☐ Non

Partie 2b. Traitement des transactions

Comment et dans quelle mesure l'entreprise stocke-t-elle, traite-t-elle et/ou transmet-elle des données de titulaire de carte?

Fournir les renseignements suivants concernant les applications de paiement que l'organisation utilise :

Application de paiement utilisée	**Numéro de version**	**Dernière version validée selon les normes PABP/PA-DSS**

Partie 3. Validation des PCI DSS

En fonction des résultats du QAÉ D du *(date à laquelle il a été rempli)*, *(Nom de la société du commerçant)* déclare le statut de conformité suivant (cocher une case) :

☐ **Conforme :** toutes les sections du QAÉ PCI sont remplies et toutes les questions ont reçu une réponse affirmative, d'où une évaluation globale **CONFORME**, **et** une analyse a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. *(Nom de la société du commerçant)* est donc conforme aux normes PCI DSS.

☐ **Non conforme :** les sections du QAÉ PCI DSS n'ont pas toutes été remplies ou certaines questions n'ont pas reçu la réponse « Oui », d'où une évaluation globale **NON CONFORME**, **ou** aucune analyse n'a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. *(Nom de la société du commerçant)* n'est donc pas conforme aux normes PCI DSS.

Date cible de mise en conformité :

Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à remplir le plan d'action décrit dans la Partie 4 de ce document. *Vérifier ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

Partie 3a. Confirmation de l'état de conformité

Le commerçant confirme les éléments suivants :

☐	Le questionnaire d'auto-évaluation D des PCI DSS, version *(version du QAÉ)*, a été rempli selon les instructions fournies dans ce document.
☐	Tous les renseignements présents dans le questionnaire d'auto-évaluation susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats des évaluations, à tous points de vue.
☐	J'ai obtenu confirmation auprès du fournisseur de l'application de paiement que cette dernière ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu les normes PCI DSS et m'engage à garantir ma conformité avec leurs exigences à tout moment.
☐	Aucune preuve de stockage de données de bandes magnétiques (c'est-à-dire des pistes)[2], de données CAV2, CVC2, CID ou CVV2[3], ou de données du NIP[4] après autorisation de transaction n'a été trouvée sur AUCUN des systèmes examinés pendant cette évaluation.

Partie 3b. Accusé de réception du commerçant

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

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

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

Signature du représentant du commerçant ↑	*Date ↑*
Nom du représentant du commerçant ↑	*Titre ↑*

Nom de la société représentée ↑

Partie 4. Plan d'action en cas d'état Non conforme

Sélectionner l'état de conformité approprié pour chaque exigence. Si la réponse « NON » est donnée à la moindre exigence, indiquer la date à laquelle la société devra se mettre en conformité et une brève description des actions à mettre en œuvre à cette fin. *Vérifier ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

Exigence PCI DSS	Description de l'exigence	État de conformité (cocher une seule option)		Date et actions de mise en conformité (si l'état de conformité est « NON »)
		OUI	NON	
1	Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données de titulaire de carte stockées	☐	☐	
4	Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts	☐	☐	
5	Utiliser des logiciels antivirus et les mettre à jour régulièrement	☐	☐	
6	Développer et gérer des systèmes et des applications sécurisés	☐	☐	
7	Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître	☐	☐	
8	Affecter un ID unique à chaque utilisateur d'ordinateur	☐	☐	
9	Limiter l'accès physique aux données de titulaire de carte	☐	☐	

		État de conformité (cocher une seule option)		
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	
12	Gérer une politique qui adresse les renseignements de sécurité à tout le personnel	☐	☐	

Attestation de conformité, QAÉ D – Version prestataire de services

Instructions de transmission

Le prestataire de services doit remplir cette attestation de conformité pour confirmer son statut de conformité avec le document *Normes de sécurité des données du secteur des cartes de paiement (PCI DSS) – Conditions et procédures d'évaluation de sécurité.* Remplir toutes les sections applicables et se reporter aux instructions de transmission au niveau de « Étapes de mise en conformité avec les PCI DSS » dans ce document.

Partie 1. Renseignements sur le prestataire de services et l'évaluateur de sécurité qualifié

Partie 1a. Renseignements sur l'organisation de prestation de services

Nom de la société :		DBA(s) :	
Nom du contact :		Poste occupé :	
Téléphone :		Courriel :	
Adresse professionnelle :		Ville :	

État/province :		Pays :		Code postal :	
URL :					

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

Nom de la société :	

Nom du principal contact QSA :			Poste occupé :		
Téléphone :			Courriel :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					

Partie 2. Renseignements concernant l'évaluation PCI DSS

Partie 2a. Services fournis COMPRIS dans la portée de l'évaluation PCI DSS (cocher toutes les cases concernées)

☐ Fournisseur d'hébergement sécurisé 3-D	☐Fournisseur d'hébergement – Matériel	☐ Traitement des paiements – GAB
☐ Gestion des comptes	☐ Fournisseur d'hébergement – Web	☐ Traitement des paiements – CCTC
☐ Autorisation	☐ Traitement des émetteurs	☐ Traitement des paiements – Internet
☐ Services administratifs	☐ Programmes de fidélité	☐ Traitement des paiements – Point de vente
☐ Gestion de la facturation	☐ Services gérés	☐ Services prépayés
☐ Compensation et règlement	☐ Services aux commerçants	☐ Gestion des dossiers
☐ Préparation des données	☐ Fournisseur réseau/Transmetteur	☐ Paiements des impôts/au gouvernement
☐ Services des fraudes et des rejets de débits	☐ Portail de paiement/Commutateur	

☐ Autres (préciser) :

Indiquer les installations et les sites compris dans l'examen PCI DSS :

Partie 2b. Si certains des services indiqués sont fournis par le prestataire de services mais *NE SONT PAS COMPRIS* dans la portée de l'évaluation PCI DSS, les cocher ci-dessous :		
☐ Fournisseur d'hébergement sécurisé 3-D	☐Fournisseur d'hébergement – Matériel	☐ Traitement des paiements – GAB
☐ Gestion des comptes	☐ Fournisseur d'hébergement – Web	☐ Traitement des paiements – CCTC
☐ Autorisation	☐ Traitement des émetteurs	☐ Traitement des paiements – Internet
☐ Services administratifs	☐ Programmes de fidélité	☐ Traitement des paiements – Point de vente
☐ Gestion de la facturation	☐ Services gérés	☐ Services prépayés
☐ Compensation et règlement	☐ Services aux commerçants	☐ Gestion des dossiers
☐ Préparation des données	☐ Fournisseur réseau/Transmetteur	☐ Paiements des impôts/au gouvernement
☐ Services des fraudes et des rejets de débits	☐ Portail de paiement/Commutateur	
☐ Autres (préciser) :		

Partie 2c. Relations		
La société entretient-elle une relation avec un ou plusieurs prestataires de services tiers (par exemple, passerelles, sociétés d'hébergement sur le Web, tour opérateurs, agents de programmes de fidélité, etc.)?	☐ Oui	☐ Non

Partie 2d. Traitement des transactions

Comment et dans quelle mesure l'entreprise stocke-t-elle, traite-t-elle et/ou transmet-elle des données de titulaire de carte?

Application de paiement utilisée	**Numéro de version**	**Dernière version validée selon les normes PABP/PA-DSS**

Fournir les renseignements suivants concernant les applications de paiement que l'organisation utilise :

Partie 3. Validation des PCI DSS

Suite aux résultats du QAÉ D du *(date à laquelle il a été rempli)*, *(Nom de la société de prestation de services)* déclare le statut de conformité suivant (cocher une case) :

☐ **Conforme :** toutes les sections du QAÉ PCI sont remplies et toutes les questions ont reçu la réponse « Oui », d'où une évaluation globale **CONFORME**, **et** une analyse a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. *(Nom de la société de prestation de services)* est donc conforme aux normes PCI DSS.

☐ **Non conforme :** les sections du QAÉ PCI n'ont pas toutes été remplies ou certaines questions ont reçu la réponse « Non », d'où une évaluation globale **NON CONFORME**, **ou** aucune analyse n'a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. *(Nom de la société de prestation de services)* n'est donc pas conforme aux normes PCI DSS.

Date cible de mise en conformité :

Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à remplir le plan d'action décrit dans la Partie 4 de ce document. *Vérifier ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas*.

Partie 3a. Confirmation de l'état de conformité

Le prestataire de services confirme les éléments suivants :

☐	Le questionnaire d'auto-évaluation D, version *(indiquer le numéro de version)*, a été rempli conformément aux instructions fournies dans ce document.
☐	Tous les renseignements présents dans le questionnaire d'auto-évaluation susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de l'évaluation.
☐	J'ai lu les normes PCI DSS et m'engage à garantir ma conformité avec leurs exigences à tout moment.
☐	Aucune preuve de stockage de données de bandes magnétiques (c'est-à-dire des pistes)[5], de données CAV2, CVC2, CID ou CVV2[6], ou de données du NIP[7] après autorisation de transaction n'a été trouvée sur AUCUN des systèmes examinés pendant cette évaluation.

Partie 3b. Accusé de réception du prestataire de services

Signature du représentant du prestataire de services ↑	*Date* ↑
Nom du représentant du prestataire de services ↑	*Titre* ↑

Nom de la société représentée ↑

Partie 4. Plan d'action en cas d'état Non conforme

Sélectionner l'état de conformité approprié pour chaque exigence. Si la réponse « NON » est donnée à la moindre exigence, indiquer la date à laquelle la société devra se mettre en conformité et une brève description des actions à mettre en œuvre à cette fin. *Vérifier ce renseignement auprès de l'acquéreur ou de la marque de carte de paiement avant de remplir la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

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

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

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

Exigence PCI DSS	Description de l'exigence	État de conformité (cocher une seule option)		Date et actions de mise en conformité (si l'état de conformité est « NON »)
		OUI	NON	
1	Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données de titulaire de carte stockées	☐	☐	
4	Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts	☐	☐	
5	Utiliser des logiciels antivirus et les mettre à jour régulièrement	☐	☐	
6	Développer et gérer des systèmes et des applications sécurisés	☐	☐	
7	Limiter l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître	☐	☐	
8	Affecter un ID unique à chaque utilisateur d'ordinateur	☐	☐	
9	Limiter l'accès physique aux données de titulaire de carte	☐	☐	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	
12	Gérer une politique qui adresse les renseignements de sécurité à tout le personnel	☐	☐	

Questionnaire d'auto-évaluation D

Remarque : *les questions suivantes sont numérotées conformément aux exigences et procédures de test des normes PCI DSS, comme défini dans le document* Conditions et procédures d'évaluation de sécurité des normes PCI DSS*.*

Date de réalisation :

