



**Secteur des cartes de paiement
Normes de sécurité des données
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 2.0

Octobre 2010

Modifications apportées au document

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

Table des matières

Modifications apportées au document	i
Normes de sécurité des données du PCI : documents connexes	iii
Avant de commencer	iv
Remplir le questionnaire d’auto-évaluation	iv
Étapes de mise en conformité avec les normes PCI DSS	v
Directives sur la non-applicabilité de certaines exigences spécifiques	v
Attestation de conformité, QAÉ C	1
Questionnaire d’auto-évaluation C	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>8</i>
Protection des données de titulaire de carte de crédit	9
<i>Exigence 3 : Protéger les données de titulaire de carte stockées</i>	<i>9</i>
<i>Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts</i>	<i>10</i>
Gestion d’un programme de gestion des vulnérabilités	11
<i>Exigence 5 : Utiliser des logiciels ou des programmes antivirus et les mettre à jour régulièrement</i>	<i>11</i>
<i>Exigence 6 : Développer et gérer des systèmes et des applications sécurisés</i>	<i>11</i>
Mise en œuvre de mesures de contrôle d’accès strictes	12
<i>Exigence 7 : Restreindre l’accès aux données de titulaire de carte aux seuls individus qui doivent les connaître</i>	<i>12</i>
<i>Exigence 8 : Affecter un ID unique à chaque utilisateur d’ordinateur</i>	<i>12</i>
<i>Exigence 9 : Restreindre l’accès physique aux données de titulaire de carte</i>	<i>12</i>
Surveillance et test réguliers des réseaux	14
<i>Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité</i>	<i>14</i>
Gérer une politique de sécurité des renseignements	16
<i>Exigence 12 : Gérer une politique qui adresse les renseignements de sécurité à tout le personnel</i>	<i>16</i>
Annexe A : (non utilisée)	18
Annexe B : Contrôles compensatoires	19
Annexe C : Fiche de contrôles compensatoires	21
Fiche de contrôles compensatoires – Exemple complété	22
L’Annexe D : Explication de non-applicabilité	23

Normes de sécurité des données du PCI : documents connexes

Les documents suivants ont été conçus de manière à aider les commerçants et les prestataires de services à comprendre les normes de sécurité des données du secteur des cartes de paiement (PCI DSS) et le QAÉ relatif à ces normes.

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

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

Avant de commencer

Remplir le questionnaire d'auto-évaluation

Le QAÉ 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 (par exemple, par DSL, modem câble, etc.) mais qui ne stockent des 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.

Les commerçants QAÉ C sont définis ici et dans le document *Instructions et directives concernant le questionnaire d'auto-évaluation relatif aux normes PCI DSS*. Les commerçants QAÉ C traitent les données de titulaire de carte par système d'application de paiement connecté à Internet, ne stockent aucune donnée de titulaire de carte sur des systèmes informatiques et prennent en charge les transactions de type authentique (carte présente) ou de type commerce électronique ou commande par courrier/téléphone (carte absente). Ils doivent obtenir une validation de conformité en remplissant le QAÉ C et l'attestation de conformité associée, en confirmant les éléments suivants :

- la société possède un système d'application de paiement et une connexion Internet sur le même dispositif et/ou le même réseau local (LAN);
- le dispositif Internet/application de paiement n'est pas connecté aux autres systèmes au sein de l'environnement (cela peut être réalisé par une segmentation de réseau pour isoler le dispositif Internet/système d'application de paiement de tous les autres systèmes);
- le magasin de la société n'est pas connecté à d'autres emplacements de magasin et un LAN correspond à un seul magasin uniquement;
- la société ne conserve que des rapports sur papier ou des copies sur papier des reçus;
- la société ne stocke aucune donnée de titulaire de carte au format électronique; et
- le fournisseur de l'application de paiement de la société a recours à des techniques sécurisées afin d'offrir un service d'assistance à distance pour l'application de paiement.

