Payment Card Industry (PCI)
Data Security Standard

Questionnaire d'auto-évaluation A-EP et attestation de conformité

Commerçants en commerce électronique à sous-traitance partielle utilisant un site Internet tiers pour le traitement des paiements

Version 3.0

Février 2014

Modifications apportées au document

Date	Version	Description
S.O.	1.0	Non utilisé.
S.O.	2.0	Non utilisé.
Février 2014	3.0	Nouveau SAQ pour adresser les conditions applicables aux commerçants du commerce électronique qui ne reçoivent pas eux-mêmes les données de titulaire de carte, mais qui ont une influence sur la sécurité de la transaction de paiement et/ou l'intégrité de la page qui accepte les données de titulaire de carte du consommateur. Le contenu est harmonisé avec les conditions de la norme PCI DSS v3.0 et des procédures de test.

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Table des matières

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Avant de commencer

Le SAQ A-EP a été développé pour adresser les conditions applicables aux commerçants du commerce électronique dont le ou les sites Internet ne reçoivent pas eux-mêmes les données de titulaire de carte, mais qui ont une influence sur la sécurité de la transaction de paiement et/ou l'intégrité de la page qui accepte les données de titulaire de carte du consommateur.

Les commerçants SAQ A-EP sont des commerçants en commerce électronique qui sous-traitent partiellement le réseau de paiement de commerce électronique à des tiers validés PCI DSS et qui ne stockent, traitent et ne transmettent pas de données de titulaire de carte par voie électronique sur leurs systèmes ou dans leurs locaux.

Commerçants SAQ A-EP confirmer que, pour ce réseau de paiement :

- Votre société accepte uniquement les transactions du commerce électronique ;
- Tous les traitements de données de titulaire de carte sont sous-traités à une entreprise de traitement tierce validée PCI DSS ;
- Votre site de commerce électronique ne reçoit pas de données de titulaire de carte, mais il contrôle comment les clients, ou leurs données de titulaire de carte sont orientés vers une entreprise de traitement tierce validée PCI DSS ;
- Votre site de commerce électronique n'est connecté à aucun autre système dans votre environnement (cela peut être obtenu en utilisant la segmentation de réseau pour isoler les autres périphériques POI des autres systèmes) ;
- Si le site Internet du commerçant est hébergé par un prestataire tiers, le prestataire est validé pour toutes les conditions applicables de la norme PCI DSS (par ex. inclure l'annexe A de PCI DSS si le prestataire est un fournisseur d'hébergement partagé) ;
- Tous les éléments des pages de paiement qui sont livrées sur l'ordinateur de client proviennent du site Internet du commerçant ou d'un ou de plusieurs prestataires de services conformes à la norme PCI DSS ;
- Votre société ne stocke, ne traite ni ne transmet des données de titulaires de carte sur ses systèmes ou dans ses locaux, mais confie la gestion de toutes ces fonctions à un ou plusieurs tiers ;
- Votre société a confirmé que le ou les tiers qui gèrent le stockage, le traitement et/ou la transmission des données de titulaire de carte sont conformes à la norme PCI DSS ; **et**
- Votre société conserve uniquement des reçus ou rapports papier avec des données de titulaire de carte, et ces documents ne sont pas reçus de manière électronique.

Ce SAQ s'applique à tous les réseaux de commerce électronique.

Cette version abrégée du SAQ comprend des questions s'appliquant à un type particulier d'environnement de petit commerçant, tel qu'il est défini dans les critères de qualification ci-dessus. S'il existe des conditions PCI DSS applicables à votre environnement qui ne sont pas couvertes par ce SAQ, cela peut être une indication du fait que ce SAQ n'est pas adapté à votre environnement. En outre, vous devez vous conformer à toutes les conditions PCI DSS applicables afin d'être conforme à la norme PCI DSS.

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

1. Identifier le SAQ applicable pour votre environnement – Consultez les *Instructions et directives relatives aux questionnaires d'auto-évaluation* sur le site Internet de PCI SSC pour de plus amples informations.
2. Confirmez que les paramètres de votre environnement sont corrects et correspondent aux critères d'éligibilité pour le SAQ que vous utilisez (ainsi que le définit la partie 2g de l'attestation de conformité).
3. Évaluer la conformité de votre environnement aux conditions applicables de la norme PCI DSS.
4. Complétez toutes les sections de ce document :
   - Section 1 (Parties 1 & 2 de l'AOC) – Informations relatives à l'évaluation et résumé.
   - Section 2 – Questionnaire d'auto-évaluation PCI DSS (SAQ A-EP)
   - Section 3 (Parties 3 & 4 de l'AOC) – Détails de validation et d'attestation, plan d'action pour les conditions de non-conformité (s'il y a lieu)
5. Envoyer le SAQ et l'attestation de conformité, ainsi que toute autre documentation requise, telle que des rapports d'analyse ASV, à votre acquéreur, à la marque de paiement ou autre demandeur.

