



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

Questionnaire d'auto-évaluation C et attestation de conformité

**Application de paiement connectée à Internet,
aucun stockage électronique de données de
titulaire de carte**

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 C	1
Questionnaire d’auto-évaluation C	5
Création et gestion d’un réseau sécurisé	5
<i>Exigence 1 : Installer et gérer une configuration de pare-feu pour protéger les données...</i>	<i>5</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>5</i>
Protection des données de titulaire de carte de crédit	6
<i>Exigence 3 : Protéger les données de titulaire de carte stockées</i>	<i>6</i>
<i>Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts</i>	<i>7</i>
Gestion d’un programme de gestion des vulnérabilités	8
<i>Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement</i>	<i>8</i>
<i>Exigence 6 : Développer et gérer des systèmes et des applications sécurisés</i>	<i>8</i>
Mise en œuvre de mesures de contrôle d’accès strictes	9
<i>Exigence 7 : Restreindre l’accès aux données de titulaire de carte aux seuls individus qui doivent les connaître</i>	<i>9</i>
<i>Exigence 8 : Affecter un ID unique à chaque utilisateur d’ordinateur</i>	<i>9</i>
<i>Exigence 9 : Restreindre l’accès physique aux données de titulaire de carte</i>	<i>9</i>
Surveillance et test réguliers des réseaux	10
<i>Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte</i>	<i>10</i>
<i>Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité</i>	<i>10</i>
Gestion d’une politique de sécurité des informations	11
<i>Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants</i>	<i>11</i>
Annexe A : (non utilisée)	12
Annexe B : Contrôles compensatoires	13
Annexe C : Fiche de contrôles compensatoires	14
Fiche de contrôles compensatoires – Exemple complété	15
Annexe D : Explication de non-applicabilité	16

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 C a été conçu pour répondre aux besoins des commerçants qui traitent les données de titulaire de carte à l'aide d'applications de paiement (par exemple, systèmes de point de vente) connectées à Internet (via connexion haut débit, DSL, modem câble, etc.) mais qui ne stockent de données de titulaire de carte sur aucun autre système informatique. Ces applications de paiement sont connectées à Internet pour l'une des raisons suivantes :

1. L'application de paiement se trouve sur un ordinateur personnel connecté à Internet.
2. L'application de paiement est connectée à Internet pour transmettre des données de titulaire de carte.

Ces commerçants répondent au type de validation SAQ 4 selon ce document et les instructions et directives sur le questionnaire d'auto-évaluation PCI DSS. Les commerçants répondant au type de validation 4 traitent les données de titulaire de carte à l'aide de machines de point de vente connectées à Internet, ne stockent aucune donnée de titulaire de carte sur des systèmes informatiques et prennent en charge les transactions de type clic et mortier (carte présente) ou de type commerce électronique ou commande par courrier/téléphone (carte absente). Ils doivent obtenir une validation de conformité en complétant le SAQ C et l'attestation de conformité associée, en confirmant les éléments suivants :

- Votre entreprise possède un système d'application de paiement et une connexion Internet sur le même appareil.
- L'appareil avec l'application de paiement et la connexion Internet n'est connecté à aucun autre système dans votre environnement.
- Votre entreprise ne conserve que des rapports sur papier ou des copies sur papier des reçus.
- Votre entreprise ne stocke aucune donnée de titulaire de carte au format électronique.
- Le fournisseur de l'application de paiement de votre entreprise a recours à des techniques sécurisées afin d'offrir un service d'assistance à distance pour votre application de paiement.

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 C) 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.

Directives sur la non-applicabilité et l'exclusion de certaines exigences spécifiques

Exclusion : S'il vous est demandé de répondre au SAQ C pour valider votre conformité aux normes PCI DSS, il est nécessaire de considérer l'exception suivante. 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, exigence 2.1.1). 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.