Chaque section de ce questionnaire est consacrée à un thème de sécurité spécifique, selon les exigences dans les *procédures d'évaluation de sécurité et exigences des normes PCI DSS*. Cette version abrégée du QAÉ comprend des questions qui s'appliquent à un type spécifique d'environnement de petit commerçant, tel qu'il est défini dans les critères d'admissibilité ci-dessus. S'il existe des exigences PCI DSS applicables à un environnement qui ne sont pas couvertes dans ce QAÉ, cela peut indiquer que ce QAÉ n'est pas adapté à cet environnement. En outre, il faut se conformer à toutes les exigences PCI DSS applicables pour être conforme aux normes PCI DSS.

Étapes de mise en conformité avec les normes PCI DSS

1. Évaluer la conformité d'un environnement aux normes PCI DSS.
2. Remplir le questionnaire d'auto-évaluation (QAÉ C) conformément aux instructions du document *Instructions et directives concernant le questionnaire d'auto-évaluation*.
3. Faire faire une analyse des vulnérabilités par un prestataire de services d'analyse agréé (ASV) par le PCI SSC et se procurer auprès de lui un justificatif de l'exécution réussie de ces analyses.
4. Remplir l'attestation de conformité dans son intégralité.
5. Envoyer le questionnaire, le justificatif d'analyse réussie et l'attestation de conformité, avec tout autre document requis, à l'acquéreur.

Directives sur la non-applicabilité de certaines exigences spécifiques

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

- Les questions spécifiques à la technologie sans fil concernent uniquement les organisations dont le réseau est équipé de la technologie sans fil (par exemple, exigences 1.2.3, 2.1.1 et 4.1.1). Il est nécessaire de répondre à l'exigence 11.1 (utilisation d'un processus pour identifier les points d'accès sans fil non autorisés) même si le réseau n'est pas doté de la technologie sans fil car le processus détecte les dispositifs non autorisés ou malveillants qui auraient pu être ajoutés sournoisement.

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

Attestation de conformité, QAÉ C

Instructions de transmission

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

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

Partie 1a. Renseignements sur la société du commerçant

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

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

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

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

- Détaillant
 Télécommunications
 Épiceries et supermarchés
 Pétrole
 Commerce électronique

 Vente par correspondance/téléphone
 Autres (préciser) :

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

Partie 2a. Relations

La société entretient-elle une relation avec un ou plusieurs prestataires de services tiers (par exemple, passerelles, sociétés d'hébergement sur le Web, tour opérateurs, agents de

Oui Non

programmes de fidélité, etc.)?

La société entretient-elle une relation avec plusieurs acquéreurs?

Oui
Non

Partie 2b. Traitement des transactions

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

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

<u>Application de paiement utilisée</u>	<u>Numéro de version</u>	<u>Dernière version validée conformément aux PABP/PA-DSS</u>

Partie 2c. Conditions à remplir pour compléter le QAÉ C

Le commerçant déclare être en droit de remplir 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 dispositif et/ou le même réseau local (LAN).
<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 magasin du commerçant n'est pas connecté à d'autres sites de magasin et un LAN correspond à un seul magasin uniquement.
<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 des PCI DSS

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

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

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

Date cible de mise en conformité :

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

Partie 3a. Confirmation de l'état de conformité

Le commerçant confirme les éléments suivants :

<input type="checkbox"/>	Le questionnaire d'auto-évaluation C des PCI DSS, version (<i>version du QAÉ</i>), a été rempli selon les instructions fournies dans ce document.
<input type="checkbox"/>	Tous les renseignements présents dans le questionnaire d'auto-évaluation susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats des évaluations, à tous points de vue.
<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 bandes magnétiques (c'est-à-dire des pistes) ² , de données CAV2, CVC2, CID ou CVV2 ³ , ou de données du NIP ⁴ après autorisation de transaction n'a été trouvée sur AUCUN des systèmes examinés pendant cette évaluation.