Comprendre le questionnaire d'auto-évaluation

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

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

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

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

Tests attendus

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Remplir le questionnaire d'auto-évaluation

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

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

Réponse	Quand utiliser cette réponse :
Oui	Le test attendu a été effectué et tous les éléments de la condition ont été remplis ainsi qu'il est précisé.
Oui, avec CCW (Fiche de contrôle compensatoire)	Le test attendu a été effectué et tous les éléments de la condition ont été remplis avec l'aide d'un contrôle compensatoire. Pour toutes les réponses de cette colonne, remplir la fiche de contrôle compensatoire (CCW) dans l'annexe B du SAQ. Les informations concernant l'utilisation des contrôles compensatoires et les conseils pour aider à remplir la fiche se trouvent dans le PCI DSS.
Non	Certains, ou la totalité, des éléments de la condition n'ont pas été remplis, sont en cours de mise en œuvre, ou nécessitent d'autres tests avant de savoir s'ils sont en place.
S.O. (Sans objet)	La condition ne s'applique pas à l'environnement de l'organisation. (Voir ci-dessous les exemples de *directives de non-applicabilité de certaines conditions particulières spécifiques*). Toutes les réponses de cette colonne nécessitent une explication justificative dans l'Annexe C du SAQ.

Directives de non-applicabilité de certaines conditions particulières

Si certaines conditions sont considérées comme n'étant pas applicables à votre environnement, sélectionnez l'option « S.O. » pour cette condition spécifique et remplir la fiche « Explication de la non-applicabilité » dans l'annexe C pour chaque indication « S.O. ».

Exceptions légales

Si votre organisation est sujette à une restriction légale qui l'empêche de respecter une condition PCI DSS, cocher la colonne « Non » pour cette condition et remplir l'attestation pertinente dans la partie 3.

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Section 1 : Informations relatives à l'évaluation

Instructions de transmission

Ce document doit être complété en tant que déclaration des résultats de l'auto-évaluation du commerçant vis-à-vis des *Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données du secteur des cartes de paiement (PCI DSS).* Complétez toutes les sections : le commerçant est responsable de s'assurer que chaque section est remplie par les parties pertinentes, le cas échéant. Contacter l'acquéreur (la banque du commerçant) ou la marque de paiement pour déterminer les procédures de rapport et de demande.

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

Partie 1a. Informations sur le commerçant

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

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

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

Partie 2. Résumé

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

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

Quels types de réseaux de paiement votre entreprise sert-elle ? ☐ Commande postale/commande par téléphone (MOTO)	Quels réseaux de paiement sont couverts par ce SAQ ? ☐ Commande postale/commande par téléphone (MOTO)

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

☐ Commerce électronique ☐ Carte présente (face à face)	☐ Commerce électronique ☐ Carte présente (face à face)

Remarque : *Si votre organisation utilise un réseau ou un processus de paiement qui n'est pas couvert par ce SAQ, consultez votre acquéreur ou votre marque de paiement à propos de la validation des autres réseaux.*

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

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

Partie 2c. Emplacements

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

Type de local	Emplacement(s) du local (ville, pays)

Partie 2d. Application de paiement

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

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

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

Partie 2e. Description de l'environnement

Donner une description ***détaillée*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions entrantes et sortantes à l'environnement de données de titulaire de carte (CDE).* • *Composants critiques du système dans le CDE, tels que les appareils de POS, les bases de données, les serveurs Internet, etc., ainsi que les autres composants de paiement nécessaires, le cas échéant.*	
Est-ce que votre entreprise utilise la segmentation de réseau pour affecter la portée de votre environnement PCI DSS ?	☐ Oui

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

(Consulter la section « Segmentation de réseau » de PCI DSS pour les recommandations concernant la segmentation de réseau)	☐ Non

Partie 2f. Prestataires de services tiers

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

Si oui :

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

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

Partie 2g. Admissibilité à participer au questionnaire SAQ A-EP

Le commerçant certifie son admissibilité à compléter cette version abrégée du Questionnaire d'auto-évaluation dans la mesure où, pour ce réseau de paiement :

☐	Le commerçant accepte uniquement les transactions du commerce électronique ;
☐	Tous les traitements de données de titulaire de carte sont sous-traités à une entreprise de traitement tierce validée PCI DSS ;
☐	Le site de commerce électronique du commerçant ne reçoit pas de données de titulaire de carte, mais il contrôle comment les clients, ou leurs données de titulaire de carte sont orientés vers une entreprise de traitement tierce validée PCI DSS ;
☐	Le site de commerce électronique du commerçant n'est connecté à aucun autre système dans son environnement (cela peut être obtenu en utilisant la segmentation de réseau pour isoler les autres périphériques POI des autres systèmes) ;
☐	Si le site Internet du commerçant est hébergé par un prestataire tiers, le prestataire est validé pour toutes les conditions applicables de la norme PCI DSS (par ex. inclure l'annexe A de PCI DSS si le prestataire est un fournisseur d'hébergement partagé) ;
☐	Tous les éléments des pages de paiement qui sont livrées sur l'ordinateur de client proviennent du site Internet du commerçant ou d'un ou de plusieurs prestataires de services conformes à la norme PCI DSS ;
☐	Le commerçant société ne stocke, ne traite ni ne transmet des données de titulaires de carte sur ses systèmes ou dans ses locaux, mais confie la gestion de toutes ces fonctions à un ou plusieurs tiers ;
☐	Le commerçant a confirmé que le ou les tiers qui gèrent le stockage, le traitement et/ou la transmission des données de titulaire de carte sont conformes à la norme PCI DSS ; **et**
☐	Le commerçant conserve uniquement des reçus ou rapports papier avec des données de titulaire de carte, et ces documents ne sont pas reçus de manière électronique.

