



**Payment Card Industry (PCI)
Data Security Standard**

Questionnaire d'auto-évaluation D et attestation de conformité

**Tous les autres commerçants et tous les
prestataires de services pouvant compléter un
questionnaire d'auto-évaluation**

Version 1.2

Octobre 2008

Modifications apportées au document

Date	Version	Description
1 ^{er} octobre 2008	1.2	Aligner le contenu avec la nouvelle procédure PCI DSS v1.2 et implémenter les changements mineurs notés depuis la v1.1 d'origine.

Table des matières

Modifications apportées au document	i
Normes PCI DSS : Documents connexes	iii
Avant de commencer	iv
Compléter le questionnaire d’auto-évaluation	iv
Étapes de mise en conformité avec les normes PCI DSS	iv
Directives sur la non-applicabilité et l’exclusion de certaines exigences spécifiques	v
Attestation de conformité, SAQ D—Version commerçant	1
Attestation de conformité, SAQ D—Version prestataire de services	4
Questionnaire d’auto-évaluation D	7
Création et gestion d’un réseau sécurisé	7
<i>Exigence 1 : Installer et gérer une configuration de pare-feu pour protéger les données...</i>	<i>7</i>
<i>Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur</i>	<i>9</i>
Protection des données de titulaire de carte de crédit	11
<i>Exigence 3 : Protéger les données de titulaire de carte stockées</i>	<i>11</i>
<i>Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts</i>	<i>13</i>
Gestion d’un programme de gestion des vulnérabilités	15
<i>Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement</i>	<i>15</i>
<i>Exigence 6 : Développer et gérer des systèmes et des applications sécurisés</i>	<i>15</i>
Mise en œuvre de mesures de contrôle d’accès strictes	18
<i>Exigence 7 : Restreindre l’accès aux données de titulaire de carte aux seuls individus qui doivent les connaître</i>	<i>18</i>
<i>Exigence 8 : Affecter un ID unique à chaque utilisateur d’ordinateur</i>	<i>18</i>
<i>Exigence 9 : Restreindre l’accès physique aux données de titulaire de carte</i>	<i>20</i>
Surveillance et test réguliers des réseaux	23
<i>Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte</i>	<i>23</i>
<i>Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité</i>	<i>24</i>
Gestion d’une politique de sécurité des informations	26
<i>Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants</i>	<i>26</i>
Annexe A : Autres exigences des normes PCI DSS s’appliquant aux fournisseurs d’hébergement partagé	29
<i>Exigence A.1 : Les prestataires de services d’hébergement partagé doivent protéger l’environnement des données de titulaire de carte</i>	<i>29</i>
Annexe B : Contrôles compensatoires	30
Annexe C : Fiche de contrôles compensatoires	31
Fiche de contrôles compensatoires – Exemple complété	32
Annexe D : Explication de non-applicabilité	33

Normes PCI DSS : 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 questionnaire d'auto-évaluation PCI DSS.

Document	Public
<i>Normes de sécurité des données de la PCI : Conditions et procédures d'évaluation de sécurité</i>	Tous les commerçants et les prestataires de services
<i>Navigation dans les normes PCI DSS : Comprendre l'objectif des exigences</i>	Tous les commerçants et les prestataires de services
<i>Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation</i>	Tous les commerçants et les prestataires de services
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation A et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation B et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation C et attestation</i>	Commerçants ¹
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation D et attestation</i>	Commerçants ¹ et tous les prestataires de services
<i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>	Tous les commerçants et les prestataires de services

¹ Pour déterminer le questionnaire d'auto-évaluation approprié, consultez le document *Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation*, « Sélection du questionnaire d'auto-évaluation et de l'attestation les plus appropriés pour votre entreprise ».

Avant de commencer

Compléter le questionnaire d'auto-évaluation

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

Type de validation SAQ	Description	SAQ
1	Commerçants carte absente (commerce électronique ou commande par courrier/téléphone), sous-traitance de toutes les fonctions de données de titulaire de carte. <i>Ne peut s'appliquer aux commerçants en face-à-face.</i>	A
2	Commerçants avec dispositif d'impression uniquement, sans stockage électronique de données de titulaire de carte	B
3	Commerçants avec terminal autonome, aucun stockage électronique de données de titulaire de carte	B
4	Commerçants avec systèmes de point de vente connectés à Internet, aucun stockage électronique de données de titulaire de carte	C
5	Tous les autres commerçants (non inclus dans les descriptions des SAQ A à C ci-dessus) et tous les prestataires de services pouvant compléter un questionnaire de par une marque de carte de paiement	D

Les commerçants ne répondant pas aux critères des SAQ A à C ci-dessus et tous les prestataires de services pouvant compléter un questionnaire d'auto-évaluation de par une marque de carte de paiement sont définis comme répondant au type de validation SAQ 5, selon ce document et les *instructions et directives sur le questionnaire d'auto-évaluation PCI DSS*.

Si la plupart des entreprises complétant le SAQ D doivent obtenir une validation de conformité pour toutes les exigences PCI DSS, certaines présentant des modèles commerciaux spécifiques ne sont pas concernées par l'ensemble des exigences. Par exemple, une entreprise qui n'utilise pas la technologie sans fil ne se voit pas contrainte d'obtenir une validation de conformité pour les sections des normes PCI DSS relatives à la technologie sans fil. Consultez les directives qui suivent pour plus d'informations 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. Complétez le questionnaire d'auto-évaluation (SAQ D) conformément aux *instructions du document Instructions et directives sur l'auto-évaluation*.
2. Faites faire une analyse des vulnérabilités par un prestataire de services d'analyse agréé (ASV) par le PCI SSC et procurez-vous auprès de lui un justificatif de l'exécution réussie de ces analyses.
3. Complétez l'attestation de conformité dans son intégralité.
4. Envoyez le questionnaire, le justificatif d'analyse réussie et l'attestation de conformité, avec tout autre document requis, à votre 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 et l'exclusion de certaines exigences spécifiques

Exclusion : S'il vous est demandé de répondre au SAQ D pour valider votre conformité aux normes PCI DSS, il est nécessaire de considérer les exceptions suivantes. Reportez-vous à la section « Non-applicabilité » ci-après pour plus d'informations.