Création et gestion d'un réseau sécurisé

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

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
1.1	Les normes de configuration définies des pare-feu et des routeurs comprennent-elles les éléments suivants :				
	1.1.1	Existe-t-il un processus formel d'approbation et de test de toutes les connexions réseau externes et des modifications apportées aux configurations des pare-feu et des routeurs?	☐	☐	
	1.1.2	(a) Existe-t-il un schéma de réseau actuel (par exemple, montrant les flux de données de titulaire de carte sur le réseau) et documente-t-il toutes les connexions aux données de titulaire de carte, y compris les réseaux sans fil?	☐	☐	
		(b) Le schéma est-il tenu à jour?	☐	☐	
	1.1.3	(a) Les normes de configuration comprennent-elles des exigences pour un pare-feu à chaque connexion Internet et entre la zone démilitarisée (DMZ) et la zone de réseau interne?	☐	☐	
		(b) Le schéma de réseau actuel est-il cohérent avec les normes de configuration des pare-feu?	☐	☐	
	1.1.4	Les normes de configuration des pare-feu et des routeurs comprennent-elles une description des groupes, des rôles et des responsabilités pour la gestion logique des composants de réseau?	☐	☐	
	1.1.5	(a) Les normes de configuration des pare-feu et des routeurs comprennent-elles une liste documentée des services, protocoles et ports nécessaires à l'activité – par exemple, le protocole de transfert hypertexte (HTTP), le protocole SSL, le protocole SSH, et les protocoles de réseaux privés virtuels (VPN)?	☐	☐	
		(b) Tous les services, protocoles et ports non sécurisés autorisés sont-ils nécessaires, et les fonctions de sécurité sont-elles documentées et mises en œuvre pour chacun? *Remarque : des exemples de services, protocoles, ou ports non sécurisés comprennent, mais sans s'y limiter, FTP, Telnet, POP3, IMAP et SNMP.*	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	1.1.6	(a) Les normes de configuration des pare-feu et des routeurs exigent-elles un examen des règles des pare-feu et des routeurs au moins tous les six mois?	☐	☐	
		(b) Les ensembles de règles des pare-feu et des routeurs sont-ils examinés au moins tous les six mois?	☐	☐	
1.2	Les configurations de pare-feu limitent-elles les connexions entre les réseaux non approuvés et les systèmes dans l'environnement des données de titulaire de carte, comme suit : *Remarque : un « réseau non approuvé » est un réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.*				
	1.2.1	(a) Le trafic entrant et sortant est-il limité au trafic nécessaire à l'environnement des données de titulaire de carte, et ces limitations sont-elles documentées?	☐	☐	
		(b) Tous les autres trafics entrants et sortants sont-ils spécifiquement refusés (par exemple en utilisant un paramètre « refuser tout » explicite ou un refus implicite après une autorisation)?	☐	☐	
	1.2.2	Les fichiers de configuration du routeur sont-ils sécurisés et synchronisés?	☐	☐	
	1.2.3	Des pare-feu de périmètre sont-ils installés entre tous les réseaux sans fil et l'environnement des données de titulaire de carte, et ces pare-feu sont-ils paramétrés pour refuser ou contrôler le trafic (si celui-ci est nécessaire pour des raisons professionnelles) de l'environnement sans fil vers l'environnement des données de titulaire de carte?	☐	☐	
1.3	La configuration de pare-feu empêche-t-elle l'accès public direct entre Internet et les composants du système dans l'environnement des données de titulaire de carte comme suit :				
	1.3.1	Une zone démilitarisée est-elle mise en œuvre pour limiter le trafic entrant aux seuls composants du système qui fournissent les services, les protocoles, et les ports autorisés accessibles au public?	☐	☐	
	1.3.2	Le trafic Internet entrant est-il limité aux adresses IP dans la zone démilitarisée?	☐	☐	
	1.3.3	Les connexions directes sont-elles bannies pour le trafic entrant ou sortant entre Internet et l'environnement des données de titulaire de carte?	☐	☐	
	1.3.4	Le passage des adresses internes d'Internet dans la zone démilitarisée est-il proscrit?	☐	☐	
	1.3.5	Le trafic sortant de l'environnement des données de titulaire de carte vers Internet est-il explicitement autorisé?	☐	☐	
	1.3.6	Un contrôle avec état, également appelé « filtrage dynamique à paquets » est-il mis en place (seules les connexions établies sont autorisées sur le réseau)?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	1.3.7	Les composants du système qui stockent les données de titulaire de carte (comme une base de données) sont-ils placés dans une zone de réseau interne, distincte de la zone démilitarisée et d'autres réseaux non approuvés?	☐	☐	
	1.3.8	(a) Des méthodes sont-elles en place pour empêcher la divulgation d'adresses IP et de renseignements d'acheminement privés des réseaux internes vers Internet? ***Remarque** : les méthodes pour rendre les adresses IP illisibles peuvent comprendre, mais sans s'y limiter :* • *la traduction d'adresse de réseau (NAT);* • *la mise en place de serveurs contenant des données de titulaire de carte derrière des serveurs/pare-feu proxy ou des caches de contenu;* • *l'enlèvement ou le filtrage des avertissements d'acheminement pour les réseaux privés qui emploient des adresses enregistrées;* • *l'usage interne de l'espace adresse RFC1918 au lieu d'adresses enregistrées.*	☐	☐	
		(b) La divulgation d'adresses IP privées et de renseignements d'acheminement aux entités externes est-elle autorisée?	☐	☐	
1.4		(a) Un logiciel pare-feu personnel est-il installé sur les ordinateurs portables et/ou ordinateurs appartenant à des employés équipés d'une connexion directe à Internet (par exemple, ordinateurs portables dont se servent les employés), qui sont utilisés pour accéder au réseau de l'organisation?	☐	☐	
		(b) Le logiciel pare-feu personnel est-il configuré selon des normes spécifiques et ne peut-il pas être altéré par les utilisateurs d'ordinateurs portables et/ou ordinateurs appartenant à un employé?	☐	☐	

Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
2.1	Les paramètres par défaut définis par le fournisseur sont-ils systématiquement modifiés avant d'installer un système sur le réseau? *Les paramètres par défaut définis par le fournisseur comprennent, mais sans s'y limiter, les mots de passe et les protocoles de gestion de réseau simples (SNMP), et l'élimination des comptes qui ne sont pas nécessaires.*		☐	☐	
2.1.1	Dans les environnements sans fil connectés à l'environnement de données de titulaire de carte ou la transmission de données de titulaire de carte, les paramètres par défaut sont-ils modifiés comme suit :				
	(a) Les clés de cryptage par défaut sont-elles changées à l'installation, et chaque fois que quelqu'un ayant eu connaissance de ces clés a quitté la société ou changé de poste?		☐	☐	
	(b) Les chaînes de communauté SNMP par défaut sur les dispositifs sans fil sont-elles changées?		☐	☐	
	(c) Les mots de passe/phrases passe par défaut sur les points d'accès sont-ils changés?		☐	☐	
	(d) Le micrologiciel sur les dispositifs sans fil est-il mis à jour afin de prendre en charge un cryptage performant pour l'authentification et la transmission sur les réseaux sans fil?		☐	☐	
	(e) Les autres paramètres par défaut du fournisseur du dispositif sans fil, relatifs à la sécurité, sont-ils changés, le cas échéant?		☐	☐	
2.2	(a) Des normes de configuration sont-elles développées pour tous les composants du système et sont-elles cohérentes avec les normes renforçant les systèmes en vigueur dans le secteur? Les sources des normes renforçant les systèmes en vigueur dans le secteur peuvent comprendre, mais sans s'y limiter, l'Institut SANS (SysAdmin Audit Network Security), le NIST (National Institute of Standards Technology), l'organisation internationale de normalisation (ISO), et le centre pour la sécurité Internet (CIS).		☐	☐	
	(b) Les normes de configuration du système sont-elles mises à jour ainsi que les nouvelles vulnérabilités identifiées, comme défini dans l'exigence 6.2?		☐	☐	
	(c) Les normes de configuration du système sont-elles appliquées lorsque de nouveaux systèmes sont configurés?		☐	☐	
	(d) Les normes de configuration du système comprennent-elles ce qui suit :				

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	2.2.1	(a) Une seule fonction primaire est-elle mise en œuvre par serveur pour empêcher les fonctions nécessitant différents niveaux de sécurité de coexister sur le même serveur? (par exemple, les serveurs Web, les serveurs de base de données, et les serveurs de nom de domaine (DNS) doivent être mis en œuvre sur des serveurs séparés).	☐	☐	
		(b) Si des technologies de virtualisation sont utilisées, une seule fonction primaire est-elle mise en œuvre par composant du système ou par dispositif virtuels?	☐	☐	
	2.2.2	(a) Les seuls services, protocoles, démons, etc. nécessaires sont-ils activés comme exigé par la fonction du système (les services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction spécifiée du dispositif sont désactivés)?	☐	☐	
		(b) Tous les services, démons ou protocoles activés sont-ils justifiés, et les fonctions de sécurité sont-elles documentées et mises en œuvre? *(Par exemple, des technologies sécurisées comme SSH, S-FTP, SSL ou IPSec VPN sont-elles utilisées pour protéger les services non sécurisés comme NetBIOS, le partage de fichier, Telnet, FTP, etc.?)*	☐	☐	
	2.2.3	(a) Les administrateurs de système et/ou le personnel configurant les composants du système connaissent-ils bien la configuration des paramètres de sécurité communs pour ces composants du système?	☐	☐	
		(b) La configuration des paramètres de sécurité communs du système est-elle comprise dans les normes de configuration du système?	☐	☐	
		(c) La configuration des paramètres de sécurité est-elle correctement installée sur les composants du système?	☐	☐	
	2.2.4	(a) Toutes les fonctions qui ne sont pas utiles, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus, ont-elles été supprimées?	☐	☐	
		(b) Les fonctions activées sont-elles documentées et prennent-elles en charge une configuration sécurisée?	☐	☐	
		(c) Seule la fonctionnalité documentée est-elle présente dans les composants du système?	☐	☐	
2.3	L'accès administratif non-console est-il crypté afin de : *utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion par le Web et autres accès administratifs non-console.*				

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	(a) Tous les accès administratifs non-console sont-ils cryptés avec une cryptographie performante, et une méthode de cryptographie performante est-elle invoquée avant de demander le mot de passe de l'administrateur?		☐	☐	
	(b) Tous les services et les fichiers de paramètre du système sont-ils configurés pour empêcher l'utilisation de Telnet et d'autres commandes de connexion à distance non sécurisées?		☐	☐	
	(c) L'accès de l'administrateur aux interfaces de gestion basées sur le Web est-il crypté avec une cryptographie performante?		☐	☐	
2.4	Pour les fournisseurs d'hébergement partagé : les systèmes sont-ils configurés pour protéger les données de titulaire de carte et l'environnement hébergé de chaque entité? *Voir l'*Annexe A : Exigences supplémentaires des PCI DSS s'appliquant aux fournisseurs d'hébergement partagé *afin de satisfaire à des exigences spécifiques.*		☐	☐	