Partie 3b. Accusé de réception du commerçant

<i>Signature du représentant du commerçant</i> ↑	<i>Date</i> ↑
<i>Nom du représentant du commerçant</i> ↑	<i>Titre</i> ↑

Nom de la société représentée ↑

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

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

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

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

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

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 qui adresse les renseignements de sécurité à tout le personnel	<input type="checkbox"/>	<input type="checkbox"/>	

Questionnaire d'auto-évaluation C

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

Date de réalisation :

Création et gestion d'un réseau sécurisé

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

Question PCI DSS		Réponse :	Oui	Non	Spécial*
1.2	Les configurations de pare-feu limitent-elles 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 un réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.</i>				
1.2.1	(a) Le trafic entrant et sortant est-il limité au trafic nécessaire à l'environnement des données de titulaire de carte, et ces limitations sont-elles documentées?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Tous les autres trafics entrants et sortants sont-ils spécifiquement refusés (par exemple en utilisant un paramètre « refuser tout » explicite ou un refus implicite après une autorisation)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Des pare-feu de périmètre sont-ils installés entre tous les réseaux sans fil et l'environnement des données de titulaire de carte, et ces pare-feu sont-ils configurés 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"/>	
1.3	La configuration de pare-feu empêche-t-elle l'accès public direct entre Internet et les composants du système dans l'environnement des données de titulaire de carte comme suit :				
1.3.3	Les connexions directes sont-elles bannies pour le trafic entrant ou sortant entre Internet et l'environnement des données de titulaire de carte?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Le trafic sortant de l'environnement des données de titulaire de carte vers Internet est-il explicitement autorisé?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	Le contrôle avec état, également appelé « filtrage dynamique à paquets » est-il mis en place (seules les connexions établies sont autorisées sur le réseau)?		<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 PCI DSS		Réponse :	Oui	Non	Spécial*
2.1	Les paramètres par défaut définis par le fournisseur sont-ils systématiquement modifiés avant d'installer un système sur le réseau? <i>Les paramètres par défaut définis par le fournisseur comprennent, mais sans s'y limiter, les mots de passe et les protocoles de gestion de réseau simples (SNMP), et l'élimination des comptes qui ne sont pas nécessaires.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	Dans les environnements sans fil connectés à l'environnement de données de titulaire de carte ou la transmission de données de titulaire de carte, les paramètres par défaut sont-ils modifiés comme suit :				
	(a) Les clés de cryptage par défaut sont-elles changées à l'installation, et chaque fois que quelqu'un ayant eu connaissance de ces clés a quitté la société ou changé de poste?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les chaînes de communauté SNMP par défaut sur les dispositifs sans fil sont-elles changées?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Les mots de passe/phrases passe par défaut sur les points d'accès sont-ils changés?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Le micrologiciel sur les dispositifs sans fil est-il mis à jour afin de prendre en charge un cryptage performant pour l'authentification et la transmission sur les réseaux sans fil?		<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Les autres paramètres par défaut du fournisseur du dispositif sans fil, relatifs à la sécurité, sont-ils changés, le cas échéant?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	(a) Les seuls services, protocoles, démons, etc. nécessaires sont-ils activés comme exigé par la fonction du système (les services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction spécifiée du dispositif sont désactivés)?		<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Tous les accès administratifs non-console sont-ils cryptés afin de : <i>Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion via le Web et autres accès administratifs non-console.</i>				