- Les questions spécifiques à la technologie sans fil ne concernent que les entreprises 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 analyseur sans fil) même si votre réseau ne fait pas intervenir la technologie sans fil, l'analyseur détectant les périphériques non autorisés ou malveillants qui auraient pu être ajoutés à l'insu du commerçant.
- Les questions portant sur le code et les applications personnalisés (exigences 6.3-6.5) ne s'adressent qu'aux entreprises écrivant leurs propres applications Web personnalisées.
- Les questions des exigences 9.1-9.4 ne concernent que les installations avec des zones sensibles, comme définies ici. Par « zones sensibles », nous entendons tout centre de données, salle de serveurs ou zone abritant des systèmes qui stockent, traitent ou transmettent 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.

Non-applicabilité : Ces exigences et toutes celles jugées non applicables à votre environnement doivent être définies comme telles par la mention « s.o. » dans la colonne « Spécial » du SAQ. Vous devez compléter la fiche d'explication de non-applicabilité dans l'annexe pour chaque entrée « s.o. ».

Attestation de conformité, SAQ D—Version commerçant

Instructions de transmission

Le commerçant doit compléter cette attestation de conformité pour confirmer son statut de conformité avec le document *Normes de sécurité des données de la Payment Card Industry (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 normes PCI DSS » dans ce document.

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

Nom de l'entreprise :			
Nom du principal contact QSA :	Poste occupé :		
Téléphone :	Adresse électronique :		
Adresse professionnelle :	Ville :		
État/province :	Pays :	Code postal :	
URL :			

Partie 2. Informations sur le commerçant

Nom de l'entreprise :	DBA(s) :		
Nom du contact :	Poste occupé :		
Téléphone :	Adresse électronique :		
Adresse professionnelle :	Ville :		
État/province :	Pays :	Code postal :	
URL :			

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

- Détaillant
 Télécommunications
 Épicerie et supermarchés
 Pétrole
 Commerce électronique
 Commande par courrier/téléphone
 Autres (préciser) :

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

Partie 2b. Relations

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

Votre société entretient-elle une relation avec plusieurs acquéreurs ? Oui Non

Partie 2c. Traitement des transactions

Application de paiement utilisée : _____ Version de l'application de paiement : _____

Partie 3. Validation PCI DSS

Suite aux résultats du SAQ D du (*completion date*), (*Merchant Company Name*) déclare le statut de conformité suivant (cocher une case) :

- Conforme** : Toutes les sections du SAQ PCI sont complétées et toutes les questions ont reçu la réponse « Oui », d'où une note globale **CONFORME**, et une analyse a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. (*Merchant Company Name*) est donc en conformité avec les normes PCI DSS.
- Non conforme** : Toutes les sections du SAQ PCI ne sont pas complétées ou certaines questions ont reçu la réponse « Non », d'où une note 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. (*Merchant Company Name*) n'est donc pas en conformité avec les normes 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 cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter 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 normes PCI DSS, version (*version of SAQ*), a été complété conformément aux instructions fournies dans ce document.
- Toutes les informations présentes 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 bande magnétique (c'est-à-dire de pistes)², de données CAV2, CVC2, CID ou CVV2³, ou de données de code PIN⁴ suite à l'autorisation d'une transaction n'a été décelée sur AUCUN système lors de cette évaluation.

Partie 3b. Accusé de réception du commerçant

<i>Signature du représentant du commerçant</i> ↑	<i>Date</i> ↑
<i>Nom du représentant du commerçant</i> ↑	<i>Poste occupé</i> ↑

Nom de l'entreprise représentée ↑

² Données encodées sur la bande magnétique utilisée 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 ou à 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 PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

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

Sélectionner l'état de conformité approprié pour chaque condition. Si la réponse « Non » est donnée à la moindre condition, 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 cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

Exigences 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protéger les données de titulaire de carte stockées	<input type="checkbox"/>	<input type="checkbox"/>	
4	Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts	<input type="checkbox"/>	<input type="checkbox"/>	
5	Utiliser des logiciels antivirus et les mettre à jour régulièrement	<input type="checkbox"/>	<input type="checkbox"/>	
6	Développer et gérer des systèmes et des applications sécurisés	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître	<input type="checkbox"/>	<input type="checkbox"/>	
8	Affecter un ID unique à chaque utilisateur d'ordinateur	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restreindre l'accès physique aux données de titulaire de carte	<input type="checkbox"/>	<input type="checkbox"/>	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte	<input type="checkbox"/>	<input type="checkbox"/>	
11	Tester régulièrement les processus et les systèmes de sécurité	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gérer une politique de sécurité des informations	<input type="checkbox"/>	<input type="checkbox"/>	

Attestation de conformité, SAQ D—Version prestataire de services

Instructions de transmission

Le prestataire de services doit compléter cette attestation de conformité pour confirmer son statut de conformité avec le document *Normes de sécurité des données de la Payment Card Industry (PCI DSS) – Conditions et procédures d'évaluation de sécurité*. Il doit ensuite compléter toutes les sections applicables et se reporter aux instructions de transmission au niveau de « Étapes de mise en conformité avec les normes PCI DSS » dans ce document.

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

Nom de l'entreprise :					
Nom du principal contact QSA :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 2. Informations sur le prestataire de services

Nom de l'entreprise :					
Nom du contact :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 2a. Services

Services fournis (cocher toutes les cases adéquates) :

- | | | |
|--|---|---|
| <input type="checkbox"/> Autorisation | <input type="checkbox"/> Programmes de fidélité | <input type="checkbox"/> Serveur de contrôle d'accès sécurisé 3-D |
| <input type="checkbox"/> Commutation | <input type="checkbox"/> IPSP (commerce électronique) | <input type="checkbox"/> Traitement des transactions sur bandes magnétiques |
| <input type="checkbox"/> Passerelle de paiements | <input type="checkbox"/> Compensation et règlements | <input type="checkbox"/> Traitement des transactions MO/TO |
| <input type="checkbox"/> Hébergement | <input type="checkbox"/> Traitement des émissions | <input type="checkbox"/> Autres (préciser) : |

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

Partie 2b. Relations

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

Partie 2c. Traitement des transactions

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

Applications de paiement utilisées ou fournies dans le cadre de vos services :	Version de l'application de paiement :
--	--

Partie 3. Validation PCI DSS

Suite aux résultats du SAQ D du (*completion date of SAQ*), (*Service Provider Company Name*) déclare le statut de conformité suivant (cocher une case) :

Conforme : Toutes les sections du SAQ PCI sont complétées et toutes les questions ont reçu la réponse « Oui », d'où une note globale **CONFORME**, et une analyse a été réalisée avec succès par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. (*Service Provider Company Name*) est donc en conformité avec les normes PCI DSS.