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Section 2 : Questionnaire d'auto-évaluation A-EP

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

Date d'achèvement de l'auto-évaluation :

Création et gestion d'un réseau sécurisé

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
1.1.4	(a) Un pare-feu est-il requis et implémenté au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne ?	▪ Examiner les standards de configuration de pare-feu ▪ Observer les configurations de réseau pour vérifier qu'un ou plusieurs pare-feu sont en place	☐	☐	☐	☐
	(b) Le schéma de réseau actuel est-il conforme aux normes de configuration des pare-feu ?	▪ Comparer les standards de configuration du pare-feu au schéma actualisé du réseau	☐	☐	☐	☐
1.1.6	(a) Les standards de configuration de pare-feu et de routeurs comprennent-ils une liste détaillée des services, protocoles et ports, avec la justification commerciale (protocoles HTTP [Hypertext Transfer Protocol], SSL [Secure Sockets Layer], SSH [Secure Shell] et VPN [Virtual Private Network]) ?	▪ Examiner les standards de configuration de pare-feu et de routeur	☐	☐	☐	☐
	(b) Tous les services, protocoles et ports non sécurisés sont-ils identifiés et les fonctions de sécurité sont-elles documentées et implémentées pour chaque service identifié ? ***Remarque :*** *Les protocoles FTP, Telnet, POP3, IMAP et SNMP sont des exemples de services, protocoles ou ports non sécurisés, mais ne sont pas les seuls.*	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
1.2	Les configurations de pare-feu restreignent-elles les connexions entre les réseaux non approuvés et les composants du système dans l'environnement des données des titulaires de carte comme suit : ***Remarque :*** *Un « réseau non approuvé » est tout réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.*					
1.2.1	(a) Les trafics entrants et sortants sont-ils restreints au trafic nécessaire à l'environnement des données des titulaires de carte ?	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
	(b) Tous les autres trafics entrants et sortants sont-ils explicitement refusés (par exemple à l'aide d'une instruction « refuser tout » explicite ou d'un refus implicite après une instruction d'autorisation) ?	▪ Examiner les standards de configuration de pare-feu et de routeur ▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.4	Des mesures anti-usurpation sont-elles mises en œuvre pour détecter et pour empêcher les adresses IP de source frauduleuses de pénétrer sur le réseau ? (Par exemple, bloquer le trafic originaire d'Internet avec une adresse interne).	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.5	Le trafic sortant de l'environnement des données des titulaires de carte vers Internet est-il explicitement autorisé ?	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
1.3.6	Un contrôle avec état, également connu comme filtrage des paquets dynamique, est-il en place, c'est-à-dire, seules les connexions établies sont autorisées sur le réseau ?	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
1.3.8	(a) Des moyens sont-ils en place pour prévenir la divulgation d'adresses IP et d'informations d'acheminement confidentielles sur Internet ? ***Remarque :*** *Quelques-unes des méthodes permettant de dissimuler les adresses IP sont présentées ci-après :* • *Traduction d'adresse réseau (Network Address Translation – NAT) ;* • *Protéger les serveurs contenant des données du titulaire derrière des serveurs proxy/pare-feu,* • *Retrait ou filtrage des annonces d'acheminement pour les réseaux privés employant des adresses enregistrées,* *Utilisation interne de l'espace d'adresse RFC1918 au lieu d'adresses enregistrées*.	▪ Examiner les configurations de pare-feu et de routeur	☐	☐	☐	☐
	(b) La divulgation d'adresses IP et d'informations d'acheminement confidentielles à des entités externes est-elle autorisée ?	▪ Examiner les configurations de pare-feu et de routeur ▪ Interroger le personnel	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.1	(a) Les paramètres par défaut définis par le fournisseur sont-ils toujours changés avant l'installation d'un système sur le réseau ? *Cette pratique s'applique à TOUS les mots de passe par défaut, y compris, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, application ou comptes de système, point de vente (POS) terminaux, chaînes de communauté de protocoles de gestion de réseau simple [SNMP], etc.).*	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Observer les configurations du système et les paramètres de compte ▪ Interroger le personnel	☐	☐	☐	☐
	(b) Les comptes par défaut inutiles sont-ils supprimés ou désactivés avant l'installation d'un système sur le réseau ?	▪ Examiner les politiques et les procédures ▪ Examiner la documentation du vendeur ▪ Examiner les configurations du système et les paramètres de compte ▪ Interroger le personnel	☐	☐	☐	☐
2.2	(a) Des normes de configurations sont-elles conçues pour tous les composants du système et sont-elles cohérentes avec les normes renforçant les systèmes en vigueur dans le secteur ? *Les sources des normes renforçant les systèmes en vigueur dans le secteur peuvent comprendre, entre autres, l'Institut SANS (SysAdmin Audit Network Security), le NIST (National Institute of Standards Technology), l'ISO (International Organization for Standardization) et le CIS (Center for Internet Security).*	▪ Examiner les standards de configuration du système ▪ Examiner les standards renforçant les serveurs acceptés par l'industrie ▪ Examiner les politiques et les procédures ▪ Interroger le personnel	☐	☐	☐	☐
	(b) Les normes de configuration du système sont-elles mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités, comme indiqué dans la condition 6.1 ?	▪ Examiner les politiques et les procédures ▪ Interroger le personnel	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(c) Les normes de configuration du système sont-elles appliquées lorsque de nouveaux systèmes sont configurés ?	▪ Examiner les politiques et les procédures ▪ Interroger le personnel	☐	☐	☐	☐
	(d) Les standards de configuration du système comprennent-ils tous les points suivants : • Changement de tous les paramètres par défaut fournis par le fournisseur et élimination de tous les comptes par défaut inutiles ? • Application d'une fonction primaire unique par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents ? • Activation unique des services, protocoles, démons, etc. nécessaires pour le fonctionnement du système ? • Implémentation des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaires que l'on estime non sécurisés ? • Configuration des paramètres de sécurité du système pour empêcher les actes malveillants ? • Suppression de toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus ?	▪ Examiner les standards de configuration du système	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.2.1	(a) Une seule fonction principale est-elle déployée par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents ? *Par exemple, les serveurs Web, les serveurs de bases de données et les serveurs DNS doivent être déployés sur des serveurs distincts.*	▪ Examiner les configurations de système	☐	☐	☐	☐
	(b) Si des technologies de virtualisation sont utilisées, seule une fonction principale est déployée par composant de système ou périphérique virtuels ?	▪ Examiner les configurations de système	☐	☐	☐	☐
2.2.2	(a) Seuls les services, protocoles, démons, etc. nécessaires sont-ils activés pour le fonctionnement du système (les services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction du périphérique sont désactivés) ?	▪ Examiner les standards de configuration ▪ Examiner les configurations de système	☐	☐	☐	☐
	(b) Les services, démons ou protocoles actifs et non sécurisés sont-ils justifiés selon les normes de configuration documentées ?	▪ Examiner les standards de configuration ▪ Interroger le personnel ▪ Examiner les paramètres de configuration ▪ Comparer les services activés, etc. aux justifications documentées	☐	☐	☐	☐
2.2.3	Les fonctions de sécurité supplémentaires sont-elles documentées et implémentées pour tout service, protocole ou démon nécessaire que l'on estime non sécurisé ? *Utiliser par exemple des technologies sécurisées, SSH, S-FTP, SSL ou IPSec VPN, pour protéger des services non sécurisés comme NetBIOS, le partage de fichiers, Telnet, FTP, etc.*	▪ Examiner les standards de configuration ▪ Examiner les paramètres de configuration	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
2.2.4	(a) Les administrateurs système et/ou le personnel paramétrant les composants du système connaissent-ils la configuration des paramètres de sécurité courants pour ces composants du système ?	▪ Interroger le personnel	☐	☐	☐	☐
	(b) La configuration des paramètres de sécurité courants est-elle comprise dans les normes de configuration du système ?	▪ Examiner les standards de configuration du système	☐	☐	☐	☐
	(c) La configuration des paramètres de sécurité est-elle installée de manière appropriée sur les composants du système ?	▪ Examiner les composants du système ▪ Examiner les paramètres de sécurité ▪ Comparer les paramètres aux standards de configuration du système	☐	☐	☐	☐
2.2.5	(a) Toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus, ont-elles été supprimées ?	▪ Examiner les paramètres de sécurité sur les composants du système	☐	☐	☐	☐
	(b) Les fonctions activées sont-elles détaillées et prennent-elles en charge une configuration sécurisée ?	▪ Examiner la documentation ▪ Examiner les paramètres de sécurité sur les composants du système	☐	☐	☐	☐
	(c) Seule la fonctionnalité documentée est-elle présente sur les composants de système ?	▪ Examiner la documentation ▪ Examiner les paramètres de sécurité sur les composants du système	☐	☐	☐	☐
2.3	L'accès administratif non-console est-il crypté de manière à : *Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion via le Web et autre accès administratif non-console.*					