	(a) Tous les accès administratifs non-console sont-ils cryptés avec une cryptographie performante, et une méthode de cryptographie performante est-elle invoquée avant de demander le mot de passe de l'administrateur?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Tous les services et les fichiers de paramètre du système sont-ils configurés pour empêcher l'utilisation de Telnet et d'autres commandes de connexion à distance non sécurisées?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) L'accès de l'administrateur aux interfaces de gestion basées sur le Web est-il crypté avec une cryptographie performante?		<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 PCI DSS	Réponse :	Oui	No n	Spécial*
3.2 (b) Si des données d'authentification sensibles sont reçues et supprimées, les processus sont-ils mis en œuvre pour sécuriser la suppression des données afin de garantir que les données sont irrécupérables?		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Tous les systèmes respectent-ils les exigences suivantes en ce qui concerne le non-stockage des données d'authentification sensibles après autorisation (même cryptées)?				
3.2.1 La totalité du contenu d'une quelconque piste de bande magnétique (située au verso d'une carte, données équivalentes sur une puce ou ailleurs) n'est-elle jamais stockée, en aucune circonstance? Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique. <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> <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. <i>Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2 Le code ou la valeur de validation de la carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement) ne sont-ils jamais stockés, en aucune circonstance?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3 Le code NIP (numéro d'identification personnel) ou le bloc NIP crypté ne sont-ils jamais stockés, en aucune circonstance?		<input type="checkbox"/>	<input type="checkbox"/>	
3.3 Le PAN est-il masqué lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés)? <i>Remarques :</i> <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. 		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question PCI DSS		Réponse :	Oui	Non	Spécial*
4.1	<p>(a) Des protocoles de cryptographie et de sécurité performantes, 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>De exemples de réseaux publics ouverts dans la portée des PCI DSS, comprennent, mais sans s'y limiter, Internet, technologies sans fil, GSM (Global System For Mobile Communications) et GPRS (General Packet Radio Service).</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Seuls les clés et/ou certificats approuvés sont-ils acceptés?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Les protocoles de sécurité sont-ils mis en œuvre pour utiliser uniquement des configurations sécurisées et ne pas prendre en charge des versions ou configurations non sécurisées?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) La puissance de cryptage adéquate est-elle mise en œuvre au regard de la méthodologie de cryptage utilisée (vérifier les recommandations/meilleures pratiques du fournisseur)?		<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(e) Pour les mises en œuvre SSL/TLS :</p> <ul style="list-style-type: none"> • HTTPS apparaît-il dans l'adresse URL? • Les données de titulaire de carte sont-elles exigées uniquement lorsque HTTPS apparaît dans l'adresse URL? 		<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	<p>Les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont-elles utilisées pour appliquer un cryptage performant pour l'authentification et la transmission pour les réseaux sans fil sur lesquels sont transmises les données de titulaire de carte ou qui sont connectés à l'environnement des données de titulaire de carte?</p> <p>Remarque : <i>l'utilisation du protocole WEP comme contrôle de sécurité est interdit depuis le 30 juin 2010.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
4.2	(b) Des politiques précisant que les PAN non protégés ne doivent pas être envoyés par des technologies de messagerie pour les utilisateurs finaux sont-elles en place?		<input type="checkbox"/>	<input type="checkbox"/>	