Non conforme : Toutes les sections du SAQ PCI ne sont pas complétées ou certaines questions ont reçu la réponse « Non », d'où une note 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. (*Service Provider Company Name*) n'est donc pas en conformité avec les normes 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 cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter 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 (*insert version number*), a été complété conformément aux instructions fournies dans ce document.
- Toutes les informations présentes 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 bande magnétique (c'est-à-dire de pistes)⁵, de données CAV2, CVC2, CID ou CVV2⁶, ou de données de code PIN⁷ suite à l'autorisation d'une transaction n'a été décelée sur AUCUN système lors de cette évaluation.

Partie 3b. Accusé de réception du prestataire de services

<i>Signature du représentant du prestataire de services</i> ↑	<i>Date</i> ↑
<i>Nom du représentant du prestataire de services</i> ↑	<i>Poste occupé</i> ↑

Nom de l'entreprise représentée ↑

⁵ Données encodées sur la bande magnétique utilisée 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 ou à 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 PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

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

Sélectionner l'état de conformité approprié pour chaque condition. Si la réponse « Non » est donnée à la moindre condition, 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 cette information auprès de l'acquéreur ou de la marque de carte de paiement avant de compléter la Partie 4, puisque toutes les marques de cartes de paiement ne l'exigent pas.*

Exigences 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protéger les données de titulaire de carte stockées	<input type="checkbox"/>	<input type="checkbox"/>	
4	Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts	<input type="checkbox"/>	<input type="checkbox"/>	
5	Utiliser des logiciels antivirus et les mettre à jour régulièrement	<input type="checkbox"/>	<input type="checkbox"/>	
6	Développer et gérer des systèmes et des applications sécurisés	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître	<input type="checkbox"/>	<input type="checkbox"/>	
8	Affecter un ID unique à chaque utilisateur d'ordinateur	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restreindre l'accès physique aux données de titulaire de carte	<input type="checkbox"/>	<input type="checkbox"/>	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte	<input type="checkbox"/>	<input type="checkbox"/>	
11	Tester régulièrement les processus et les systèmes de sécurité	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gérer une politique de sécurité des informations	<input type="checkbox"/>	<input type="checkbox"/>	

Questionnaire d'auto-évaluation D

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		Réponse :	Oui	Non	Spécial*
1.1	Les normes définies de configuration des pare-feu et des routeurs incluent-elles les éléments suivants :				
1.1.1	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		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	Schéma de réseau actuel indiquant toutes les connexions aux données de titulaire de carte, notamment tous les réseaux sans fil		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	Exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Description des groupes, des rôles et des responsabilités pour la gestion logique des composants réseau		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	Documentation et justification professionnelle de l'utilisation de tous les services, protocoles et ports autorisés, y compris la documentation des fonctions de sécurité mises en œuvre pour les protocoles considérés comme étant non sécurisés		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Nécessité d'examiner les règles des pare-feu et des routeurs au moins tous les six mois		<input type="checkbox"/>	<input type="checkbox"/>	
1.2	La configuration de pare-feu limite-t-elle les connexions entre les réseaux non approuvés et tout système dans l'environnement des données de titulaire de carte, comme suit ? <i>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.</i>				
1.2.1.	Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données de titulaire de carte		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.2	Sécuriser et synchroniser les fichiers de configuration des routeurs		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Installer des pare-feu de périmètre entre tous les réseaux sans fil et l'environnement des données de titulaire de carte, et configurer ces pare-feu pour refuser ou contrôler le trafic (si celui-ci est nécessaire à des fins professionnelles) de l'environnement sans fil vers l'environnement des données de titulaire de carte		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :		
		Oui	Non	Spécial*
1.3	La configuration de pare-feu empêche-t-elle l'accès public direct entre Internet et tout composant du système dans l'environnement des données de titulaire de carte ?			
1.3.1	Une zone démilitarisée est-elle déployée pour limiter le trafic entrant et sortant aux seuls protocoles nécessaires à l'environnement des données de titulaire de carte ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	Le trafic Internet entrant est-il limité aux adresses IP dans la zone démilitarisée ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	Les acheminements directs sont-ils bannis pour le trafic entrant ou sortant entre Internet et l'environnement des données de titulaire de carte ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	Le passage des adresses internes d'Internet dans la zone démilitarisée est-il proscrit ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Le trafic sortant de l'environnement des données de titulaire de carte vers Internet est-il limité de sorte que ce trafic ne puisse accéder qu'aux adresses IP dans la zone démilitarisée ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	Le contrôle avec état, également appelé « filtrage des paquets dynamique » est-il mis en place (seules les connexions établies sont autorisées sur le réseau) ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	La base de données est-elle placée dans une zone de réseau interne, isolée de la zone démilitarisée ?	<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	Des masques IP sont-ils appliqués pour empêcher la conversion des adresses internes et leur divulgation sur Internet, à l'aide de l'espace d'adresse RFC 1918 ? <i>Utiliser des technologies de traduction d'adresses réseau (NAT, Network Address Translation), par exemple, la traduction d'adresses de ports (PAT, Port Address Translation).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
1.4	Un logiciel pare-feu personnel est-il installé sur tout ordinateur portable et/ou ordinateur appartenant à un employé équipé d'une connexion directe à Internet (par exemple, ordinateurs portables utilisés par les employés), qui est utilisé pour accéder au réseau de l'entreprise ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

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

Question		Réponse : <u>Oui</u> <u>Non</u> <u>Spécial*</u>		
2.1	<p>Les paramètres par défaut définis par le fournisseur sont-ils systématiquement modifiés avant d'installer un système sur le réseau ?</p> <p><i>Par exemple : inclure des mots de passe et des chaînes de communauté SNMP (Simple Network Management Protocol), et éliminer les comptes qui ne sont pas nécessaires.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	<p>(a) Les paramètres par défaut** pour les environnements sans fil connectés à l'environnement de données de titulaire de carte ou la transmission de données de titulaire de carte sont-ils modifiés avant d'installer un système sans fil ?</p> <p><i>** Par exemple : mots de passe, chaînes de communauté SNMP et clés de cryptage sans fil par défaut.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(b) Les paramètres de sécurité des périphériques sans fil sont-ils activés afin d'appliquer un cryptage robuste aux fonctionnalités d'authentification et de transmission ?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	<p>(a) Des normes de configuration ont-elles été élaborées pour tous les composants du système ?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(b) Ces normes couvrent-elles les vulnérabilités de sécurité connues et sont-elles compatibles avec les normes renforçant les systèmes en vigueur dans le secteur, par exemple SANS (SysAdmin Audit Network Security), NIST (National Institute of Standards Technology) et CIS (Center for Internet Security) ?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(c) Les contrôles garantissent-ils les éléments suivants :</p>			
2.2.1	N'y a-t-il qu'une seule fonction principale implémentée par serveur ?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Tous les services et protocoles non sécurisés et non requis (services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction spécifiée du périphérique) sont-ils désactivés ?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Les paramètres de sécurité du système sont-ils configurés de manière à empêcher les actes malveillants ?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	Toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus, sont-elles supprimées ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