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
	(a) Tous les accès administratifs non-console sont-ils cryptés avec une cryptographie robuste, et une méthode de cryptographie robuste est-elle invoquée avant de demander le mot de passe administrateur ?	▪ Examiner les composants du système ▪ Examiner les configurations de système ▪ Observer un administrateur se connecter	☐	☐	☐	☐
	(b) Tous les fichiers de services du système et de paramètres sont-ils configurés afin de prévenir l'utilisation de Telnet et d'autres commandes de connexions à distances non sécurisées ?	▪ Examiner les composants du système ▪ Examiner les services et les fichiers	☐	☐	☐	☐
	(c) L'accès administrateur aux interfaces de gestion Web est-il crypté au moyen d'une méthode de cryptage robuste ?	▪ Examiner les composants du système ▪ Observer un administrateur se connecter	☐	☐	☐	☐
	(d) Pour la technologie utilisée, une cryptographie robuste est-elle implémentée conformément aux meilleures pratiques du secteur et/ou aux recommandations du fournisseur ?	▪ Examiner les composants du système ▪ Examiner la documentation du vendeur ▪ Interroger le personnel	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Protection des données du titulaire

Condition 3 : Protéger les données du titulaire stockées

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
3.2	(c) Les données d'identification sensibles sont-elles supprimées ou rendues irrécupérables une fois le processus d'autorisation terminé ?	▪ Examiner les politiques et les procédures ▪ Examiner les configurations de système ▪ Examiner les processus de suppression	☐	☐	☐	☐
	(d) Tous les systèmes adhèrent-ils aux conditions suivantes concernant le non-stockage de données d'authentification sensibles après autorisation (même si elles sont cryptées) :					
3.2.2	Le code ou la valeur de vérification de carte (numéro à trois ou quatre chiffres imprimé sur le recto ou le verso d'une carte de paiement) n'est pas stocké après autorisation ?	▪ Examiner les sources de données, y compris : • Les données de transaction entrantes ; • Tous les journaux • Les fichiers d'historique • Les fichiers trace • Le schéma de base de données • Le contenu des bases de données	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
3.2.3	Le code d'identification personnelle (PIN) ou le bloc PIN crypté ne sont pas stockés après autorisation ?	▪ Examiner les sources de données, y compris : • Les données de transaction entrantes ; • Tous les journaux • Les fichiers d'historique • Les fichiers trace • Le schéma de base de données • Le contenu des bases de données	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Condition 4 : Crypter la transmission des données du titulaire sur les réseaux publics ouverts