Protection des données de titulaire de carte de crédit

Exigence 3 : Protéger les données de titulaire de carte stockées

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
3.1	Des politiques et des procédures de conservation et de suppression des données sont-elles mises en œuvre comme suit :				
3.1.1	(a) Des politiques et des procédures de conservation et de suppression des données sont-elles mises en œuvre et comprennent-elles des exigences spécifiques pour la conservation des données de titulaire de carte à des fins professionnelles, légales et/ou réglementaires? *Par exemple, les données de titulaire de carte ont besoin d'être conservées pour une période X pour les raisons professionnelles Y.*		☐	☐	
	(b) Les politiques et procédures comprennent-elles des dispositions relatives à l'élimination sécurisée des données lorsqu'il n'existe plus de raison légale, réglementaire ou commerciale, y compris pour les données de titulaire de carte?		☐	☐	
	(c) Les politiques et procédures couvrent-elles l'ensemble du stockage des données de titulaire de carte?		☐	☐	
	(d) Les processus et procédures comprennent-ils au moins un des points suivants? • Un processus pragmatique (automatique ou manuel) destiné à supprimer, au moins chaque trimestre, les données de titulaire de carte stockées qui dépassent les exigences définies dans la politique de conservation des données. • Des exigences pour une vérification, au moins trimestrielle, afin de vérifier que les données de titulaire de carte stockées ne dépassent pas les exigences définies dans la politique de conservation des données.		☐	☐	
	(e) Toutes les données de titulaire de carte stockées satisfont-elles aux exigences définies dans la politique de conservation des données?		☐	☐	
3.2	(a) Pour les émetteurs et/ou sociétés qui prennent en charge les services d'émissions et stockent des données d'authentification sensibles, existe-t-il une justification commerciale au stockage de ces données, et ces dernières sont-elles sécurisées?		☐	☐	
	(b) Pour toutes les autres entités, si des données d'authentification sensibles sont reçues et supprimées, des processus sont-ils mis en œuvre pour sécuriser la suppression des données afin de garantir que les données sont irrécupérables?		☐	☐	
	(c) Tous les systèmes respectent-ils les exigences suivantes en ce qui concerne le non-stockage des données d'authentification sensibles après autorisation (même cryptées) :				

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	3.2.1	La totalité du contenu d'une quelconque piste de bande magnétique (située au verso d'une carte, données équivalentes sur une puce ou ailleurs) n'est-elle jamais stockée, en aucune circonstance? Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique. *Remarque : dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique ci-après :* ▪ *le nom du titulaire de la carte;* ▪ *numéro de compte principal (PAN, Primary Account Number);* ▪ *date d'expiration;* ▪ *code de service.* *Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.*	☐	☐	
	3.2.2	Le code ou la valeur de validation de la carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement) ne sont-ils jamais stockés, en aucune circonstance?	☐	☐	
	3.2.3	Le code NIP (numéro d'identification personnel) ou le bloc NIP crypté ne sont-ils jamais stockés, en aucune circonstance?	☐	☐	
3.3		Le PAN est-il masqué lorsqu'il s'affiche (les six premiers et les quatre derniers chiffres sont le maximum de chiffres affichés)? *Remarques :* ▪ *cette exigence ne s'applique pas aux employés et autres parties qui présentent le besoin spécifique de voir l'intégralité du PAN;* ▪ *cette exigence ne se substitue pas aux exigences plus strictes qui sont en place et qui régissent l'affichage des données de titulaire de carte, par exemple, pour les reçus des points de vente.*	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
3.4	Le PAN est-il rendu illisible partout où il est stocké (y compris les référentiels de données, supports numériques portables, supports de sauvegarde et journaux), en utilisant l'une des méthodes suivantes? ▪ Hachage unilatéral s'appuyant sur une méthode cryptographique performante (le PAN entier doit être haché) ▪ Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ▪ Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ▪ Cryptographie performante associée à des processus et des procédures de gestion des clés. *Remarque : il s'agit d'un effort relativement mineur pour un individu malveillant de reconstruire les données du PAN d'origine s'il possède à la fois l'accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachée et tronquée du même PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être en place pour assurer que les versions hachée et tronquée ne peuvent pas être corrélées pour la reconstruction du PAN original.*		☐	☐	
3.4.1	Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès est-il géré comme suit :				
	(a) L'accès logique aux systèmes de fichiers cryptés est-il géré séparément des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, sans utiliser de bases de données de comptes d'utilisateur locales)?		☐	☐	
	(b) Les clés cryptographiques sont-elles stockées de manière sécurisée (par exemple, stockée sur des supports amovibles qui sont adéquatement protégés avec des contrôles d'accès stricts)?		☐	☐	
	(c) Les données du titulaire de carte sur support amovible sont-elles cryptées quel que soit l'endroit où elles sont stockées? ***Remarque** : si un cryptage par disque n'est pas utilisé pour crypter un support amovible, les données stockées sur ce support devront être rendues illisibles par une autre méthode.*		☐	☐	
3.5	Les clés utilisées pour sécuriser des données de titulaire de carte sont-elles protégées contre la divulgation et l'utilisation illicites comme suit : ***Remarque** : cette exigence s'applique également aux clés de cryptage de clés utilisées pour protéger les clés de cryptage de données. De telles clés de cryptage de clés doivent être au moins aussi performantes que la clé de cryptage de données.*				
3.5.1	L'accès aux clés cryptographiques est-il limité au plus petit nombre d'opérateurs possible?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	3.5.2	(a) Les clés sont-elles stockées sous format crypté et les clés de cryptage de clés sont-elles stockées séparément des clés de cryptage des données?	☐	☐	
		(b) Les clés cryptographiques sont-elles stockées dans aussi peu d'emplacements et de formes que possible?	☐	☐	
3.6		(a) Les processus et les procédures de gestion des clés sont-ils tous documentés en détail et mis en œuvre pour les clés de cryptage utilisées pour les données de titulaire de carte?	☐	☐	
		(b) Pour les prestataires de services uniquement : si des clés sont partagées avec des clients pour la transmission ou le stockage des données de titulaire de carte, une documentation comprenant des directives sur la manière de transmettre, de stocker ou de mettre à jour de façon sécurisée les clés du client, est-elle fournie aux clients conformément aux exigences 3.6.1 à 3.6.8 ci-dessous?	☐	☐	
		(c) Les processus et procédures de gestion de clés sont-ils mis en œuvre pour exiger ce qui suit :			
	3.6.1	Les procédures de clés cryptographiques comprennent-elles la génération de clés cryptographiques performantes?	☐	☐	
	3.6.2	Les procédures de clés cryptographiques comprennent-elles la distribution sécurisée des clés cryptographiques?	☐	☐	
	3.6.3	Les procédures de clés cryptographiques comprennent-elles le stockage sécurisé des clés cryptographiques?	☐	☐	
	3.6.4	Les procédures de clés cryptographiques comprennent-elles le remplacement des clés cryptographiques qui ont atteint la fin de leur cryptopériode (par exemple, après une période définie écoulée et/ou après qu'une certaine quantité de cryptogramme a été produite par une clé donnée), comme défini par le fournisseur d'applications associées ou le propriétaire de la clé, et en fonction des meilleures pratiques et directives du secteur (par exemple, publication spéciale NIST 800-57)?	☐	☐	
	3.6.5	(a) Les procédures de clés cryptographiques comprennent-elles le retrait ou le remplacement des clés cryptographiques (par exemple, en les archivant, les détruisant, et/ou les révoquant), lorsque le degré d'intégrité de la clé a été affaibli (par exemple, le départ d'un employé ayant connaissance du texte clair d'une clé)?	☐	☐	
		(b) Les procédures de clés cryptographiques comprennent-elles un remplacement des clés compromises ou soupçonnées de l'avoir été?	☐	☐	
		(c) Si des clés cryptographiques retirées ou remplacées sont conservées, ces clés sont-elles utilisées uniquement à des fins de décryptage/vérification (non pour des opérations de cryptage)?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
3.6.6	Les procédures de clés cryptographiques comprennent-elles le fractionnement de connaissance et le double contrôle des clés cryptographiques (par exemple, la nécessité de deux ou trois personnes, chacune connaissant uniquement sa propre partie de la clé, pour reconstruire la clé entière) pour les opérations de gestion des clés en texte clair? ***Remarque** : des exemples d'opérations de gestion manuelle de clés comprennent, mais sans s'y limiter : la génération de clés, la transmission, le chargement, le stockage et la destruction.*		☐	☐	
3.6.7	Les procédures de clés cryptographiques comprennent-elles la prévention de la substitution non autorisée de clés cryptographiques?		☐	☐	
3.6.8	Les opérateurs chargés de la gestion de clés cryptographiques doivent-ils reconnaître (par écrit ou de manière électronique) qu'ils comprennent et acceptent leurs responsabilités?		☐	☐	

Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
4.1	(a) Des protocoles de cryptographie et de sécurité performants, tels que SSL/TLS, SSH ou IPSEC, sont-ils utilisés pour sauvegarder les données de titulaire de carte sensibles lors de leur transmission sur des réseaux publics ouverts? *Des exemples de réseaux publics ouverts dans la portée des PCI DSS, comprennent, mais sans s'y limiter, Internet, les technologies sans fil, GSM (Global System For Mobile Communications) et GPRS (General Packet Radio Service).*		☐	☐	
	(b) Seuls les clés et/ou certificats approuvés sont-ils acceptés?		☐	☐	
	(c) Les protocoles de sécurité sont-ils mis en œuvre pour utiliser uniquement des configurations sécurisées et ne pas prendre en charge des versions ou configurations non sécurisées?		☐	☐	
	(d) La puissance de cryptage adéquate est-elle mise en œuvre au regard de la méthodologie de cryptage utilisée (vérifier les recommandations/meilleures pratiques du fournisseur)?		☐	☐	
	(e) Pour les mises en œuvre SSL/TLS : • La mention HTTPS apparaît-elle dans l'adresse URL? • Les données de titulaire de carte sont-elles exigées uniquement lorsque HTTPS apparaît dans l'adresse URL?		☐	☐	
	4.1.1 Les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont-elles utilisées pour appliquer un cryptage performant pour l'authentification et la transmission pour les réseaux sans fil sur lesquels sont transmises les données de titulaire de carte ou qui sont connectés à l'environnement des données de titulaire de carte? ***Remarque** : l'utilisation du protocole WEP comme contrôle de sécurité est interdit depuis le 30 juin 2010.*		☐	☐	
4.2	(a) Les PAN sont-ils rendus illisibles ou sécurisés avec une cryptographie performante chaque fois qu'ils sont envoyés par des technologies de messagerie pour utilisateurs finaux (par exemple, courriel, messagerie instantanée, ou clavardage)?		☐	☐	
	(b) Des politiques précisant que les PAN non protégés ne doivent pas être envoyés par des technologies de messagerie pour les utilisateurs finaux sont-elles en place?		☐	☐	

Gestion d'un programme de gestion des vulnérabilités

Exigence 5 : Utiliser des logiciels ou des programmes antivirus et les mettre à jour régulièrement