	Question	Réponse : <u>Oui</u> <u>Non</u> <u>Spécial*</u>		
2.3	Tous les accès administratifs non-console sont-ils cryptés ? <i>Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion via le Web et autres accès administratifs non-console.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
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 ? Pour plus d'informations sur les exigences spécifiques à respecter, voir Annexe A : Autres exigences des normes PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.	<input type="checkbox"/>	<input type="checkbox"/>	

Protection des données de titulaire de carte de crédit

Exigence 3 : Protéger les données de titulaire de carte stockées

Question		Réponse :		Oui	Non	Spécial*
3.1	(a) Le stockage des données de titulaire de carte est-il limité au niveau minimal et la quantité des données stockées et les délais de conservation sont-ils limités aux conditions requises par l'entreprise, la loi et/ou les réglementations ?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Existe-t-il une politique de conservation et d'élimination des données et inclut-elle les limitations mentionnées en (a) ci-dessus ?	<input type="checkbox"/>	<input type="checkbox"/>			
3.2	Tous les systèmes respectent-ils les exigences suivantes en ce qui concerne le stockage des données d'authentification sensibles après autorisation (même cryptées) ?	<input type="checkbox"/>	<input type="checkbox"/>			
3.2.1	<p>Ne jamais stocker la totalité du contenu d'une quelconque piste de la bande magnétique (au verso d'une carte, sur une puce ou ailleurs). Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique.</p> <p><i>Remarque : Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique ci-après :</i></p> <ul style="list-style-type: none"> ▪ le nom du titulaire de la carte ; ▪ le numéro de compte principal (PAN, Primary Account Number) ; ▪ la date d'expiration ; ▪ le code de service. <p><i>Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité. NE JAMAIS stocker le code de vérification de la carte, ni la valeur, ni des éléments de données de valeur de vérification du code PIN.</i></p> <p><i>Remarque : Pour plus d'informations, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>			
3.2.2	<p>Ne pas stocker le code ou la valeur de validation (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement), utilisé pour vérifier les transactions carte absente.</p> <p><i>Remarque : Pour plus d'informations, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>			
3.2.3	Ne pas stocker de code PIN (Personal Identification Number) ou de bloc PIN crypté.	<input type="checkbox"/>	<input type="checkbox"/>			

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

	Question	Réponse :	Oui	Non	Spécial*
3.3	<p>Le PAN est-il masqué lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés) ?</p> <p>Remarques :</p> <ul style="list-style-type: none"> ▪ 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 (POS). 		<input type="checkbox"/>	<input type="checkbox"/>	
3.4	<p>Le PAN est-il rendu au minimum illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes ?</p> <ul style="list-style-type: none"> ▪ Hachage unilatéral s'appuyant sur une méthode cryptographique robuste ▪ Troncature ▪ Index tokens et Index pads (les pads doivent être stockés de manière sécurisée) ▪ Cryptographie robuste associée à des processus et des procédures de gestion des clés <p>En ce qui concerne les coordonnées de compte, au MINIMUM, le PAN doit être rendu illisible.</p> <p>Si, pour quelque raison que ce soit, une société ne peut pas rendre le PAN illisible, voir l'annexe B : « Contrôles compensatoires ».</p> <p>Remarque : Le terme « cryptographie robuste » est défini dans le Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	<p>Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne) :</p> <p>(a) L'accès logique est-il géré indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales) ?</p> <p>(b) Les clés de décryptage sont-elles indépendantes des comptes d'utilisateur ?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	<p>Les clés de cryptage utilisées pour le cryptage des données de titulaire de carte sont-elles protégées contre la divulgation et l'utilisation illicite ?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	<p>L'accès aux clés cryptographiques est-il limité au plus petit nombre d'opérateurs possible ?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	<p>Les clés cryptographiques sont-elles stockées de manière sécurisée dans aussi peu d'emplacements et de formes que possible ?</p>		<input type="checkbox"/>	<input type="checkbox"/>	

Question		Réponse :	Oui	Non	Spécial*
3.6	(a) Les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données de titulaire de carte sont-ils documentés en détail et déployés ? (b) Incluent-ils les éléments suivants ?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.1	Générer des clés cryptographiques robustes		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Sécuriser la distribution des clés cryptographiques		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Sécuriser le stockage des clés cryptographiques		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Changer périodiquement les clés cryptographiques : <ul style="list-style-type: none"> ▪ Comme cela est jugé nécessaire et recommandé par l'application associée (par exemple, recomposition) ; de préférence, automatiquement ▪ Au moins une fois par an 		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Supprimer ou remplacer les clés cryptographiques obsolètes ou soupçonnées d'avoir été compromises		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Fractionner les connaissances et l'établissement d'un double contrôle des clés cryptographiques		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Empêcher la substitution non autorisée des clés cryptographiques		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Exiger des opérateurs chargés de la gestion de clés cryptographiques de signer un formulaire reconnaissant qu'ils comprennent et acceptent leurs responsabilités		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		Réponse :	Oui	Non	Spécial*
4.1	Des protocoles de cryptographie et de sécurité robustes, tels que SSL/TLS ou IPSEC, sont-ils utilisés pour sauvegarder les données de titulaire de carte sensibles lors de leur transmission sur des réseaux publics ouverts ? <i>Voici des exemples de réseaux publics ouverts dans le cadre des normes PCI DSS : Internet, technologies sans fil, GSM (Global System For Mobile Communications) et GPRS (General Packet Radio Service).</i>		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question	Réponse :	<u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
4.1.1	<p>Les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont-elles utilisées pour appliquer un cryptage robuste 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 ?</p> <p><i>Remarques :</i></p> <ul style="list-style-type: none"> ▪ <i>Dans le cadre des nouveaux déploiements sans fil, la mise en œuvre du protocole WEP est interdite à compter du 31 mars 2009.</i> ▪ <i>Dans le cadre des déploiements actuels, la mise en œuvre du protocole WEP est interdite après le 30 juin 2010.</i> 	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	<p>Des politiques, procédures et pratiques sont-elles établies pour empêcher l'envoi de PAN non cryptés à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple, les e-mails, la messagerie instantanée, le chat) ?</p>	<input type="checkbox"/>	<input type="checkbox"/>	