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

	Question PCI DSS	Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
	(e) Pour les implémentations SSL/TLS, le SSL/TLS est activé lorsque les données du titulaire sont transmises ou reçues ? *Par exemple, pour les implémentations basées sur le navigateur :* • *La mention « HTTPS » apparaît comme protocole de l'adresse URL (Universal Record Locator, localisateur uniforme de ressource) du navigateur et* • *Les données du titulaire sont uniquement requises lorsque la mention « HTTPS » apparaît dans l'adresse URL.*	▪ Examiner les configurations de système	☐	☐	☐	☐
4.2	(b) Des politiques sont-elles déployées pour interdire la transmission de PAN non protégé à l'aide de technologies de messagerie pour utilisateurs finaux ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Gestion d'un programme de gestion des vulnérabilités

Condition 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
6.2	(a) Tous les logiciels et les composants du système sont-ils protégés des vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐
	(b) Les correctifs de sécurité essentiels sont-ils installés dans le mois qui suit leur publication ? ***Remarque** : Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.*	▪ Examiner les politiques et les procédures ▪ Examiner les composants du système ▪ Comparer la liste des correctifs de sécurité installés aux listes de correctifs fournis par les vendeurs	☐	☐	☐	☐
6.4.5	(a) Les procédures de contrôle de changement pour la mise en œuvre de correctifs de sécurité et les modifications de logiciel sont-elles documentées et nécessitent-elles les points suivants ? • Documentation de l'impact • Approbation de changement documentée par les parties autorisées • Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système. • Procédures de suppression	▪ Examiner les processus et les procédures de contrôle des changements	☐	☐	☐	☐
	(b) Les opérations suivantes sont-elles effectuées et documentées pour tous les changements :					
6.4.5.1	L'impact est-il documenté ?	▪ Retracer les changements sur la documentation de contrôle des changements ▪ Examiner la documentation de contrôle des changements	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
6.4.5.2	Le changement détaillé est-il approuvé par les responsables appropriés ?	▪ Retracer les changements sur la documentation de contrôle des changements ▪ Examiner la documentation de contrôle des changements	☐	☐	☐	☐
6.4.5.3	(a) Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système ?	▪ Retracer les changements sur la documentation de contrôle des changements ▪ Examiner la documentation de contrôle des changements	☐	☐	☐	☐
	(b) Pour les changements de code personnalisé, les tests de mises à jour du point de vue de la conformité à la condition 6.5 de la norme PCI DSS sont-ils effectués avant leur mise en production ?	▪ Retracer les changements sur la documentation de contrôle des changements ▪ Examiner la documentation de contrôle des changements	☐	☐	☐	☐
6.4.5.4	Procédures de suppression ?	▪ Retracer les changements sur la documentation de contrôle des changements ▪ Examiner la documentation de contrôle des changements	☐	☐	☐	☐
6.5	(c) Les applications sont-elles développées sur des directives de codage sécurisé afin de protéger les applications, au minimum, des vulnérabilités suivantes :					
6.5.1	Les techniques de codage adressent-elles les attaques par injection, en particulier injection de commandes SQL ? ***Remarque :*** *Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.*	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
6.5.2	Est-ce que les techniques de codage adressent les vulnérabilités de saturation de la mémoire tampon ?	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐
Pour les applications Web et les interfaces d'application (interne ou externe), les applications sont-elles développées sur la base de directives de codage sécurisé afin de protéger les applications des vulnérabilités suivantes :						
6.5.7	Les techniques de codage adressent-elles les vulnérabilités aux attaques XSS (Cross-Site) ?	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐
6.5.8	Les techniques de codage adressent-elles le contrôle d'accès inapproprié, tel que des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès URL, le survol de répertoire et la non-restriction de l'accès utilisateur aux fonctions ?	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐
6.5.9	Les techniques de codage adressent-elles les attaques CSRF (Cross-Site Request Forgery) ?	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐
6.5.10	Les techniques de codage adressent-elles la gestion de rupture d'authentification et de session ? ***Remarque :*** *La condition 6.5.10 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.*	▪ Examiner les politiques et les procédures de développement de logiciel. ▪ Interroger le personnel responsable	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
6.6	Pour les applications Web orientées public, les nouvelles menaces et vulnérabilités sont-elles traitées régulièrement et ces applications sont-elles protégées contre les attaques connues à l'aide de *l'une* des méthodes suivantes ? ▪ Réviser les applications Web orientées public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuels, comme suit : o Au moins une fois par an ; o Après toute modification ; o Par une société spécialisée dans la sécurité des applications ; o Toutes les vulnérabilités sont corrigées ; o L'application est réévaluée après les corrections. ***Remarque** : Cette évaluation est différente des scans de vulnérabilité effectués pour la condition 11.2.* **– OU –** ▪ Installer une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) devant les applications Web ouvertes au public pour vérifier continuellement tout le trafic.	▪ Examiner les processus documentés ▪ Interroger le personnel ▪ Examiner les registres d'évaluation de la sécurité des applications ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	**Oui, avec CCW**	**Non**	**S.O.**
7.1	L'accès aux composants du système et aux données des titulaires de carte est-il restreint aux seuls individus qui doivent y accéder pour mener à bien leur travail, comme suit :					
7.1.2	L'accès aux ID privilégiés est restreint comme suit : ▪ Au moins de privilèges nécessaires pour la réalisation du travail ? ▪ Uniquement affecté aux rôles qui nécessitent spécifiquement cet accès privilégié ?	▪ Examiner les politiques de contrôle d'accès ▪ Interroger le personnel ▪ Gestion de l'entretien ▪ Examiner les ID d'utilisateur privilégié	☐	☐	☐	☐
7.1.3	Les accès sont-ils basés sur la classification et la fonction professionnelles de chaque employé ?	▪ Examiner les politiques de contrôle d'accès ▪ Gestion de l'entretien ▪ Examiner les ID d'utilisateur	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Condition 8 : Identifier et authentifier l'accès aux composants du système