Gestion d'un programme de gestion des vulnérabilités

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

Question PCI DSS		Réponse :	Oui	Non	Spécial*
5.1	Des logiciels antivirus sont-ils déployés sur tous les systèmes régulièrement affectés par des logiciels malveillants?		<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 ces fléaux (par exemple, virus, chevaux de Troie, vers, logiciels espions, logiciels publicitaires et dissimulateurs d'activité)?		<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 registres de vérification comme suit :				
	(a) La politique anti-virus exige-t-elle une mise à jour des définitions et du logiciel anti-virus?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) L'installation principale du logiciel est-elle activée pour des mises à jour et analyses automatiques?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Des mises à jour et des analyses périodiques automatiques sont-elles activées?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Tous les mécanismes anti-virus génèrent-ils des journaux de vérification et les journaux sont-ils conservés conformément à l'exigence 10.7 des normes PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question PCI DSS		Réponse :	Oui	Non	Spécial*
6.1	(a) Tous les logiciels et composants du système sont-ils protégés des vulnérabilités connues en étant dotés des derniers correctifs de sécurité développés par le fournisseur?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les correctifs de sécurité stratégiques sont-ils installés dans le mois qui suit leur commercialisation?		<input type="checkbox"/>	<input type="checkbox"/>	

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 PCI DSS		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, comme suit :			
7.1.1	Les droits d'accès accordés aux ID d'utilisateur privilégiés sont-ils restreints aux privilèges les plus faibles nécessaires pour la réalisation du travail?	<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Les privilèges sont-ils octroyés aux individus sur la base de la classification et de la fonction professionnelles (également nommée « contrôle d'accès basé sur les fonctions » ou RBAC)?	<input type="checkbox"/>	<input type="checkbox"/>	

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

Question PCI DSS		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>(Par exemple, service d'usager commuté à authentification distante (RADIUS) avec jetons; protocole d'authentification TACACS (terminal access controller access control system, système de contrôle d'accès du contrôleur d'accès au terminal) avec jetons; ou autres technologies qui permettent l'authentification à deux facteurs).</i> Remarque : l'authentification à deux facteurs exige que deux des trois méthodes d'authentification (voir l'exigence 8.2 pour des descriptions des méthodes d'authentification) soient utilisées pour l'authentification. L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe séparés) n'est pas considérée comme une authentification à deux facteurs.	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	(a) Les comptes utilisés par les fournisseurs pour l'accès à distance, la maintenance ou l'assistance sont-ils activés uniquement pendant la période nécessaire?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les comptes d'accès à distance des fournisseurs sont-ils surveillés lors de leur utilisation?	<input type="checkbox"/>	<input type="checkbox"/>	

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

Question PCI DSS		Réponse :		
		Oui	Non	Spécial*

Question PCI DSS		Réponse :		Spécial*
		Oui	Non	
9.6	Tous les supports sont-ils physiquement sécurisés (y compris, mais sans s'y limiter, les ordinateurs, les supports électroniques amovibles, les reçus papier, les rapports papier et les télécopies)? <i>Dans le cadre de l'exigence 9, le terme « support » concerne tous les documents papier et les supports électroniques contenant des données de titulaire de carte.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) La distribution interne ou externe de tout type de support est-elle soumise à un contrôle strict?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les contrôles comprennent-ils les procédures suivantes :			
9.7.1	Les supports sont-ils classifiés afin que la confidentialité des données puisse être déterminée?	<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Les supports sont-ils envoyés par coursier ou toute autre méthode d'expédition sécurisée qui peut faire l'objet d'un suivi?	<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Les journaux sont-ils gérés pour suivre tous les supports qui sont déplacés d'une zone sécurisée, et l'approbation de gestion est-elle obtenue avant le déplacement des supports (en particulier lorsque le support est distribué aux individus)?	<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Un contrôle strict est-il assuré concernant le stockage et l'accessibilité des supports?	<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Tous les supports sont-ils éliminés lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou juridiques?	<input type="checkbox"/>	<input type="checkbox"/>	
	La destruction a-t-elle été effectuée comme suit :			
9.10.1	(a) Les documents papier sont-ils déchiquetés, brûlés ou réduits en pâte de manière à ce qu'il soit impossible de les reconstituer?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Les conteneurs utilisés pour le stockage des renseignements à détruire sont-ils sécurisés pour empêcher l'accès aux contenus? (Par exemple, un conteneur de « documents à déchiqueter » possède une serrure empêchant l'accès à son contenu.	<input type="checkbox"/>	<input type="checkbox"/>	