Gestion d'un programme de gestion des vulnérabilités

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

Question		Réponse :	Oui	Non	Spécial*
5.1	Des logiciels antivirus sont-ils déployés sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs) ?		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Tous les programmes antivirus sont-ils capables de détecter et d'éliminer tous les types de logiciels malveillants connus, et de constituer une protection efficace contre ce fléau ?		<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Tous les mécanismes antivirus sont-ils à jour, en cours d'exécution et capables de générer des journaux d'audit ?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		Réponse :	Oui	Non	Spécial*
6.1	(a) Tous les logiciels et les composants du système sont-ils dotés des derniers correctifs de sécurité développés par le fournisseur ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les correctifs de sécurité stratégiques sont-ils installés dans le mois qui suit leur commercialisation ? <i>Remarque : Une entreprise 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 stratégiques (par exemple, bases de données, périphériques et systèmes orientés public) une priorité supérieure à celle des périphériques internes moins cruciaux, de sorte que les systèmes et les périphériques hautement prioritaires soient traités dans un délai d'un mois, tandis que les périphériques et systèmes moins stratégiques le soient dans un délai de trois mois.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) Existe-t-il un processus d'identification des nouvelles vulnérabilités de la sécurité (par exemple, abonnement à des services de notification gratuits sur Internet) ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les normes de configuration sont-elles mises à jour comme le demande l'exigence 2.2 des normes PCI DSS afin de résoudre les nouvelles vulnérabilités ?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Les applications logicielles sont-elles développées conformément aux normes PCI DSS (par exemple, authentification et connexion sécurisées) et sur la base des meilleures pratiques du secteur, et incorporent-elles des informations sur la sécurité tout au long du cycle de développement des logiciels ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les contrôles incluent-ils les procédures suivantes :				

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :	Oui	Non	Spécial*
6.3.1	Tester tous les correctifs de sécurité, ainsi que toute modification de configuration de système ou de logiciel avant déploiement, notamment ce qui suit :		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.1	Validation de toutes les entrées (afin d'empêcher les attaques XSS (Cross-Site Scripting), les attaques par injection, l'exécution de fichier malveillant, etc.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.2	Validation du traitement approprié des erreurs		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validation du stockage cryptographique sécurisé		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validation des communications sécurisées		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validation du RBAC (Role-Based Access Control) approprié		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Séparer les environnements de développement/test et de production		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Séparer les obligations entre les environnements de développement/test et de production		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Supprimer les données et les comptes de test avant que les systèmes de production ne deviennent actifs		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.6	Supprimer les comptes d'application personnalisés, les noms d'utilisateur et les mots de passe avant l'activation des applications ou leur mise à la disposition des clients		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.7	Examiner le code personnalisé avant sa mise en production ou sa mise à la disposition des clients afin d'identifier toute vulnérabilité du codage éventuelle <i>Remarque : Cette exigence s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de développement du système défini par l'exigence 6.3 des normes PCI DSS. Les examens du code peuvent être réalisés par le personnel interne compétent. 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 normes PCI DSS.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) Les procédures de contrôle des changements sont-elles respectées pour toutes les modifications apportées à des composants du système ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les procédures garantissent-elles les éléments suivants ?				
6.4.1	Documentation de l'impact		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Validation de la gestion par les parties appropriées		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Tests de fonctionnalité opérationnelle		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Procédures de suppression		<input type="checkbox"/>	<input type="checkbox"/>	

Question		Réponse :		Oui	No n	Spécial*
6.5	(a) Toutes les applications Web (internes et externes, y compris l'accès administratif Web au produit) sont-elles développées sur la base des meilleures pratiques de codage sécurisé, telles que celles décrites dans le Guide de l'OWASP (<i>Open Web Application Security Project</i>) ?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Les vulnérabilités de codage courantes sont-elles couvertes dans les processus de développement de logiciel, afin d'inclure les éléments suivants : <i>Remarque : Les vulnérabilités décrites aux points 6.5.1 à 6.5.10 étaient actualisées dans le guide de l'OWASP au moment de la publication des normes PCI DSS v1.2. Toutefois, si le guide de l'OWASP est mis à jour, il convient d'utiliser la version la plus récente de ces exigences.</i>					
6.5.1	Attaques XSS (Cross-Site Scripting)	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.2	Attaques par injection, notamment les injections de commandes SQL <i>Considérer également les attaques par injection LDAP et Xpath ainsi que les autres attaques par injection.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.3	Exécution de fichiers malveillants	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.4	Références d'objets directes non sécurisées	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.5	Attaques CSRF (Cross-Site Request Forgery)	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.6	Fuites d'information et traitement inapproprié des erreurs	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.7	Rupture dans la gestion des authentifications et des sessions	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.8	Stockage cryptographique non sécurisé	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.9	Communications non sécurisées	<input type="checkbox"/>	<input type="checkbox"/>			
6.5.10	Impossibilité de limiter l'accès aux URL	<input type="checkbox"/>	<input type="checkbox"/>			
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 : <ul style="list-style-type: none"> ▪ Examen des 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, au moins une fois par an et après toute modification ▪ Installation d'un pare-feu pour applications Web devant les applications Web orientées public 	<input type="checkbox"/>	<input type="checkbox"/>			

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Mise en œuvre de mesures de contrôle d'accès strictes