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.1.1	Tous les utilisateurs se voient-ils assigner un ID unique avant d'être autorisés à accéder aux composants du système ou aux données de titulaires de cartes ?	▪ Examiner les procédures de mot de passe ▪ Interroger le personnel	☐	☐	☐	☐
8.1.3	L'accès des utilisateurs qui ne travaillent plus pour la société est-il immédiatement désactivé ou révoqué ?	▪ Examiner les procédures de mot de passe ▪ Examiner les comptes d'utilisateur fermés ▪ Examiner les listes d'accès actuelles ▪ Observer les appareils d'authentification physique renvoyés	☐	☐	☐	☐
8.1.5	(a) Les comptes utilisés par les commerçants pour l'accès, le soutien ou la maintenance des composants du système par accès à distance sont activés uniquement pendant la période de temps nécessaire et désactivés lorsqu'ils ne sont pas utilisés ?	▪ Examiner les procédures de mot de passe ▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐
	(b) Les comptes d'accès à distance des fournisseurs sont-ils surveillés lorsqu'ils sont utilisés ?	▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐
8.1.6	(a) Les tentatives d'accès répétées sont-elles restreintes en verrouillant l'ID utilisateur après six tentatives au maximum ?	▪ Examiner les procédures de mot de passe ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐
8.1.7	Une fois un compte utilisateur verrouillé, la durée de verrouillage est-elle réglée à un minimum de 30 minutes ou jusqu'à ce que l'administrateur active l'ID utilisateur ?	▪ Examiner les procédures de mot de passe ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.2	Outre l'assignation d'un ID unique, l'une ou plusieurs des méthodes suivantes sont-elles employées pour authentifier tous les utilisateurs ? ▪ Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; ▪ Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; ▪ Quelque chose concernant l'utilisateur, comme une mesure biométrique.	▪ Examiner les procédures de mot de passe ▪ Observer les processus d'authentification	☐	☐	☐	☐
8.2.1	(a) Une cryptographie robuste est-elle utilisée pour rendre tous les justificatifs d'authentification (tels que les mots/phrases de passe) illisibles pendant la transmission et le stockage sur tous les composants du système ?	▪ Examiner les procédures de mot de passe ▪ Examiner la documentation du vendeur ▪ Examiner les paramètres de configuration du système ▪ Observer les fichiers de mot de passe ▪ Observer les transmissions de données	☐	☐	☐	☐
8.2.3	(a) Les paramètres de mot de passe utilisateur sont-ils configurés de sorte que les mots/phrases de passe respectent les points suivants ? • Des mots de passe d'une longueur d'au moins sept caractères. • Contenant à la fois des caractères numériques et des caractères alphabétiques. Autrement, les mots/phrases de passe doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.	▪ Examiner les réglages de configuration du système pour vérifier les paramètres de mot de passe.	☐	☐	☐	☐
8.2.4	(a) Les mots/phrases de passe utilisateurs sont-ils changés au moins tous les 90 jours ?	▪ Examiner les procédures de mot de passe ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.2.5	(a) Un individu doit-il soumettre un nouveau mot/phrase de passe différent des quatre derniers mots/phrases de passe qu'il a utilisés ?	▪ Examiner les procédures de mot de passe ▪ Essayer les composants du système ▪ Examiner les paramètres de configuration du système	☐	☐	☐	☐
8.2.6	Les mots/phrases de passe sont-ils définis sur une valeur unique pour chaque utilisateur à la première utilisation et chaque utilisateur doit-il modifier son mot de passe immédiatement après la première utilisation ?	▪ Examiner les procédures de mot de passe ▪ Examiner les paramètres de configuration du système ▪ Observer le personnel de sécurité	☐	☐	☐	☐
8.3	Une authentification à deux facteurs est-elle incorporée pour les accès à distance du personnel issu de l'extérieur du réseau (y compris pour les utilisateurs et les administrateurs) et pour tous les tiers (y compris l'accès du fournisseur à fin d'assistance ou de maintenance) ? ***Remarque :*** *L'authentification à deux facteurs requiert d'utiliser deux des trois méthodes d'authentification (voir la condition 8.2 pour la description des méthodes d'authentification). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à deux facteurs.* *Les exemples de technologies à deux facteurs comprennent l'authentification à distance et service de renseignements par téléphone (RADIUS) avec jetons ; les systèmes de contrôle d'accès au contrôleur d'accès du terminal (TACACS) avec jetons et les autres technologies permettant une authentification à deux facteurs.*	▪ Examiner les politiques et les procédures ▪ Examiner les configurations de système ▪ Observer le personnel	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
8.5	Les comptes et mots de passe ou autres méthodes d'authentification de groupe, partagée ou générique sont-ils interdits comme suit : ▪ Les ID d'utilisateur et les comptes génériques sont désactivés ou supprimés ; ▪ Il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ; ▪ Les ID d'utilisateur partagés ou génériques ne sont pas utilisés pour l'administration du moindre composant du système ?	▪ Examiner les politiques et les procédures ▪ Examiner les listes d'ID utilisateur ▪ Interroger le personnel	☐	☐	☐	☐
8.6	Lorsque les autres mécanismes d'authentification sont utilisés (par exemple, des jetons de sécurité logiques ou physiques, des cartes électroniques, certificats, etc.) l'utilisation de ces mécanismes est-elle assignée comme suit ? ▪ Les mécanismes d'authentification doivent être affectés à un compte individuel et non pas partagés par de multiples comptes ▪ Les contrôles logiques et/ou physiques doivent être en place pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès	▪ Examiner les politiques et les procédures ▪ Interroger le personnel ▪ Examiner les réglages de configuration du système et/ou les contrôles physiques	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
9.1	Des contrôles d'accès aux installations appropriés sont-ils en place pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de carte ?	▪ Observer les contrôles d'accès physique ▪ Observer le personnel	☐	☐	☐	☐
9.5	Tous les supports sont-ils physiquement sécurisés (entre autres, ordinateurs, supports électroniques amovibles, réseaux, reçus et rapports sur papier, et fax) ? *Dans le cadre de la condition 9, « support » se rapporte à tout support papier ou support électronique contenant des données de titulaires de carte.*	▪ Examiner les politiques et procédures en termes de sécurisation physique des supports ▪ Interroger le personnel	☐	☐	☐	☐
9.6	(a) Un contrôle strict s'applique-t-il à la distribution interne ou externe d'un type de support ?	▪ Examiner les politiques et procédures de distribution des supports	☐	☐	☐	☐
	(b) Les contrôles comprennent-ils les éléments suivants :					
9.6.1	Les supports sont-ils classés afin de déterminer la sensibilité des données qu'ils contiennent ?	▪ Examiner les politiques et procédures de classification des supports ▪ Interroger le personnel de la sécurité	☐	☐	☐	☐
9.6.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?	▪ Interroger le personnel ▪ Examiner les journaux de suivi et la documentation de distribution des supports	☐	☐	☐	☐
9.6.3	L'approbation de la direction est-elle obtenue avant le déplacement des supports (particulièrement lorsque le support est distribué aux individus) ?	▪ Interroger le personnel ▪ Examiner les journaux de suivi et la documentation de distribution des supports	☐	☐	☐	☐
9.7	Un contrôle strict est-il réalisé sur le stockage et l'accessibilité des supports ?	▪ Examiner les politiques et les procédures	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
9.8	(a) Tous les supports sont-ils détruits lorsqu'ils ne sont plus utiles pour des raisons professionnelles ou légales ?	▪ Examiner les politiques et procédures de destruction régulière de supports	☐	☐	☐	☐
	(c) La destruction des supports est-elle réalisée comme suit :					
9.8.1	(a) Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de sorte que les données de titulaires de carte ne puissent pas être reconstituées ?	▪ Examiner les politiques et procédures de destruction régulière de supports ▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐
	(b) Les contenants utilisés pour stocker les informations à détruire sont-ils sécurisés pour prévenir l'accès à leur contenu ?	▪ Examiner la sécurité des contenants de stockage	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Surveillance et test réguliers des réseaux

Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données du titulaire

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
10.3.2	Type d'événement ?	▪ Interroger le personnel ▪ Observer les journaux d'audit. ▪ Examiner les paramètres de journal d'audit.	☐	☐	☐	☐
10.3.3	Date et heure ?	▪ Interroger le personnel ▪ Observer les journaux d'audit. ▪ Examiner les paramètres de journal d'audit.	☐	☐	☐	☐
10.3.4	Indication de succès ou d'échec ?	▪ Interroger le personnel ▪ Observer les journaux d'audit. ▪ Examiner les paramètres de journal d'audit.	☐	☐	☐	☐
10.3.5	Origine de l'événement ?	▪ Interroger le personnel ▪ Observer les journaux d'audit. ▪ Examiner les paramètres de journal d'audit.	☐	☐	☐	☐
10.3.6	Identité ou nom des données, du composant du système ou de la ressource affectés ?	▪ Interroger le personnel ▪ Observer les journaux d'audit. ▪ Examiner les paramètres de journal d'audit.	☐	☐	☐	☐
10.5.4	Les registres des technologies orientées vers l'extérieur (par exemple, sans-fil, pare-feu, DNS, messagerie) sont-ils écrits sur un serveur de journal interne centralisé et sécurisé ou un support ?	▪ Interroger les administrateurs du système ▪ Examiner les configurations et les permissions du système	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
10.6	Les journaux et les événements de sécurité de tous les composants du système sont-ils analysés pour identifier les anomalies ou les activités suspectes comme suit ? ***Remarque :*** *Les outils de journalisation, d'analyse et d'alerte peuvent être utilisés conformément à la condition 10.6.*					
10.6.1	(b) Les journaux et événements de sécurité suivants sont-ils examinés au moins une fois par jour ? • Tous les événements de sécurité • Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD, ou qui pourraient avoir un impact sur la sécurité des CHD ou SAD • Les journaux de tous les composants critiques du système • Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.)	▪ Examiner les politiques de sécurité et les procédures ▪ Observer les processus ▪ Interroger le personnel	☐	☐	☐	☐
10.6.2	(b) Les journaux de tous les autres composants du système sont-ils examinés régulièrement - soit manuellement, soit à l'aide d'outils de journalisation, sur la base des politiques et de la stratégie de gestion des risques de l'organisation ?	▪ Examiner les politiques de sécurité et les procédures ▪ Examiner la documentation d'évaluation des risques ▪ Interroger le personnel	☐	☐	☐	☐
10.6.3	(b) Le suivi des exceptions et anomalies est-il identifié pendant le processus d'examen ?	▪ Examiner les politiques de sécurité et les procédures ▪ Observer les processus ▪ Interroger le personnel	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
10.7	(b) Les journaux d'audit sont-ils conservés pendant au moins un an ?	▪ Examiner les politiques de sécurité et les procédures ▪ Interroger le personnel ▪ Examiner les journaux d'audit	☐	☐	☐	☐
	(c) Les trois derniers mois de journaux au moins sont-ils disponibles pour analyse ?	▪ Interroger le personnel ▪ Observer les processus	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Gestion d'une politique de sécurité des informations