Surveillance et test réguliers des réseaux

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

Question PCI DSS	Réponse :	Oui	No n	Spécial*
11.1 (a) Un processus documenté est-il mis en œuvre pour détecter et identifier les points d'accès sans fil sur une base trimestrielle? Remarque : les méthodes qui peuvent être utilisées dans le processus comprennent, mais sans s'y limiter, les analyses de réseau sans fil, les inspections physiques/logiques des composants du système et des infrastructures, les contrôles d'accès au réseau (NAC), ou les IDS (systèmes de détection d'intrusion) et les IPS (systèmes de prévention d'intrusion) sans fil. Quelles que soient les méthodes utilisées, elles doivent être suffisantes pour détecter et identifier les dispositifs non autorisés.		<input type="checkbox"/>	<input type="checkbox"/>	
(b) La méthodologie détecte-t-elle et identifie-t-elle les points d'accès sans fil non autorisés, y compris au moins les points suivants : <ul style="list-style-type: none"> • des cartes de réseau local sans fil (WLAN) insérées dans des composants du système; • des dispositifs sans fil portables connectés aux composants du système (par exemple, par USB, etc.); • des dispositifs sans fil reliés à un port réseau ou à un dispositif réseau? 		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Le processus pour identifier les points d'accès sans fil non autorisés est-il exécuté au moins tous les trimestres?		<input type="checkbox"/>	<input type="checkbox"/>	
(d) Si une surveillance automatique est utilisée (par exemple, IDS/IPS sans fil, NAC, etc.), la surveillance est-elle configurée pour générer des alertes pour le personnel?		<input type="checkbox"/>	<input type="checkbox"/>	
(e) Le plan de réponse aux incidents (exigence 12.9) comprend-il une réponse dans le cas où des dispositifs sans fil non autorisés sont détectés?		<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 dans le réseau (par exemple, l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits) comme suit : Remarque : il n'est pas exigé que quatre analyses trimestrielles soient réalisées pour une conformité initiale aux normes PCI DSS si 1) le plus récent résultat d'analyse a été une analyse réussie, 2) l'entité a documenté les politiques et procédures exigeant l'analyse trimestrielle, et 3) les vulnérabilités notées ont été corrigées, ce qui sera confirmé par une nouvelle analyse. Lors des années suivant la vérification PCI DSS initiale, quatre analyses trimestrielles doivent être réalisées et réussies.				
11.2.1 (a) Des analyses de vulnérabilité interne trimestrielles sont-elles exécutées?		<input type="checkbox"/>	<input type="checkbox"/>	

Question PCI DSS		Réponse :		<u>O</u> <u>u</u>	<u>N</u> <u>n</u>	<u>Spécial</u> *
	(b) Le processus d'analyse interne trimestriel comprend-il de nouvelles analyses jusqu'à ce que des résultats satisfaisants soient obtenus ou que toutes les vulnérabilités à « haut risque », définies dans l'exigence 6.2 des normes PCI DSS, soient résolues?	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Des analyses trimestrielles internes sont-elles effectuées par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié, et le cas échéant, l'indépendance organisationnelle de la personne qui a effectué le test (il n'est pas exigé d'être un QSA ou un ASV)?	<input type="checkbox"/>	<input type="checkbox"/>			
11.2.2	(a) Des analyses de vulnérabilité externe trimestrielles sont-elles exécutées?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Les résultats des analyses trimestrielles satisfont-ils aux exigences du guide du programme ASV (par exemple, aucune vulnérabilité nominale supérieure à 4.0 selon le CVSS et aucune défaillance automatique)?	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Des analyses des vulnérabilités externes trimestrielles sont-elles effectuées par un prestataire de services d'analyse agréé (ASV) par le PCI SSC (conseil de normes de sécurité du secteur des cartes de paiement)?	<input type="checkbox"/>	<input type="checkbox"/>			
11.2.3	(a) Des analyses externes et internes sont-elles réalisées après des changements significatifs (comme l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits)? <i>Remarque : les analyses réalisées après la modification des réseaux peuvent être effectuées par le personnel interne.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Le processus d'analyse comprend-il de nouvelles analyses jusqu'à ce que : <ul style="list-style-type: none"> • il n'existe aucune vulnérabilité avec un score supérieur à 4.0 selon le CVSS, pour les analyses externes; • un résultat réussi soit obtenu ou que toutes les vulnérabilités à « haut risque » définies dans l'exigence 6.2 des normes PCI DSS, soient résolues, pour les analyses internes? 	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Les analyses sont-elles effectuées par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié, et le cas échéant, l'indépendance organisationnelle de la personne qui a effectué le test est-elle déterminée (il n'est pas exigé d'être un QSA ou un ASV)?	<input type="checkbox"/>	<input type="checkbox"/>			