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

Question		Réponse :	Oui	Non	Spécial*
7.1	(a) 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 ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les restrictions d'accès incluent-elles les éléments suivants :				
7.1.1	Restriction des droits d'accès accordés aux ID d'utilisateur privilégiés en octroyant les privilèges les plus faibles qui sont nécessaires pour la réalisation du travail		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Octroi des privilèges sur la base de la classification et de la fonction professionnelles de chaque employé		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Nécessité de faire signer par les responsables un formulaire d'autorisation qui précise les privilèges requis		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Mise en œuvre d'un système de contrôle d'accès automatique		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) Un système de contrôle d'accès est-il défini pour les systèmes comptant plusieurs utilisateurs afin de limiter l'accès aux seuls utilisateurs qui doivent accéder aux données et est-il configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Ce système de contrôle d'accès inclut-il les éléments suivants :				
7.2.1	Couverture de tous les composants du système		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Octroi de privilèges aux individus reposant sur leur classification et leur fonction professionnelles		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Configuration par défaut du paramètre « Refuser tout »		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		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 ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.2	Outre l'affectation d'un ID unique, l'une des méthodes suivantes est-elle utilisée pour authentifier tous les utilisateurs ? <ul style="list-style-type: none"> ▪ Mot de passe ▪ Authentification à deux facteurs (par exemple, dispositifs à jetons, cartes à puce, biométrie ou clés publiques) 		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :	Oui	Non	Spécial*
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 ? <i>Utiliser des technologies telles que RADIUS (Remote Authentication and Dial-in User Service) ou TACACS (Terminal Access Controller Access Control System) avec des jetons ou VPN (basé sur SSL/TLS ou IPSEC) avec des certificats individuels.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
8.4	Tous les mots de passe sont-ils rendus illisibles pendant la transmission et le stockage sur tous les composants du système à l'aide d'une méthode de cryptographie robuste (définie dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>) ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Une gestion appropriée des mots de passe et de l'authentification des utilisateurs est-elle mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants du système comme suit :				
8.5.1	L'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiant font-ils l'objet de contrôles ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	L'identité des utilisateurs est-elle vérifiée avant la réinitialisation de leur mot de passe ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	Des mots de passe initiaux uniques ont-ils été définis pour chaque utilisateur et modifiés par l'utilisateur après la première utilisation ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	L'accès de tout utilisateur qui ne travaille plus pour la société est-il immédiatement révoqué ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	Les comptes d'utilisateur inactifs sont-ils supprimés ou désactivés au moins tous les 90 jours ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	Les comptes utilisés par les fournisseurs pour la maintenance à distance sont-ils activés pendant la période nécessaire seulement ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Les politiques et les procédures relatives aux mots de passe sont-elles communiquées à tous les utilisateurs qui ont accès aux données de titulaire de carte ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	Les comptes et les mots de passe collectifs, partagés ou génériques sont-ils proscrits ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	Les mots de passe utilisateur doivent-ils être modifiés au moins tous les 90 jours ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	Les mots de passe doivent-ils comporter au moins sept caractères ?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	Les mots de passe doivent-ils comporter des caractères alphanumériques ?		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question	Réponse :	Oui	Non	Spécial*
8.5.12	Un utilisateur doit-il soumettre un nouveau mot de passe différent de ses quatre derniers mots de passe ?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	Les tentatives d'accès répétées sont-elles limitées en verrouillant l'ID d'utilisateur après six tentatives au maximum ?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.14	La durée de verrouillage est-elle réglée sur 30 minutes au moins ou jusqu'à ce que l'administrateur active l'ID d'utilisateur ?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	Si une session reste inactive pendant plus de 15 minutes, est-il demandé à l'utilisateur de saisir de nouveau son mot de passe pour réactiver le terminal ?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	Tous les accès aux bases de données contenant des données de titulaire de carte sont-ils authentifiés ? Cette exigence concerne les accès des applications, des administrateurs et de tous les autres utilisateurs.	<input type="checkbox"/>	<input type="checkbox"/>	

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

Question	Réponse :	Oui	Non	Spécial*
9.1	Des contrôles d'accès aux installations appropriés sont-ils utilisés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaire de carte ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) Des caméras vidéo ou d'autres mécanismes de contrôle d'accès sont-ils installés pour surveiller l'accès physique des individus aux zones sensibles ? <i>Remarque : Par « zones sensibles », nous entendons tout 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, tels que les zones de caisse dans un magasin.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les données recueillies à l'aide des caméras vidéo sont-elles examinées et mises en rapport avec d'autres informations ?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Les données recueillies à l'aide des caméras vidéo sont-elles conservées pendant trois mois au minimum, sauf stipulation contraire de la loi ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	L'accès physique aux prises réseau accessibles au public est-il limité ?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	L'accès physique aux passerelles, appareils mobiles de poche et points d'accès sans fil est-il limité ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :	Oui	Non	Spécial*
9.2	Des procédures sont-elles mises en place pour aider l'ensemble du personnel à faire facilement la distinction entre les employés et les visiteurs, en particulier dans les zones où sont accessibles les données de titulaire de carte ? <i>Dans le cadre de cette exigence, le terme « employé » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité. Un « visiteur » est défini comme un fournisseur, l'invité d'un employé, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Tous les visiteurs sont-ils traités de la manière suivante :				
9.3.1	Une autorisation d'accès leur est donnée avant de pénétrer dans les zones où sont traitées et conservées les données de titulaire de carte.		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.2	Ils reçoivent un jeton physique (par exemple, badge ou dispositif d'accès) doté d'une date d'expiration et qui identifie bien les visiteurs comme ne faisant pas partie du personnel.		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	Il leur est demandé de rendre le jeton physique avant de quitter les locaux ou à la date d'expiration.		<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) Un registre des visites est-il utilisé pour tenir un contrôle physique de la circulation des visiteurs ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le nom du visiteur, l'entreprise qu'il représente et l'employé qui autorise son accès physique sont-ils indiqués dans ce registre ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Ce registre est-il conservé pendant trois mois au minimum, sauf stipulation contraire de la loi ?		<input type="checkbox"/>	<input type="checkbox"/>	
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 ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) La sécurité du site est-elle inspectée au moins une fois par an ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.6	Tous les documents papier et les supports électroniques contenant des données de titulaire de carte sont-ils rangés physiquement en lieu sûr ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) La distribution interne ou externe de tout type de support contenant des données de titulaire de carte est-elle soumise à un contrôle strict ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les contrôles incluent-ils les procédures suivantes :				
9.7.1	Les supports sont-ils classifiés de manière à les identifier comme contenant des informations confidentielles ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi ?		<input type="checkbox"/>	<input type="checkbox"/>	