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
5.1	Des logiciels antivirus sont-ils déployés sur tous les systèmes régulièrement affectés par des logiciels malveillants?		☐	☐	
5.1.1	Tous les programmes antivirus sont-ils capables de détecter et de supprimer tous les types de logiciels malveillants connus, et de constituer une protection efficace contre ces fléaux (par exemple, virus, chevaux de Troie, vers, logiciels espions, logiciels publicitaires et dissimulateurs d'activité)?		☐	☐	
5.2	Tous les mécanismes antivirus sont-ils à jour, en cours d'exécution et capables de générer des registres de vérification comme suit :				
	(a) La politique anti-virus exige-t-elle une mise à jour des définitions et du logiciel anti-virus?		☐	☐	
	(b) L'installation principale du logiciel est-elle activée pour des mises à jour et analyses automatiques?		☐	☐	
	(c) Des mises à jour et des analyses périodiques automatiques sont-elles activées?		☐	☐	
	(d) Tous les mécanismes anti-virus génèrent-ils des journaux de vérification et les journaux sont-ils conservés conformément à l'exigence 10.7 des normes PCI DSS?		☐	☐	

Exigence 6 : Développer et gérer des systèmes et des applications sécurisés

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
6.1	(a) Tous les logiciels et composants du système sont-ils protégés des vulnérabilités connues en étant dotés des derniers correctifs de sécurité développés par le fournisseur?		☐	☐	
	(b) Les correctifs de sécurité essentiels sont-ils installés dans le mois qui suit leur commercialisation? ***Remarque** : une organisation peut envisager la mise en œuvre d'une approche en fonction du risque pour définir la priorité des correctifs à installer. Par exemple, en accordant aux infrastructures essentielles (par exemple, bases de données, dispositifs et systèmes orientés public) une priorité supérieure à celle des dispositifs internes moins cruciaux, de sorte que les systèmes et les dispositifs hautement prioritaires soient traités dans un délai d'un mois, tandis que les dispositifs et systèmes moins essentiels le soient dans un délai de trois mois.*		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
6.2	(a)	Existe-t-il un processus pour identifier les vulnérabilités de sécurité nouvellement découvertes, notamment un classement des risques assignés à de telles vulnérabilités? (Au minimum, les vulnérabilités de plus haut risque, plus critiques, doivent être classées comme « à haut risque »). ***Remarque** : le classement des risques doit se baser sur les meilleures pratiques du secteur. Par exemple, les critères pour un classement des vulnérabilités à « haut » risque peuvent comprendre un score de 4.0 ou plus basé sur le CVSS (Common Vulnerability Scoring System, système de notation de vulnérabilité commun), et/ou un correctif proposé et classé par le fournisseur comme « critique », et/ou une vulnérabilité affectant un composant essentiel du système.* *Le classement des vulnérabilités est considéré comme une meilleure pratique jusqu'au 30 juin 2012, après quoi, il deviendra une exigence.*	☐	☐	
	(b)	Des processus pour identifier les nouvelles vulnérabilités de sécurité comprennent-ils l'utilisation des sources externes des renseignements de vulnérabilité de sécurité?	☐	☐	
6.3	(a)	Les processus de développement de logiciel sont-ils basés sur les normes et/ou les meilleures pratiques du secteur?	☐	☐	
	(b)	La sécurité des renseignements est-elle intégrée au cycle de vie du développement d'un logiciel?	☐	☐	
	(c)	Les applications logicielles sont-elles développées conformément aux normes PCI DSS (par exemple, une authentification et une connexion sécurisées)?	☐	☐	
	(d)	Les processus de développement de logiciel garantissent-ils ce qui suit?			
6.3.1		Les comptes d'application personnalisés, les noms d'utilisateur et les mots de passe sont-ils supprimés avant l'activation des applications ou leur mise à la disposition des clients?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	6.3.2	Tous les changements des codes d'application personnalisés sont-ils examinés (pour l'utilisation des processus manuels ou automatiques) avant leur mise en production ou leur mise à la disposition des clients afin d'identifier les vulnérabilités éventuelles du codage comme suit : • Les modifications de code sont-elles examinées par des individus autres que l'auteur initial du code et compétents dans les techniques d'examen de code et les pratiques de codage sécurisées? • Les examens du code garantissent-ils que le code est développé selon les directives de codage sécurisé (voir l'exigence 6.5 des normes PCI DSS)? • Les corrections appropriées sont-elles mises en œuvre avant la commercialisation? • Les résultats de l'examen du code sont-ils passés en revue et approuvés par les responsables avant la commercialisation? ***Remarque** : cette exigence de vérification de code s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de vie du développement du système. Les examens du code peuvent être réalisés par le personnel interne compétent ou par des parties tierces. Les applications Web font également l'objet de contrôles supplémentaires si elles sont orientées public afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par l'exigence 6.6 des PCI DSS.*	☐	☐	
6.4		Les processus et procédures de contrôle des changements sont-ils suivis pour toutes les modifications des composants du système, notamment ce qui suit :			
	6.4.1	Les environnements de test/développement sont-ils séparés de l'environnement de production, et existe-t-il un contrôle d'accès pour garantir la séparation?	☐	☐	
	6.4.2	Existe-t-il une séparation entre les missions des collaborateurs affectés aux environnements de développement/test et celles des employés affectés à l'environnement de production?	☐	☐	
	6.4.3	Les données de production (PAN actifs) ***ne sont-elles*** jamais utilisées à des fins de test ou de conception?	☐	☐	
	6.4.4	Les données de test et les comptes sont-ils supprimés avant que les systèmes de production ne deviennent actifs?	☐	☐	
	6.4.5	(a) Les procédures de contrôle des modifications relatives à la mise en œuvre des correctifs de sécurité et des changements du logiciel sont-elles documentées et exigent-elles les points 6.4.5.1 à 6.4.5.4 ci-dessous?	☐	☐	
		(b) Les points suivants sont-ils en place pour tous les changements :			

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	6.4.5.1	La documentation de l'impact?	☐	☐	
	6.4.5.2	Approbation documentée de la modification par les parties autorisées appropriées?	☐	☐	
	6.4.5.3	(a) Test de fonctionnalité pour vérifier que la modification ne porte pas atteinte à la sécurité du système?	☐	☐	
		(b) Pour les modifications de code personnalisé, toutes les mises à jour sont-elles testées du point de vue de la conformité à l'exigence 6.5 des normes PCI DSS avant d'être mises en production?	☐	☐	
	6.4.5.4	Des procédures de suppression sont-elles préparées pour chaque modification?	☐	☐	
6.5		(a) Les applications sont-elles développées en fonction des directives de codage sécurisé? (Par exemple, *Guide OWASP (Open Web Application Security Project), 25 plus grands risques selon SANS CWE, codage sécurisé CERT, etc.*)	☐	☐	
		(b) Les développeurs sont-ils compétents en techniques de codage sécurisé?	☐	☐	
		(c) La prévention des vulnérabilités de codage courantes est-elle couverte dans les processus de développement de logiciel, afin de comprendre au moins les éléments suivants : *Remarque : les vulnérabilités répertoriées aux points 6.5.1 à 6.5.9 étaient compatibles avec les meilleures pratiques du secteur lorsque cette version des normes PCI DSS a été publiée. Cependant, comme les meilleures pratiques du secteur de gestion de la vulnérabilité sont actualisées, les meilleures pratiques actuelles doivent être utilisées pour ces exigences.*			
	6.5.1	Attaques par injection, notamment les injections de commandes SQL? (Valider les données entrées pour vérifier que les données utilisateur ne peuvent pas modifier le sens des commandes et des requêtes, utiliser des requêtes paramétrées, etc.). *Prendre également en considération les injections de commande OS, les attaques par injection LDAP et XPath ainsi que les autres attaques par injection.*	☐	☐	
	6.5.2	Saturation de la mémoire? (Valider les limites de la mémoire et tronquer les chaînes d'entrée).	☐	☐	
	6.5.3	Stockage cryptographique non sécurisé? (Empêcher les attaques cryptographiques).	☐	☐	
	6.5.4	Communications non sécurisées? (Crypter correctement toutes les communications authentifiées et sensibles).	☐	☐	
	6.5.5	Traitement inapproprié des erreurs? (Ne laisser filtrer aucun renseignement par le biais de messages d'erreur).	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	6.5.6	Toutes les vulnérabilités à « haut risque » sont-elles identifiées dans le processus d'identification des vulnérabilités (défini dans l'exigence 6.2 des normes PCI DSS)? ***Remarque** : ce point est considéré comme une meilleure pratique jusqu'au 30 juin 2012, après quoi il sera considéré comme une exigence.*	☐	☐	
	Pour les applications Web et les interfaces d'application (internes ou externes), les vulnérabilités supplémentaires suivantes sont-elles également couvertes :				
	6.5.7	Attaques par script intersite (XSS)? (Valider tous les paramètres avant l'inclusion, utiliser un mécanisme d'échappement sensible au contexte, etc.).	☐	☐	
	6.5.8	Contrôle d'accès inapproprié, comme des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès aux URL, et aux échanges? (Authentifier correctement les utilisateurs et expurger l'entrée. N'exposer en aucun cas les références d'objets internes aux utilisateurs).	☐	☐	
	6.5.9	Attaques CSRF (Cross-Site Request Forgery)? (Ne pas répondre aux renseignements d'autorisation ni aux jetons automatiquement envoyés par les navigateurs).	☐	☐	
6.6		Pour les applications Web orientées public, les nouvelles menaces et vulnérabilités sont-elles traitées de manière régulière et ces applications sont-elles protégées contre les attaques connues à l'aide de *l'une* des méthodes suivantes? ▪ Examiner les applications Web orientées public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuels, comme suit : o au moins une fois par an; o après un changement; o par une organisation qui est spécialisée en sécurité d'application; o que toutes les vulnérabilités sont corrigées; o que l'application est réévaluée après les corrections. *– ou –* ▪ Installer un pare-feu de couche d'application Web devant les applications Web orientées public pour détecter et empêcher les attaques basées sur le Web. ***Remarque** : « une organisation spécialisée dans le sécurité des applications » peut être à la fois une société tierce ou une organisation interne, tant que les examinateurs sont spécialisés dans la sécurité des applications et peuvent démontrer leur indépendance par rapport à l'équipe de développement.*	☐	☐	