Non-applicabilité : Cette exigence 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 C

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 2d. Conditions à remplir pour compléter le SAQ C

Le commerçant déclare être en droit de compléter cette version abrégée du questionnaire d'auto-évaluation en confirmant les éléments suivants :

- | | |
|--------------------------|--|
| <input type="checkbox"/> | Le commerçant possède un système d'application de paiement et une connexion Internet ou à un réseau public sur le même appareil. |
| <input type="checkbox"/> | L'appareil avec le système d'application de paiement et la connexion Internet n'est connecté à aucun autre système dans l'environnement du commerçant. |
| <input type="checkbox"/> | Le commerçant ne stocke aucune donnée de titulaire de carte au format électronique. |
| <input type="checkbox"/> | Si le commerçant stocke des données de titulaire de carte, il s'agit uniquement de rapports sur papier ou de copies de reçus sur papier, et ces documents ne sont pas reçus au format électronique. |
| <input type="checkbox"/> | Le fournisseur du logiciel d'application de paiement du commerçant a recours à des techniques sécurisées afin d'offrir un service d'assistance à distance pour le système d'application de paiement. |

Partie 3. Validation PCI DSS

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

- | | |
|--------------------------|--|
| <input type="checkbox"/> | 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. (<i>Merchant Company Name</i>) est donc en conformité avec les normes PCI DSS. |
| <input type="checkbox"/> | 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. (<i>Merchant Company Name</i>) 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 :

- | | |
|--------------------------|--|
| <input type="checkbox"/> | Le questionnaire d'auto-évaluation C des normes PCI DSS, version (<i>version of SAQ</i>), a été complété conformément aux instructions fournies dans ce document. |
| <input type="checkbox"/> | 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. |
| <input type="checkbox"/> | 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. |
| <input type="checkbox"/> | J'ai lu les normes PCI DSS et m'engage à garantir ma conformité avec leurs exigences à tout moment. |
| <input type="checkbox"/> | Aucune preuve de stockage de données de bande magnétique (c'est-à-dire de pistes) ² , de données CAV2, CVC2, CID ou CVV2 ³ , ou de données de code PIN ⁴ suite à l'autorisation d'une transaction n'a été décelée sur AUCUN système lors de cette évaluation. |

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 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 ↑

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"/>	
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 C

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 : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
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>	<input type="checkbox"/>	<input type="checkbox"/>	
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 ?	<input type="checkbox"/>	<input type="checkbox"/>	

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 Les paramètres par défaut définis par le fournisseur sont-ils systématiquement modifiés avant d'installer un système sur le réseau ? <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>	<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1 (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 ? <i>* Par exemple : mots de passe, chaînes de communauté SNMP et clés de cryptage sans fil par défaut.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
(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 ?	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	

* 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.

Protection des données de titulaire de carte de crédit

Exigence 3 : Protéger les données de titulaire de carte stockées

Question		Réponse : <u>Oui</u> <u>Non</u>		<u>Spécial*</u>
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>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"/>	
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><i>Remarques :</i></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"/>	

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

	Question	Réponse :	<u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
4.1	<p>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 ?</p> <p><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></p> <p><i>Remarque : Si votre environnement est équipé de la technologie sans fil, il est nécessaire de tenir compte des remarques suivantes :</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"/>	

* 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.

Gestion d'un programme de gestion des vulnérabilités

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

Question		Réponse : <u>Oui</u> <u>Non</u>		<u>Spécial*</u>
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 : <u>Oui</u> <u>Non</u>		<u>Spécial*</u>
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 (bases de données, périphériques et systèmes orientés public, etc.) 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"/>	

* 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 : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
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"/>	

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

Question	Réponse : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
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"/>	

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

Question	Réponse : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
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"/>	
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"/>	
9.10 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"/>	

* 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.

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 : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
Aucune question applicable dans le cadre du SAQ C.			

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

Question	Réponse : <u>Oui</u>	<u>Non</u>	<u>Spécial*</u>
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.

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 :		Spécial*
		Oui	Non	
12.1	Une politique de sécurité est-elle définie, publiée, gérée et diffusée ? Remplit-elle les fonctions suivantes :	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	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"/>	
12.3	(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"/>	
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 ?			
12.5.3	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"/>	
12.6	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"/>	
12.8	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"/>	
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"/>	
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"/>	

* 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 : (non utilisée)

Page laissée vide intentionnellement.

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.
4. 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>
7. 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>
8. 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>