	Question	Réponse :	<u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
9.8	Des processus et procédures sont-ils mis en place pour garantir l'obtention de l'approbation des responsables avant de déplacer tout ou partie des supports contenant des données de titulaire de carte d'une zone sécurisée (en particulier s'ils sont distribués à des personnes) ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Le stockage et l'accessibilité des supports contenant des données de titulaire de carte font-ils l'objet d'un contrôle strict ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	(a) Des journaux d'inventaire de tous les supports sont-ils tenus de manière appropriée ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Un inventaire des supports est-il organisé au moins une fois par an ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Les supports contenant des données de titulaire de carte sont-ils détruits lorsqu'ils ne sont plus nécessaires à des fins commerciales ou juridiques ? La destruction peut prendre diverses formes :		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de manière à ce qu'il soit impossible de les reconstituer ?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Les supports électroniques avec des données de titulaire de carte sont-ils rendus irrécupérables de sorte que les informations ne puissent pas être reconstituées ?		<input type="checkbox"/>	<input type="checkbox"/>	

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		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 root) à un utilisateur individuel ?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2	Des journaux d'audit automatiques sont-ils mis en œuvre pour tous les composants du système afin de reconstituer les événements suivants :				
10.2.1	Tous les accès des utilisateurs aux données de titulaire de carte		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	Toutes les actions exécutées par tout utilisateur avec des droits root ou administrateur		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Accès à tous les journaux d'audit		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Tentatives d'accès logique non valides		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Utilisation des mécanismes d'identification et d'authentification		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Initialisation des journaux d'audit		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Création et suppression d'objets au niveau système		<input type="checkbox"/>	<input type="checkbox"/>	
10.3	Les journaux d'audit consignent-ils au moins les entrées suivantes pour chaque événement :				
10.3.1	Identification des utilisateurs		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Type d'événement		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Date et heure		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Indication de succès ou d'échec		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origine de l'événement		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identité ou nom des données, du composant du système ou de la ressource affectés		<input type="checkbox"/>	<input type="checkbox"/>	
10.4	Toutes les heures et horloges système critiques sont-elles synchronisées ?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) Les journaux d'audit sont-ils protégés de sorte qu'ils ne puissent pas être modifiés ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les contrôles garantissent-ils les éléments suivants :				
10.5.1	L'affichage des journaux d'audit est-il limité aux utilisateurs qui en ont besoin pour mener à bien leur travail ?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	Les fichiers journaux d'audit sont-ils protégés contre toute modification non autorisée ?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	Les fichiers journaux d'audit sont-ils sauvegardés rapidement sur un serveur centralisé dédié à la journalisation ou sur des supports difficiles à altérer ?		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :	Oui	Non	Spécial*
10.5.4	Les journaux des technologies orientées vers l'extérieur sont-ils enregistrés sur un serveur dédié à la journalisation sur le réseau local (LAN) interne ?		<input type="checkbox"/>	<input type="checkbox"/>	
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) ?		<input type="checkbox"/>	<input type="checkbox"/>	
10.6	Les journaux relatifs à tous les composants du système sont-ils passés en revue au moins une fois par jour ? <i>L'examen des journaux doit inclure 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).</i> <i>Remarque : Les outils de journalisation, d'analyse et d'alerte peuvent être utilisés conformément à l'exigence 10.6.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	L'historique des journaux d'audit est-il conservé pendant une année au moins, en gardant à portée de main l'historique des journaux des trois derniers mois au moins pour une analyse immédiate (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde) ?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		Réponse :	Oui	Non	Spécial*
11.1	La présence de points d'accès sans fil est-elle testée à l'aide d'un analyseur sans fil au moins une fois par trimestre ou en déployant un IDS/IPS sans fil pour identifier tous les périphériques sans fil qui sont utilisés ?		<input type="checkbox"/>	<input type="checkbox"/>	
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 significatif des réseaux (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) ? <i>Remarque : Des analyses des vulnérabilités externes doivent être effectuées une fois par trimestre par un prestataire de services d'analyse agréé par le PCI SSC (Payment Card Industry Security Standards Council). Les analyses réalisées après la modification des réseaux peuvent être effectuées par le personnel interne de la société.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :		Oui	Non	Spécial*
11.3	(a) Des tests de pénétration externe et interne sont-ils effectués au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement) ?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Ces tests de pénétration incluent-ils ce qui suit :					
11.3.1	Tests de pénétration de la couche Réseau	<input type="checkbox"/>	<input type="checkbox"/>			
11.3.2	Tests de pénétration de la couche Application	<input type="checkbox"/>	<input type="checkbox"/>			
11.4	(a) Des systèmes de détection d'intrusions et/ou des systèmes de prévention d'intrusions sont-ils utilisés pour contrôler l'intégralité du trafic dans l'environnement des données de titulaire de carte et signaler au personnel tous les soupçons portant sur des altérations potentielles ?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Tous les moteurs de détection et de prévention des intrusions sont-ils mis à jour ?	<input type="checkbox"/>	<input type="checkbox"/>			
11.5	(a) Des logiciels de contrôle de l'intégrité des fichiers sont-ils déployés pour signaler au personnel toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques ?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Ces logiciels sont-ils configurés pour effectuer des comparaisons entre les fichiers stratégiques au moins une fois par semaine ? <i>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).</i>	<input type="checkbox"/>	<input type="checkbox"/>			