Mise en œuvre de mesures de contrôle d'accès strictes

Exigence 7 : Limiter l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
7.1		L'accès aux composants du système et aux données de titulaire de carte est-il limité aux seuls individus qui doivent y accéder pour mener à bien leur travail, comme suit :			
	7.1.1	Les droits d'accès accordés aux ID utilisateur privilégiés sont-ils limités aux privilèges les plus faibles nécessaires pour la réalisation du travail?	☐	☐	
	7.1.2	Les privilèges sont-ils octroyés aux individus sur la base de la classification et de la fonction professionnelles (également nommée « contrôle d'accès basé sur les fonctions » ou RBAC)?	☐	☐	
	7.1.3	Une approbation documentée par les parties autorisées est-elle requise (par écrit ou de manière électronique) spécifiant les privilèges exigés?	☐	☐	
	7.1.4	Les contrôles d'accès sont-ils mis en œuvre par un système de contrôle d'accès automatique?	☐	☐	
7.2		Un système de contrôle d'accès est-il défini pour les systèmes comptant plusieurs utilisateurs pour limiter l'accès aux seuls utilisateurs qui doivent accéder aux données et est-il configuré pour « refuser tout » à moins qu'il ne soit explicitement autorisé, comme suit :			
	7.2.1	Des systèmes de contrôle d'accès sont-ils en place sur tous les composants du système?	☐	☐	
	7.2.2	Les systèmes de contrôle d'accès sont-ils paramétrés pour mettre en vigueur les privilèges octroyés aux individus sur la base de la classification et de la fonction professionnelles?	☐	☐	
	7.2.3	Les systèmes de contrôle d'accès ont-il un paramètre « Refuser tout » par défaut? ***Remarque** : certains systèmes de contrôle d'accès sont paramétrés par défaut sur « Accepter tout », permettant ainsi l'accès à moins/jusqu'à ce qu'une règle soit écrite pour le refuser.*	☐	☐	

Exigence 8 : Affecter un ID unique à chaque utilisateur d'ordinateur

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
8.1	Tous les utilisateurs se voient-ils affecter un ID unique avant de pouvoir accéder à des composants du système ou aux données de titulaire de carte?		☐	☐	
8.2	Outre l'affectation d'un ID unique, l'une ou plusieurs des méthodes suivantes sont-elles utilisées pour authentifier tous les utilisateurs? ▪ Quelque chose de connu, comme un mot de passe ou une phrase passe. ▪ Quelque chose de détenu, comme un dispositif à jetons ou une carte à puce. ▪ Quelque chose propre à l'utilisateur, comme une mesure biométrique.		☐	☐	
8.3	L'authentification à deux facteurs est-elle intégrée pour l'accès à distance (accès au niveau du réseau depuis l'extérieur du réseau) des employés, des administrateurs et de tiers au réseau? *(Par exemple, service d'usager commuté à authentification distante (RADIUS) avec jetons; protocole d'authentification TACACS (terminal access controller access control system, système de contrôle d'accès du contrôleur d'accès au terminal) avec jetons; ou autres technologies qui permettent l'authentification à deux facteurs).* ***Remarque** : l'authentification à deux facteurs exige que deux des trois méthodes d'authentification (voir l'exigence 8.2 des normes PCI DSS pour la description des méthodes d'authentification) soient utilisées pour l'authentification. L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe séparés) n'est pas considérée comme une authentification à deux facteurs.*		☐	☐	
8.4	(a) Les mots de passe sont-ils tous rendus illisibles lors de la transmission et le stockage sur tous les composants du système à l'aide d'une cryptographie performante?		☐	☐	
	(b) Pour les prestataires de services uniquement : les mots de passe des clients sont-ils cryptés?		☐	☐	
8.5	Des contrôles de gestion appropriés de l'identification et de l'authentification des utilisateurs sont-ils mis en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants du système comme suit :				
8.5.1	Les compléments, suppressions et modifications d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiant sont-ils contrôlés, de sorte que les ID utilisateurs soient mis en œuvre uniquement en fonction de leur autorisation (notamment avec des privilèges spécifiés)?		☐	☐	
8.5.2	L'identité de l'utilisateur est-elle vérifiée avant la réinitialisation du mot de passe pour les requêtes d'utilisateurs faites par une méthode autre qu'en face-à-face (par exemple par téléphone, courriel ou Web)?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
8.5.3	Les mots de passe initiaux et de réinitialisation sont-ils définis sur une valeur unique pour chaque utilisateur et sont-ils modifiés par l'utilisateur après la première utilisation?		☐	☐	
8.5.4	L'accès des utilisateurs ne travaillant plus pour la société est-il immédiatement désactivé ou révoqué?		☐	☐	
8.5.5	Les comptes d'utilisateur inactifs sont-ils supprimés ou désactivés après 90 jours?		☐	☐	
8.5.6	(a) Les comptes utilisés par les fournisseurs pour l'accès à distance, la maintenance ou l'assistance sont-ils activés uniquement pendant la période nécessaire?		☐	☐	
	(b) Les comptes d'accès à distance des fournisseurs sont-ils surveillés lors de leur utilisation?		☐	☐	
8.5.7	Les politiques et procédures d'authentification sont-elles communiquées à tous les utilisateurs ayant accès aux données de titulaire de carte?		☐	☐	
8.5.8	Les comptes et mots de passe collectifs, partagés ou génériques, ou autres méthodes d'authentification, sont-ils interdits comme suit : • les comptes et ID d'utilisateurs génériques sont désactivés ou supprimés; • les ID d'utilisateurs partagés pour les activités administratives du système et d'autres fonctions essentielles n'existent pas; et • les ID génériques et partagés ne sont pas utilisés pour administrer les composants du système.		☐	☐	
8.5.9	(a) Les mots de passe utilisateur sont-ils modifiés au moins tous les 90 jours?		☐	☐	
	(b) Pour les prestataires de services uniquement : Les mots de passe d'utilisateur non consommateur doivent-ils être changés périodiquement et les utilisateurs non-clients reçoivent-ils des instructions sur la fréquence et les circonstances du changement des mots de passe?		☐	☐	
8.5.10	(a) Les mots de passe comportent-ils au moins sept caractères?		☐	☐	
	(b) Pour les prestataires de services uniquement : les mots de passe d'utilisateurs non consommateurs doivent-ils satisfaire à des exigences de longueur minimum?		☐	☐	
8.5.11	(a) Les mots de passe doivent-ils comporter des caractères alphanumériques?		☐	☐	
	(b) Pour les prestataires de services uniquement : les mots de passe utilisateurs non consommateurs doivent-ils comporter des caractères alphanumériques?		☐	☐	
8.5.12	(a) Un individu doit-il soumettre un nouveau mot de passe différent des quatre derniers mots de passe utilisés?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	(b) Pour les prestataires de services uniquement : les nouveaux mots de passe d'utilisateurs non-consommateurs doivent-ils être différents des quatre derniers mots de passe utilisés?		☐	☐	
8.5.13	(a) Les tentatives d'accès répétées sont-elles limitées en verrouillant l'ID utilisateur après un maximum de six tentatives?		☐	☐	
	(b) Pour les prestataires de services uniquement : les mots de passe d'utilisateurs non-consommateurs sont-ils temporairement verrouillés après un maximum de six tentatives d'accès non valides?		☐	☐	
8.5.14	Une fois un compte utilisateur verrouillé, la durée de verrouillage est-elle réglée sur 30 minutes au minimum ou jusqu'à ce que l'administrateur active l'ID utilisateur?		☐	☐	
8.5.15	Si une session reste inactive pendant plus de 15 minutes, est-t-il exigé des utilisateurs qu'ils se ré-authentifient (par exemple saisissent de nouveau le mot de passe) pour réactiver le terminal ou la session?		☐	☐	
8.5.16	(a) Tous les accès aux bases de données contenant des données de titulaire de carte sont-ils authentifiés? (Cela comprend les accès des applications, des administrateurs et de tous les autres utilisateurs).		☐	☐	
	(b) Tous les accès, toutes les requêtes et toutes les actions des utilisateurs (par exemple, déplacer, copier, supprimer) sur la base de données, se font-ils à travers des méthodes de programmation uniquement (par exemple, à travers des procédures stockées)?		☐	☐	
	(c) Les accès directs ou les requêtes des utilisateurs aux bases de données sont-ils limités aux administrateurs de base de données?		☐	☐	
	(d) Les ID d'application ayant un accès à la base de données peuvent-ils être utilisés par les applications uniquement (et non par des utilisateurs individuels ou d'autres processus)?		☐	☐	

Exigence 9 : Limiter l'accès physique aux données de titulaire de carte

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
9.1	Des contrôles d'accès aux installations appropriés sont-ils utilisés pour limiter et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaire de carte?		☐	☐	
9.1.1	(a) Des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès sont-ils en place pour surveiller l'accès physique des individus aux zones sensibles? ***Remarque** : « Zones sensibles », signifie centre de données, salle de serveurs ou zone abritant des systèmes qui stockent des données de titulaire de carte. Cette définition exclut les zones où ne sont installés que des terminaux de point de vente, telles que les zones de caisse dans un magasin.*		☐	☐	
	(b) Les caméras vidéo et/ou les mécanismes de contrôle d'accès sont-ils protégés de l'altération et de l'inhibition?		☐	☐	
	(c) Les données recueillies sur des caméras vidéo et/ou des mécanismes de contrôle d'accès, sont-elles examinées et corrélées avec d'autres entrées, et ces données sont-elles stockées pour au moins trois mois, sauf indication contraire de la loi?		☐	☐	
9.1.2	L'accès physique aux prises réseau accessibles au public est-il limité (par exemple, les zones accessibles aux visiteurs n'ont pas de port réseau activé à moins que l'accès au réseau ait été explicitement autorisé)? Sinon, les visiteurs sont-ils accompagnés à tout moment dans les zones comportant des prises réseau actives?		☐	☐	
9.1.3	L'accès physique aux points d'accès sans fil, passerelles, dispositifs portables, matériel de communication/mise en réseau, et lignes de télécommunications est-il limité?		☐	☐	
9.2	Des procédures sont-elles développées pour distinguer facilement les employés sur site et les visiteurs, comme suit : *Dans le cadre de l'exigence 9, le terme « employés sur site » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui sont physiquement présents sur le site de l'entité. Un « visiteur » est défini comme un fournisseur, un invité d'un(e) employé(e) sur site, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée.*				
	(a) Les processus et les procédures d'attribution des badges aux employés sur site et aux visiteurs comprennent-ils les éléments suivants : • l'octroi de nouveaux badges; • la modification des exigences d'accès; • la révocation des badges d'employés sur site ne travaillant plus pour l'entreprise, ou des badges de visiteur expirés.		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	(b) L'accès au système de badge est-il limité au personnel autorisé?		☐	☐	
	(c) Les badges identifient-ils clairement les visiteurs et permettent-ils de distinguer aisément les employés sur site des visiteurs?		☐	☐	
9.3	Tous les visiteurs sont-ils traités de la manière suivante :				
9.3.1	Une autorisation d'accès est-elle donnée aux visiteurs avant qu'ils ne pénètrent dans les zones où sont traitées et conservées les données de titulaire de carte?		☐	☐	
9.3.2	(a) Les visiteurs reçoivent-il un jeton physique (par exemple, un badge ou un dispositif d'accès) qui identifie distinctement les visiteurs des employés sur site?		☐	☐	
	(b) Les badges des visiteurs comportent-ils une date d'expiration?		☐	☐	
9.3.3	Est-il demandé aux visiteurs de rendre le jeton physique avant de quitter les locaux ou à la date d'expiration?		☐	☐	
9.4	(a) Un journal des visiteurs est-il utilisé pour enregistrer l'accès physique à l'installation ainsi qu'aux salles informatiques, et aux centres de données où sont stockées ou transmises les données de titulaire de carte?		☐	☐	
	(b) Le journal des visiteurs contient-il le nom du visiteur, l'entreprise représentée et l'employé sur site qui autorise son accès physique, et ce journal est-il conservé au moins trois mois?		☐	☐	
9.5	(a) Les sauvegardes sur support sont-elles stockées en lieu sûr, de préférence hors de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial?		☐	☐	
	(b) La sécurité du site est-elle inspectée au moins une fois par an?		☐	☐	
9.6	Tous les supports sont-ils physiquement sécurisés (y compris, mais sans s'y limiter, les ordinateurs, les supports électroniques amovibles, les reçus papier, les rapports papier et les télécopies)? *Dans le cadre de l'exigence 9, le terme « support » concerne tous les documents papier et les supports électroniques contenant des données de titulaire de carte.*		☐	☐	
9.7	(a) La distribution interne ou externe de tout type de support est-elle soumise à un contrôle strict?		☐	☐	
	(b) Les contrôles comprennent-ils les procédures suivantes :				
9.7.1	Les supports sont-ils classifiés afin que la confidentialité des données puisse être déterminée?		☐	☐	
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition sécurisée pouvant faire l'objet d'un suivi?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
9.8	Les journaux sont-ils gérés pour suivre tous les supports qui sont déplacés d'une zone sécurisée, et l'approbation de gestion est-elle obtenue avant le déplacement des supports (en particulier lorsqu'un support est distribué aux individus)?		☐	☐	
9.9	Un contrôle strict est-il assuré concernant le stockage et l'accessibilité des supports?		☐	☐	
9.9.1	Les journaux d'inventaire de tous les supports sont-ils correctement gérés et des inventaires périodiques des supports sont-ils réalisés au moins annuellement?		☐	☐	
9.10	Tous les supports sont-ils éliminés lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou juridiques?		☐	☐	
	La destruction est-elle effectuée comme suit :				
9.10.1	(a) Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de manière à ce qu'il soit impossible de les reconstituer?		☐	☐	
	(b) Les conteneurs utilisés pour le stockage des renseignements à détruire sont-ils sécurisés pour empêcher l'accès aux contenus? (Par exemple, un conteneur de « documents à déchiqueter » possède une serrure empêchant l'accès à son contenu)		☐	☐	
9.10.2	Les données de titulaire de carte sur support électronique sont-elles rendues irrécupérables par un programme d'effacement sécurisé, conformément aux normes du secteur sur la suppression sécurisée, ou sur la destruction physique du support (par exemple, la démagnétisation), de manière à ce que les données de titulaire de carte ne puissent pas être reconstituées?		☐	☐	