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

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

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.1	Une politique de sécurité est-elle établie, publiée, gérée et diffusée à tout le personnel compétent ?	▪ Examiner la politique de sécurité des informations	☐	☐	☐	☐
12.1.1	La politique de sécurité examinée comprend-elle au moins un examen annuel avec une mise à jour chaque fois que l'environnement change ?	▪ Examiner la politique de sécurité des informations ▪ Interroger le personnel responsable	☐	☐	☐	☐
12.4	La politique et les procédures de sécurité définissent-elles les responsabilités de tout le personnel en la matière ?	▪ Examiner la politique et les procédures de sécurité des informations ▪ Interroger un échantillon du personnel responsable	☐	☐	☐	☐
12.5	(b) Les responsabilités suivantes de gestion de la sécurité des informations sont-elles assignées à un individu ou à une équipe :					
12.5.3	Définir, renseigner et diffuser les procédures de remontée et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations ?	▪ Examiner la politique et les procédures de sécurité des informations	☐	☐	☐	☐
12.6	(a) Un programme formel de sensibilisation à la sécurité est-il implémenté pour sensibiliser tous les employés à l'importance de la sécurité des données de titulaires de cartes ?	▪ Examiner le programme de sensibilisation à la sécurité	☐	☐	☐	☐
12.8	Des politiques et des procédures sont-elles maintenues et mises en œuvre pour gérer les prestataires de service avec lesquels les données de titulaire de carte sont partagées, ou qui sont susceptibles d'affecter la sécurité des données de titulaire de carte, comme suit :					

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Question PCI DSS		Tests attendus	Réponse *(Cocher une seule réponse pour chaque question)*			
			Oui	Oui, avec CCW	Non	S.O.
12.10.1	(a) Un plan de réponse aux incidents a-t-il été créé pour être implémenté en cas d'intrusion dans le système ?	▪ Examiner le plan de réponse aux incidents ▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	(b) Le plan tient-il compte, au minimum des points suivants :					
	• Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Procédures de réponse aux incidents spécifiques ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Procédures de continuité et de reprise des affaires ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Processus de sauvegarde des données ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Analyse des conditions légales en matière de signalement des incidents ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Couverture et réponses de tous les composants stratégiques du système ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐
	• Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement ?	▪ Examiner les procédures de réponse aux incidents	☐	☐	☐	☐

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Annexe B : Fiche de contrôles compensatoires

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

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

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

Numéro et définition des clauses :

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Annexe C : Explication de non-applicabilité

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

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

En se basant sur les résultats mentionnés dans le SAQ A-EP en date du *(date d'achèvement)*, les signataires identifiés dans les parties 3b-3d, le cas échéant, confirment le statut de conformité suivant pour l'entité identifiée dans la partie 2 de ce document en date du *(date)* : (***biffer la mention applicable) :***

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

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

Partie 3a. Reconnaissance du statut

Le ou les signataires confirment :

(Cocher toutes les mentions applicables)

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

Partie 3b. Attestation de commerçant	
Signature du représentant du commerçant ↑	*Date :*
Nom du représentant du commerçant :	*Poste occupé :*

Partie 3c. Reconnaissance QSA (le cas échéant)	
Si un QSA a pris part ou a aidé à cette évaluation, décrire la fonction remplie :	

Signature du QSA ↑	*Date :*
Nom du QSA :	*Société QSA :*

Partie 3d. Reconnaissance ISA (le cas échéant)	
Si un ISA a pris part ou a aidé à cette évaluation, décrire la fonction remplie :	

Signature de l'ISA ↑	*Date :*
Nom de l'ISA :	*Poste occupé :*

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

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

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

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

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

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

Vérifier auprès de votre acquéreur ou de la ou des marques de paiement avant de compléter la Partie 4.

Condition PCI DSS	Description de la condition	Conforme aux conditions de la norme PCI DSS (Sélectionner un point)		Date et actions de mise en conformité (si « NON » a été sélectionné pour la moindre des conditions)
		OUI	NON	
1	Installer et gérer une configuration de pare-feu pour protéger les données du titulaire	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données du titulaire stockées	☐	☐	
4	Crypter la transmission des données du titulaire sur les réseaux publics ouverts	☐	☐	
5	Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus	☐	☐	
6	Développer et maintenir des systèmes et des applications sécurisés	☐	☐	
7	Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître	☐	☐	
8	Identifier et authentifier l'accès à tous les composants du système	☐	☐	
9	Restreindre l'accès physique aux données du titulaire	☐	☐	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données du titulaire	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.

12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐	

© 2006-2014 Conseil des normes de sécurité PCI, LLC. Tous droits réservés.