Gestion d'une politique de sécurité des informations

Exigence 12 : *Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants*

Question		Réponse :	Oui	Non	Spécial*
12.1	Une politique de sécurité est-elle définie, publiée, gérée et diffusée ? Remplit-elle les fonctions suivantes :		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Satisfait-elle toutes les exigences des normes PCI DSS ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	Inclut-elle un processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Comprend-elle au moins un examen annuel et est-elle mise à jour chaque fois que l'environnement change ?		<input type="checkbox"/>	<input type="checkbox"/>	
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) ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Des politiques d'utilisation des technologies orientées employés stratégiques (par exemple, technologies d'accès à distance, technologies sans fil, supports électroniques amovibles, ordinateurs portables, assistants numériques personnels (PDA), courrier électronique et utilisation d'Internet) sont-elles élaborées pour définir l'usage approprié de ces technologies par tous les employés et les sous-traitants ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Ces politiques d'utilisation exigent-elles ce qui suit :				
12.3.1	Approbation explicite des responsables		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentification de l'utilisation des technologies		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Liste de tous les périphériques et employés disposant d'un accès		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Indication sur les périphériques du nom de leurs propriétaires, de leurs coordonnées et de leur usage		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Usages acceptables des technologies		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Emplacements acceptables des technologies sur le réseau		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.7	Liste des produits approuvés par l'entreprise		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Activation des technologies d'accès à distance pour les fournisseurs strictement lorsque cela est nécessaire et désactivation immédiate de cet accès après usage		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question	Réponse :	Oui	Non	Spécial*
12.3.10	Lors de l'accès aux données de titulaire de carte au moyen de technologies d'accès à distance, la politique spécifie-t-elle l'interdiction de la copie, du déplacement et du stockage de données de titulaire de carte sur des disques durs locaux et des supports électroniques amovibles ?	<input type="checkbox"/>	<input type="checkbox"/>	
12.4	La politique et les procédures de sécurité définissent-elles clairement les responsabilités de tous les employés et sous-traitants en matière de sécurité des informations ?	<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Les responsabilités suivantes de gestion de la sécurité des informations sont-elles attribuées à un individu ou à une équipe ?			
12.5.1	Définir, documenter et diffuser les politiques et les procédures de sécurité	<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2	Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	
12.5.4	Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification de comptes	<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5	Surveiller et contrôler tous les accès aux données	<input type="checkbox"/>	<input type="checkbox"/>	
12.6	Un programme formel de sensibilisation à la sécurité est-il mis en place pour sensibiliser les employés à l'importance de la sécurité des données de titulaire de carte ?	<input type="checkbox"/>	<input type="checkbox"/>	
12.6.1	Les employés sont-ils sensibilisés au moment de leur recrutement et au moins une fois par an ?	<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Les employés doivent-ils reconnaître au moins une fois par an avoir lu et compris les procédures et la politique de sécurité de la société ?	<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Les employés potentiels (voir la définition du terme « employé » au point 9.2 ci-dessus) font-ils l'objet de contrôles avant leur recrutement afin de réduire les risques d'attaques depuis des sources internes ? <i>Pour les employés tels que les caissiers dans les magasins, 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.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Si des données de titulaire de carte sont partagées avec des prestataires de services, des politiques et procédures sont-elles mises en œuvre pour gérer les prestataires de services, et incluent-elles les éléments suivants ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

Question		Réponse :	Oui	Non	Spécial*
12.8.1	Une liste des prestataires de services est tenue.		<input type="checkbox"/>	<input type="checkbox"/>	
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 été signé.		<input type="checkbox"/>	<input type="checkbox"/>	
Question		Réponse :	Oui	Non	Spécial*
12.8.3	Un processus de sélection des prestataires de services est bien défini et inclut notamment des contrôles préalables à l'engagement.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Un programme est mis en place pour contrôler la conformité des prestataires de services avec les normes PCI DSS.		<input type="checkbox"/>	<input type="checkbox"/>	
12.9	Un plan de réponse aux incidents a-t-il été créé dans l'éventualité d'une intrusion dans le système ? Répond-t-il aux critères suivants :				
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 ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Le plan prévoit-il au moins les 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		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procédures de réponse aux incidents spécifiques		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procédures de continuité et de reprise des affaires		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Processus de sauvegarde des données		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Analyse des exigences légales en matière de signalement des incidents		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Couverture et réponses de tous les composants stratégiques du système		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.2	Le plan est-il testé au moins une fois par an ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	Des membres de personnel spécifiques sont-ils désignés pour répondre aux alertes 24 heures sur 24 et sept jours sur sept ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	Une formation appropriée du personnel en charge de la réponse aux violations de la sécurité est-elle organisée ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	Des alertes des systèmes de détection et de prévention des intrusions, et de contrôle de l'intégrité des fichiers sont-elles incluses ?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	Un processus de modification et de développement du plan de réponse aux incidents est-il défini en fonction des leçons apprises et de l'évolution du secteur ?		<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

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

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

Question		Réponse :		
		Oui	Non	Spécial*
A.1	<p>Les données et l'environnement hébergés de chaque entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité) sont-ils protégés conformément aux exigences A.1.1 à A.1.4 ? :</p> <p><i>Un prestataire de services d'hébergement doit satisfaire à ces exigences ainsi qu'aux autres sections pertinentes des normes PCI DSS.</i></p> <p><i>Remarque : Même si un prestataire de services d'hébergement peut satisfaire ces exigences, le respect par l'entité qui a recours au prestataire de services d'hébergement n'est pas garanti. Chaque entité doit se conformer aux normes PCI DSS et doit valider cette conformité comme applicable.</i></p>			
A.1.1	Chaque entité met-elle en œuvre uniquement les processus qui ont accès à l'environnement des données de titulaire de carte qui la concerne ?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	L'accès et les privilèges de chaque entité sont-ils limités à son propre environnement de données de titulaire de carte ?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	La journalisation et les journaux d'audit 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 ?	<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	Des processus d'investigation légale rapide sont-ils activés en cas d'incident dans l'environnement d'un commerçant ou d'un prestataire de services ?	<input type="checkbox"/>	<input type="checkbox"/>	

* Mention « s.o. » (sans objet) ou contrôle compensatoire utilisé. Les entreprises qui utilisent cette section doivent compléter la fiche de contrôles compensatoires ou la fiche d'explication de non-applicabilité, en annexe.

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 d'informations sur chaque exigence PCI DSS, voir *Navigation dans les normes PCI DSS*.)
3. Aller au-delà des autres exigences PCI DSS. (Les contrôles compensatoires ne consistent pas simplement en la conformité avec 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 entreprises 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 pas utiliser d'autres exigences relatives aux mots de passe des normes PCI DSS (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 examiné. Par exemple, l'authentification à deux facteurs est exigée par les normes PCI DSS pour l'accès à distance. L'authentification à deux facteurs à partir du 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 dans les conditions suivantes : (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 elle est 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.
- (c) Être proportionnel aux risques supplémentaires qu'implique le non-respect de l'exigence PCI DSS.

L'évaluateur doit évaluer soigneusement les contrôles compensatoires pendant 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 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.

Numéro et définition des exigences :

	Informations requises	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. Gestion	Définir les processus et les contrôles en place pour la gestion 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 ?*

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	<i>La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « root ». La société XYZ ne peut pas gérer le nom d'utilisateur « root » ni consigner toutes les activités de chaque utilisateur « root ».</i>
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	<i>L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des informations 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.</i>
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	<i>L'absence d'ID d'utilisateur unique et le fait de ne pas pouvoir consigner les informations d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.</i>
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.	<i>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 « root » 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.</i>
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	<i>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 « root ».</i>
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	<i>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 root sans que leurs activités soient consignées ou suivies.</i>