Surveillance et test réguliers des réseaux

Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
10.1	Un processus est-il défini pour associer chaque accès aux composants du système (en particulier les accès avec des droits administrateur, tels que racine) à un utilisateur individuel?		☐	☐	
10.2	Des pistes de vérification automatique sont-elles mises en œuvre pour tous les composants du système pour reconstituer les événements suivants :				
10.2.1	Tous les accès des utilisateurs aux données de titulaire de carte		☐	☐	
10.2.2	Toutes les actions exécutées par un quelconque utilisateur avec des droits racine ou administrateur		☐	☐	
10.2.3	Accès à toutes les pistes de vérification		☐	☐	
10.2.4	Tentatives d'accès logique non valides		☐	☐	
10.2.5	Utilisation des mécanismes d'identification et d'authentification		☐	☐	
10.2.6	Initialisation des registres de vérification		☐	☐	
10.2.7	Création et suppression d'objets au niveau système		☐	☐	
10.3	Les pistes de vérification consignent-elles au moins les entrées suivantes pour chaque événement :				
10.3.1	Identification des utilisateurs		☐	☐	
10.3.2	Type d'événement		☐	☐	
10.3.3	Date et heure		☐	☐	
10.3.4	Indication de succès ou d'échec		☐	☐	
10.3.5	Origine de l'événement		☐	☐	
10.3.6	Identité ou nom des données, du composant du système ou de la ressource affectés		☐	☐	
10.4	(a) Les horloges et les heures des systèmes essentiels sont-elles synchronisées par l'utilisation d'une technologie de synchronisation du temps, et la technologie est-elle gardée à jour? ***Remarque** : un exemple de technologie de synchronisation horaire est le protocole de synchronisation réseau (protocole NTP).*		☐	☐	
	(b) Les contrôles suivants sont-ils mis en œuvre pour l'acquisition, la distribution et le stockage de l'heure :				

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	10.4.1	(a) SLes serveurs horaires centraux désignés reçoivent-ils seuls les signaux horaires depuis des sources externes, et les systèmes essentiels ont-ils tous l'heure exacte et cohérente basée sur le temps atomique universel ou sur le temps universel coordonné (UTC)?	☐	☐	
		(b) Les serveurs horaires centraux désignés sont-ils couplés les uns aux autres pour garder l'heure exacte, et les autres serveurs internes reçoivent-ils l'heure uniquement à partir des serveurs horaires centraux?	☐	☐	
	10.4.2	Les données horaires sont-elles protégées comme suit : (a) L'accès aux données horaires est-il limité aux seuls employés ayant un besoin professionnel d'y avoir accès?	☐	☐	
		(b) Les modifications des paramètres horaires sur les systèmes essentiels sont-ils journalisés, surveillés et examinés?	☐	☐	
	10.4.3	Les paramètres horaires sont-ils reçus de sources horaires spécifiques acceptées par le secteur? (Ceci permet d'empêcher un individu malveillant de changer l'horloge) Ces mises à jour peuvent être cryptées de manière optionnelle par une clé symétrique, et des listes de contrôle d'accès peuvent être créées, spécifiant les adresses IP des équipements des clients qui seront fournies avec les mises à jour horaires (pour empêcher l'utilisation non autorisée des serveurs horaires internes).	☐	☐	
10.5		Les pistes de vérification sont-elles sécurisées de sorte qu'elles ne puissent pas être altérées, comme suit :			
	10.5.1	L'affichage des pistes de vérification est-il limité aux utilisateurs qui en ont besoin pour des raisons professionnelles?	☐	☐	
	10.5.2	Les fichiers de vérification sont-ils protégés contre tout changement non autorisé par des mécanismes de contrôles d'accès, une séparation physique, et/ou une ségrégation de réseau?	☐	☐	
	10.5.3	Les fichiers des registres de vérification sont-ils sauvegardés rapidement sur un serveur centralisé dédié à la consignation ou sur des supports difficiles à altérer?	☐	☐	
	10.5.4	Les journaux des technologies orientées vers l'extérieur (par exemple, sans fil, pare-feu, serveurs de nom de domaine [DNS], courriels) sont-ils téléchargés ou copiés sur un serveur ou un support réservé à la journalisation centralisée sur le réseau local interne (LAN)?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	10.5.5	Les journaux sont-ils analysés à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte)?	☐	☐	
10.6		Les journaux relatifs à tous les composants du système sont-ils passés en revue au moins une fois par jour, avec suivi des anomalies? *L'examen des journaux doit comprendre les serveurs exécutant des fonctions de sécurité, tels que les serveurs IDS (système de détection d'intrusion) et AAA (Authentication, Authorization, and Accounting) (par exemple, RADIUS).* ***Remarque :*** *les outils de consignation, d'analyse et d'alerte peuvent être utilisés conformément à l'exigence 10.6.*	☐	☐	
10.7		(a) Des politiques et procédures de conservation des journaux de vérification sont-elles en place et exigent-elles que l'historique de vérification soit conservé au moins un an?	☐	☐	
		(b) Les journaux de vérification sont-ils disponibles pendant au moins un an et des processus sont-ils en place pour restaurer immédiatement au moins les journaux des trois derniers mois pour analyse?	☐	☐	

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

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
11.1		(a) Un processus documenté est-il mis en œuvre pour détecter et identifier les points d'accès sans fil sur une base trimestrielle? ***Remarque*** *: les méthodes qui peuvent être utilisées dans le processus comprennent, mais sans s'y limiter, les analyses de réseau sans fil, les inspections physiques/logiques des composants du système et des infrastructures, les contrôles d'accès au réseau (NAC), ou les IDS (systèmes de détection d'intrusion) et les IPS (systèmes de prévention d'intrusion) sans fil.* *Quelles que soient les méthodes utilisées, elles doivent être suffisantes pour détecter et identifier les dispositifs non autorisés.*	☐	☐	
		(b) La méthodologie détecte-t-elle et identifie-t-elle les points d'accès sans fil non autorisés, y compris au moins les points suivants : • des cartes de réseau local sans fil (WLAN) insérées dans des composants du système; • des dispositifs sans fil portables connectés aux composants du système (par exemple, par USB, etc.); • des dispositifs sans fil reliés à un port réseau ou à un dispositif réseau?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
		(c) Le processus pour identifier les points d'accès sans fil non autorisés est-il exécuté au moins tous les trimestres pour tous les composants du système et toutes les installations?	☐	☐	
		(d) Si une surveillance automatique est utilisée (par exemple, IDS/IPS sans fil, NAC, etc.), la surveillance est-elle configurée pour générer des alertes pour le personnel?	☐	☐	
		(e) Le plan de réponse aux incidents (exigence 12.9) comprend-il une réponse au cas où des dispositifs sans fil non autorisés sont détectés?	☐	☐	
11.2	Les vulnérabilités potentielles des réseaux internes et externes font-elles l'objet d'une analyse au moins une fois par trimestre et après tout changement dans le réseau (par exemple, l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits) comme suit? ***Remarque** : il n'est pas exigé que quatre analyses trimestrielles soient réalisées pour une conformité initiale aux normes PCI DSS si 1) le plus récent résultat d'analyse a été une analyse réussie, 2) l'entité a documenté les politiques et procédures exigeant l'analyse trimestrielle, et 3) les vulnérabilités notées ont été corrigées, ce qui sera confirmé par une nouvelle analyse. Lors des années suivant la vérification PCI DSS initiale, quatre analyses trimestrielles doivent être réalisées et réussies.*				
11.2.1		(a) Des analyses de vulnérabilité interne trimestrielles sont-elles exécutées?	☐	☐	
		(b) Le processus d'analyse interne trimestriel comprend-il de nouvelles analyses jusqu'à ce que des résultats satisfaisants soient obtenus ou que toutes les vulnérabilités à « haut risque », définies dans l'exigence 6.2 des normes PCI DSS, soient résolues?	☐	☐	
		(c) Des analyses trimestrielles internes sont-elles effectuées par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié, et le cas échéant, l'indépendance organisationnelle de la personne qui a effectué le test (il n'est pas exigé d'être un QSA ou un ASV)?	☐	☐	
11.2.2		(a) Des analyses de vulnérabilité externe trimestrielles sont-elles exécutées?	☐	☐	
		(b) Les résultats des analyses trimestrielles satisfont-ils aux exigences du guide du programme ASV (par exemple, aucune vulnérabilité nominale supérieure à 4.0 selon le CVSS et aucune défaillance automatique)?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
		(c) Des analyses des vulnérabilités externes trimestrielles sont-elles effectuées par un prestataire de services d'analyse agréé (ASV) par le PCI SSC (conseil des normes de sécurité du secteur des cartes de paiement)?	☐	☐	
	11.2.3	(a) Des analyses externes et internes sont-elles réalisées après des modifications significatives (comme l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits)? ***Remarque** : les analyses réalisées après la modification des réseaux peuvent être effectuées par le personnel interne.*	☐	☐	
		(b) Le processus d'analyse comprend-il de nouvelles analyses jusqu'à ce que : • il n'existe aucune vulnérabilité avec un score supérieur à 4.0 selon le CVSS, pour les analyses externes; • un résultat réussi soit obtenu ou que toutes les vulnérabilités à « haut risque » définies dans l'exigence 6.2 des normes PCI DSS, soient résolues, pour les analyses internes?	☐	☐	
		(c) Les analyses sont-elles effectuées par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié, et le cas échéant, l'indépendance organisationnelle de la personne qui a effectué le test est-elle déterminée (il n'est pas exigé d'être un QSA ou un ASV)?	☐	☐	
11.3		(a) Des tests de pénétration externe et interne sont-ils effectués au moins annuellement et après une modification significative de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement)?	☐	☐	
		(b) Les vulnérabilités exploitables notées ont-elles été corrigées et le test a-t-il été répété?	☐	☐	
		(c) Les tests sont-ils effectués par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié, et le cas échéant, l'indépendance organisationnelle de la personne qui a effectué le test (il n'est pas exigé d'être un QSA ou un ASV)?	☐	☐	
		Ces tests de pénétration incluent-ils ce qui suit :			
	11.3.1	Tests de pénétration de la couche Réseau ***Remarque** : les tests doivent comprendre les composants qui prennent en charge les fonctions réseau ainsi que les systèmes d'exploitation.*	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	11.3.2	Tests de pénétration de la couche application ***Remarque** : ces tests doivent comprendre au minimum des vulnérabilités répertoriées dans l'exigence 6.5.*	☐	☐	
11.4	(a)	Des systèmes de détection d'intrusion et/ou des systèmes de prévention d'intrusion sont-ils utilisés pour surveiller l'intégralité du trafic dans l'environnement des données de titulaire de carte, ainsi que les points essentiels de cet environnement?	☐	☐	
	(b)	Les IDS et/ou IPS sont-ils configurés pour alerter le personnel si l'on suspecte des altérations potentielles?	☐	☐	
	(c)	Tous les moteurs de détection et de prévention des intrusions, les références et les signatures sont-ils tenus à jour?	☐	☐	
11.5	(a)	Des outils de surveillance de l'intégrité des fichiers sont-ils en place au sein de l'environnement des données de titulaire de carte? Exemples de fichiers qui doivent être surveillés : • les fichiers exécutables du système; • les fichiers exécutables de l'application; • les fichiers de configuration et de paramètres; • les journaux ou fichiers de vérification historiques ou archivés, stockés de manière centralisée.	☐	☐	
	(b)	Des outils de contrôle de l'intégrité des fichiers sont-ils paramétrés pour signaler au personnel tout changement non autorisé des fichiers du système, des fichiers de configuration, ou fichiers de contenu essentiels, et les outils exécutent-ils des comparaisons entre les fichiers essentiels au moins une fois par semaine? ***Remarque** : pour le contrôle de l'intégrité des fichiers, les fichiers stratégiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les produits de contrôle de l'intégrité des fichiers sont généralement préconfigurés avec les fichiers stratégiques pour le système d'exploitation associé. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).*	☐	☐	

Gérer une politique de sécurité des renseignements

Exigence 12 : Gérer une politique qui adresse les renseignements de sécurité à tout le personnel

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
12.1	Une politique est-elle définie, publiée, gérée et diffusée à tout le personnel compétent? *Dans le cadre de l'exigence 12, le terme « personnel » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou qui ont accès à l'environnement des données de titulaire de carte.*		☐	☐	
12.1.1	La politique satisfait-elle à toutes les exigences des normes PCI DSS?		☐	☐	
12.1.2	(a) Un processus annuel d'évaluation des risques est-il documenté pour identifier les menaces et les vulnérabilités, et déboucher sur une évaluation formelle des risques? (Des exemples des méthodologies d'évaluation des risques comprennent, mais sans s'y limiter, OCTAVE, ISO 27005 et NIST SP 800-30).		☐	☐	
	(b) Le processus d'évaluation des risques est-il exécuté au moins annuellement?		☐	☐	
12.1.3	La politique de sécurité des renseignements est-elle révisée au moins une fois par an et mise à jour le cas échéant, pour refléter les changements des objectifs commerciaux ou de l'environnement à risque?		☐	☐	
12.2	Des procédures de sécurité opérationnelles quotidiennes sont-elles élaborées conformément aux exigences de cette spécification (par exemple, des procédures de gestion des comptes d'utilisateur et des procédures d'examen des journaux), et comprennent-elles des procédures administratives et techniques pour chacune des exigences?		☐	☐	
12.3	Des politiques d'utilisation des technologies essentielles (par exemple, technologies d'accès à distance, technologies sans fil, supports électroniques amovibles, ordinateurs portables, assistants numériques personnels [PDA], courriel et utilisation d'Internet) sont-elles développées pour définir l'usage approprié de ces technologies par tous les employés et exigent-elles ce qui suit :				
12.3.1	L'approbation explicite des parties autorisées pour l'utilisation des technologies?		☐	☐	
12.3.2	L'authentification pour l'utilisation des technologies?		☐	☐	
12.3.3	La liste de tous les dispositifs et employés disposant d'un accès?		☐	☐	
12.3.4	Le marquage des dispositifs pour déterminer leur propriétaire, ses coordonnées et leur usage?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	12.3.5	Les usages acceptables des technologies?	☐	☐	
	12.3.6	Les emplacements acceptables des technologies sur le réseau?	☐	☐	
	12.3.7	La liste des produits reconnus par la société?	☐	☐	
	12.3.8	La déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique?	☐	☐	
	12.3.9	L'activation des technologies d'accès à distance pour les fournisseurs et les partenaires commerciaux uniquement lorsqu'ils en ont besoin, avec une désactivation immédiate après utilisation?	☐	☐	
	12.3.10	(a) Lors de l'accès du personnel aux données de titulaire de carte au moyen de technologies d'accès à distance, la politique interdit-elle la copie, le déplacement et le stockage de données de titulaire de carte sur des disques durs locaux et des supports électroniques amovibles, à moins d'une autorisation explicite pour des besoins professionnels définis?	☐	☐	
		(b) Pour le personnel possédant une autorisation adéquate, les politiques d'utilisation exigent-elles la protection des données de titulaire de carte conformément aux exigences PCI DSS?	☐	☐	
12.4		La politique et les procédures de sécurité définissent-elles clairement les responsabilités de tout le personnel en matière de sécurité des renseignements?	☐	☐	
12.5		La responsabilité de la sécurité des renseignements est-elle formellement attribuée à un chef de la sécurité ou à un autre membre compétent en sécurité de la direction?	☐	☐	
		Les responsabilités suivantes de gestion de la sécurité des renseignements sont-elles attribuées à un individu ou à une équipe :			
	12.5.1	Définir, documenter et diffuser les politiques et les procédures de sécurité	☐	☐	
	12.5.2	Contrôler et analyser les renseignements et les alertes de sécurité, et les diffuser au personnel compétent	☐	☐	
	12.5.3	Définir, documenter et diffuser des procédures d'escalade et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations	☐	☐	
	12.5.4	Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification de comptes	☐	☐	
	12.5.5	Surveiller et contrôler tous les accès aux données	☐	☐	
12.6		(a) Un programme formel de sensibilisation à la sécurité est-il mis en place pour sensibiliser tous les employés à l'importance de la sécurité des données de titulaire de carte?	☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
		(b) Les procédures du programme de sensibilisation à la sécurité comprennent-elle ce qui suit :			
	12.6.1	(a) Le programme de sensibilisation à la sécurité comporte-t-il diverses méthodes pour sensibiliser et former le personnel (par exemple, des affiches, des lettres, des mémos, une formation basée sur le Web, des réunions et des promotions)? ***Remarque :*** *les méthodes peuvent varier en fonction du rôle du personnel et de son niveau d'accès aux données de titulaire de carte.*	☐	☐	
		(a) Le personnel est-il formé au moment de son recrutement et au moins une fois par an?	☐	☐	
	12.6.2	Est-il exigé du personnel qu'il reconnaisse au moins une fois par an avoir lu et compris les procédures et la politique de sécurité?	☐	☐	
12.7		Les employés potentiels (voir la définition du terme « employé » au point 12.1 ci-dessus) font-ils l'objet de contrôles avant leur recrutement afin de réduire les risques d'attaques depuis des sources internes? (Des exemples de vérifications d'antécédents comprennent, la vérification des antécédents professionnels, du casier judiciaire, des antécédents en matière de crédit, et des références). ***Remarque*** *: pour le personnel potentiel à embaucher à certains postes, comme caissier dans un magasin, qui n'ont accès qu'à un numéro de carte à la fois à l'occasion du traitement d'une transaction, cette exigence n'est qu'une recommandation.*	☐	☐	
12.8		Si les données de titulaire de carte sont partagées avec des prestataires de services, des politiques et procédures sont-elles gérées et mises en œuvre pour la gestion de ces derniers, comme suit :			
	12.8.1	Une liste des prestataires de services est-elle tenue?	☐	☐	
	12.8.2	Un accord écrit par lequel les prestataires de services se reconnaissent responsables de la sécurité des données de titulaire de carte en leur possession a-t-il été signé?	☐	☐	
	12.8.3	Un processus de sélection des prestataires de services est-il bien défini et comprenant notamment des contrôles préalables à l'engagement?	☐	☐	
	12.8.4	Un programme est-il mis en place pour contrôler la conformité des prestataires de services aux PCI DSS au moins annuellement?	☐	☐	
12.9		Un plan de réponse aux incidents a-t-il été mis en œuvre dans la préparation d'une réponse immédiate à une faille du système, comme suit :			
	12.9.1	(a) Un plan de réponse aux incidents à mettre en œuvre en cas d'intrusion dans le système a-t-il été créé ?	☐	☐	

Question PCI DSS		Réponse :	Oui	Non	Spécial*
	(b) Le plan prévoit-il au moins les points suivants :				
		▪ Des rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment une notification des marques de cartes de paiement, au minimum.	☐	☐	
		▪ Des procédures de réponse aux incidents spécifiques.	☐	☐	
		▪ Des procédures de continuité et de reprise des affaires.	☐	☐	
		▪ Des processus de sauvegarde des données.	☐	☐	
		▪ Une analyse des exigences légales en matière de signalement des incidents.	☐	☐	
		▪ Une couverture et des réponses de tous les composants stratégiques du système.	☐	☐	
		▪ La référence ou l'inclusion des procédures de réponse aux incidents des marques de cartes de paiement.	☐	☐	
12.9.2	Le plan est-il testé au moins une fois par an?		☐	☐	
12.9.3	Des membres de personnel spécifiques sont-ils désignés pour répondre aux alertes 24 heures sur 24 et sept jours sur sept?		☐	☐	
12.9.4	Une formation appropriée du personnel en charge de la réponse aux violations de la sécurité est-elle organisée?		☐	☐	
12.9.5	Des alertes des systèmes de détection et de prévention des intrusions, et de contrôle de l'intégrité des fichiers sont-elles comprises dans le plan de réponse aux incidents?		☐	☐	
12.9.6	Un processus est-il développé et en place pour modifier et faire évoluer le plan de réponse aux incidents conformément aux leçons apprises et pour intégrer les évolutions du secteur?		☐	☐	

Annexe A : Autres exigences des PCI DSS s'appliquant aux fournisseurs d'hébergement partagé

Exigence A.1 : Les fournisseurs d'hébergement partagé doivent protéger l'environnement des données de titulaire de carte

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
A.1	Les données et l'environnement hébergé de chaque entité (c'est-à-dire un commerçant, un prestataire de services ou toute autre entité) sont-ils protégés selon les exigences A.1.1 à A.1.4 comme suit : *Un fournisseur d'hébergement doit satisfaire à ces exigences ainsi qu'aux autres sections pertinentes des normes PCI DSS.* *Remarque : même si un fournisseur d'hébergement peut satisfaire à ces exigences, le respect par l'entité qui a recours à ce dernier n'est pas garanti. Chaque entité doit se conformer aux normes PCI DSS et doit valider cette conformité comme applicable.*				
A.1.1	Chaque entité met-elle en œuvre les processus qui ont accès uniquement à l'environnement des données de titulaire de carte qui la concerne, et ces processus d'application sont-ils mis en œuvre en utilisant l'ID unique de l'entité? Par exemple : • aucune entité sur le système ne peut utiliser un ID utilisateur de serveur Web partagé. • Tous les scripts CGI utilisés par une entité doivent être créés et fonctionner en tant qu'ID utilisateur unique de l'entité.		☐	☐	
A.1.2	L'accès et les privilèges de chaque entité sont-ils limités à son propre environnement de données de titulaire de carte comme suit :				
	(a) Les ID utilisateurs pour les processus d'application ne sont-ils pas des utilisateurs privilégiés (racine/admin)?		☐	☐	
	(b) Chaque entité possède-t-elle les autorisations de lecture, écriture ou d'exécution, uniquement pour les fichiers et répertoires qu'elle possède ou pour des fichiers systèmes nécessaires (limités par l'autorisation d'un système de fichiers, des listes de contrôle d'accès, de commande chroot, d'interpréteur de commandes extrêmement limité, etc.)? *Important : les fichiers d'une entité ne peuvent pas être partagés par groupe.*		☐	☐	
	(c) Tous les utilisateurs d'une entité n'ont-ils pas un accès d'écriture aux données binaires d'un système partagé?		☐	☐	
	(d) La consultation des entrées du journal est-elle limitée à l'entité propriétaire?		☐	☐	

	Question PCI DSS	Réponse :	Oui	Non	Spécial*
	(e) Des restrictions sont-elles en place pour l'utilisation de ces ressources du système? • Espace de disque • Bande passante • Mémoire • Unité centrale *Cela garantit que chaque entité ne peut monopoliser les ressources de serveur pour exploiter les vulnérabilités (par exemple, erreur, fonctionnement et conditions de redémarrage entraînant, par exemple, la saturation de la mémoire tampon).*		☐	☐	
A.1.3	La consignation et les registres de vérification sont-ils activés, uniques à l'environnement des données de titulaire de carte de chaque entité et conformes à l'exigence 10 des normes PCI DSS? La journalisation est-elle activée comme suit pour chaque environnement de commerçant et de prestataire de services :		☐	☐	
	• Les journaux sont-ils activés pour des applications courantes de tiers?		☐	☐	
	• Les journaux sont-ils activés par défaut?		☐	☐	
	• Les journaux sont disponibles pour révision par l'entité propriétaire?		☐	☐	
	• Les emplacements des journaux sont-ils clairement communiqués à l'entité propriétaire?		☐	☐	
A.1.4	Des politiques et des processus écrits sont-ils activés pour fournir une investigation légale rapide en cas de compromission d'un commerçant ou d'un prestataire de services hébergé?		☐	☐	

Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux exigences PCI DSS telles qu'elles sont stipulées, en raison de contraintes commerciales documentées ou de contraintes techniques légitimes, mais qu'elle a parallèlement suffisamment atténué les risques associés par la mise en œuvre d'autres contrôles, appelés « contrôles compensatoires ».

Les contrôles compensatoires doivent satisfaire aux critères suivants :

1. Respecter l'intention et la rigueur de l'exigence initiale des normes PCI DSS.
2. Fournir une protection similaire à celle de l'exigence initiale des normes PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par l'exigence initiale (Pour plus de renseignements sur chaque exigence PCI DSS, voir *Parcourir les normes PCI DSS*).
3. Aller au-delà des autres exigences PCI DSS (Les contrôles compensatoires ne consistent pas simplement à se trouver en conformité à d'autres exigences PCI DSS).

   Lors de l'évaluation de la portée des contrôles compensatoires, il est essentiel de considérer les points suivants :

   Remarque : les points a) à c) ci-dessous sont cités à titre d'exemple seulement. L'évaluateur qui effectue l'examen des normes PCI DSS doit déterminer et valider la suffisance de tous les contrôles compensatoires. L'efficacité d'un contrôle compensatoire dépend des caractéristiques spécifiques de l'environnement dans lequel il est mis en œuvre, des contrôles de sécurité associés et de la configuration du contrôle proprement dit. Les sociétés doivent avoir conscience qu'un contrôle compensatoire particulier ne sera pas efficace dans tous les environnements.

   a) Les exigences existantes des normes PCI DSS NE PEUVENT PAS être considérées comme des contrôles compensatoires si elles sont déjà exigées pour l'élément examiné. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être transmis sous forme cryptée afin de limiter les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut utiliser d'autres exigences PCI DSS relatives aux mots de passe (blocage des intrus, mots de passe complexes, etc.) pour compenser l'absence de mots de passe cryptés, puisque celles-ci ne limitent pas les risques d'interception des mots de passe en texte clair. Par ailleurs, les autres contrôles de mots de passe sont déjà exigés par les normes PCI DSS pour l'élément examiné (à savoir les mots de passe).

   b) Les exigences existantes des normes PCI DSS PEUVENT être considérées comme des contrôles compensatoires si elles sont exigées dans un autre domaine, mais pas pour l'élément faisant l'objet d'une vérification. Par exemple, l'authentification à deux facteurs est exigée par les normes PCI DSS pour l'accès à distance. L'authentification à deux facteurs *depuis le réseau interne* peut aussi être considérée comme un contrôle compensatoire de l'accès administrateur non-console lorsque la transmission des mots de passe cryptés ne peut pas être prise en charge. L'authentification à deux facteurs peut être un contrôle compensatoire acceptable si : (1) elle satisfait l'intention de l'exigence initiale en résolvant les risques d'interception des mots de passe administrateur en texte clair, et (2) elle est correctement configurée et mise en œuvre dans un environnement sécurisé.

   c) Les exigences existantes des normes PCI DSS peuvent être associées à de nouveaux contrôles et constituer alors un contrôle compensatoire. Par exemple, si une société n'est pas en mesure de rendre les données de titulaire de carte illisibles conformément à l'exigence 3.4 (par exemple, par cryptage), un contrôle compensatoire pourrait consister en un dispositif ou un ensemble de dispositifs, d'applications et de contrôles qui assurent : (1) la segmentation du réseau interne; (2) le filtrage des adresses IP ou MAC; et (3) l'authentification à deux facteurs à partir du réseau interne.
4. Être proportionnel aux risques supplémentaires qu'implique le non-respect de l'exigence PCI DSS.

L’évaluateur doit évaluer soigneusement les contrôles compensatoires lors de chaque évaluation annuelle des normes PCI DSS afin de confirmer que chaque contrôle compensatoire couvre de manière appropriée le risque ciblé par l’exigence initiale des normes PCI DSS, conformément aux points 1 à 4 présentés ci-dessus. Pour maintenir la conformité, des processus et des contrôles doivent être en place pour garantir que les contrôles compensatoires restent efficaces après l'évaluation.

Annexe C : Fiche de contrôles compensatoires

Se référer à cette fiche pour définir des contrôles compensatoires pour toute exigence où la case « Oui » a été cochée et où des contrôles compensatoires ont été mentionnés dans la colonne « Spécial ».

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

Numéro et définition des exigences :

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

Fiche de contrôles compensatoires – Exemple complété

Se référer à cette fiche pour définir des contrôles compensatoires pour toute exigence où la case « Oui » a été cochée et où des contrôles compensatoires ont été mentionnés dans la colonne « Spécial ».

Numéro d'exigence : *8.1 – Tous les utilisateurs sont-ils identifiés avec un nom d'utilisateur unique qui les autorise à accéder aux composants du système ou aux données de titulaire de carte?*

	Renseignements requis	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	*La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « racine ». La société XYZ ne peut pas gérer le nom d'utilisateur « racine » ni consigner toutes les activités de chaque utilisateur « racine ».*
2. Objectif	Définir l'objectif du contrôle initial; identifier l'objectif satisfait par le contrôle compensatoire.	*L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des renseignements d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière.*
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	*L'absence d'ID d'utilisateur unique et le fait de ne pas pouvoir consigner les renseignements d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.*
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	*Une société XYZ va demander à tous les utilisateurs de se connecter aux serveurs à partir de leur bureau à l'aide de la commande SU. Cette commande autorise les utilisateurs à accéder au compte « racine » et à exécuter des actions sous ce compte, tout en permettant de consigner leurs activités dans le répertoire du journal SU. Il est ainsi possible de suivre les actions de chaque utilisateur par le biais du compte SU.*
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	*La société XYZ démontre à l'évaluateur l'exécution de la commande SU et lui montre que celle-ci permet d'identifier les utilisateurs connectés qui exécutent des actions sous le compte « racine ».*
6. Maintenance	Définir les processus et les contrôles en place pour la maintenance des contrôles compensatoires.	*La société XYZ décrit les processus et les procédures mis en place pour éviter la modification, l'altération ou la suppression des configurations SU de sorte que des utilisateurs individuels puissent exécuter des commandes racine sans que leurs activités soient consignées ou suivies.*

Annexe D : Explication de non-applicabilité

Si la mention « s.o. » ou « sans objet » a été saisie dans la colonne « Spécial », il est nécessaire d'utiliser cette fiche pour expliquer les raisons de la non-applicabilité des exigences à l'organisation.

Exigence	Raisons de non-applicabilité
Exemple : *9.3.1*	*Les visiteurs ne sont pas admis dans les zones où sont traitées ou conservées les données de titulaire de carte.*