Gérer une politique de sécurité des renseignements

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

Question PCI DSS		Réponse :	Oui	Non	Spécial*
12.1	Une politique est-elle définie, publiée, gérée et diffusée à tout le personnel compétent? <i>Dans le cadre de l'exigence 12, le terme « personnel » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou qui ont accès à l'environnement des données de titulaire de carte.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	La politique de sécurité des renseignements est-elle révisée au moins une fois par an et mise à jour le cas échéant, pour refléter les changements des objectifs commerciaux ou de l'environnement à risque?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Des politiques d'utilisation des technologies stratégiques (par exemple, technologies d'accès à distance, technologies sans fil, supports électroniques amovibles, ordinateurs portables, assistants numériques personnels (PDA), courriel et utilisation d'Internet) sont-elles développées pour définir l'usage approprié de ces technologies par tous les employés et exigent-elles ce qui suit :				
12.3.1	L'approbation explicite des parties autorisées pour l'utilisation des technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	L'authentification pour l'utilisation des technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	La liste de tous les dispositifs et employés disposant d'un accès?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Les usages acceptables des technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Les emplacements acceptables des technologies sur le réseau?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	La 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	L'activation des technologies d'accès à distance pour les fournisseurs et les partenaires commerciaux uniquement lorsqu'ils en ont besoin, avec une désactivation immédiate après utilisation?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	La politique et les procédures de sécurité définissent-elles clairement les responsabilités de tout le personnel en matière de sécurité des renseignements?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Les responsabilités suivantes de gestion de la sécurité des renseignements sont-elles attribuées à un individu ou à une équipe :				

Question PCI DSS		Réponse :	<u>Oui</u>	<u>Non</u>	<u>Spécial</u> *
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	(a) Un programme formel de sensibilisation à la sécurité est-il mis en place pour sensibiliser tous les employés à l'importance de la sécurité des données de titulaire de carte?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Si les données de titulaire de carte sont partagées avec des prestataires de services, des politiques et procédures sont-elles gérées et mises en œuvre pour la gestion de ces derniers, comme suit :				
12.8.1	Une liste des prestataires de services est-elle tenue?		<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-t-il été signé?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Un processus de sélection des prestataires de services est-il bien défini, comprenant notamment des contrôles préalables à l'engagement?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Un programme est-il mis en place pour contrôler la conformité des prestataires de services aux PCI DSS au moins annuellement?		<input type="checkbox"/>	<input type="checkbox"/>	

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 de renseignements sur chaque exigence PCI DSS, voir *Parcourir les normes PCI DSS*).
3. Aller au-delà des autres exigences PCI DSS (Les contrôles compensatoires ne consistent pas simplement à se trouver en conformité à d'autres exigences PCI DSS).

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

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

- a) Les exigences existantes des normes PCI DSS NE PEUVENT PAS être considérées comme des contrôles compensatoires si elles sont déjà exigées pour l'élément examiné. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être transmis sous forme cryptée afin de limiter les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut utiliser d'autres exigences PCI DSS relatives aux mots de passe (blocage des intrus, mots de passe complexes, etc.) pour compenser l'absence de mots de passe cryptés, puisque celles-ci ne limitent pas les risques d'interception des mots de passe en texte clair. Par ailleurs, les autres contrôles de mots de passe sont déjà exigés par les normes PCI DSS pour l'élément examiné (à savoir les mots de passe).
 - b) Les exigences existantes des normes PCI DSS PEUVENT être considérées comme des contrôles compensatoires si elles sont exigées dans un autre domaine, mais pas pour l'élément faisant l'objet d'une vérification. Par exemple, l'authentification à deux facteurs est exigée par les normes PCI DSS pour l'accès à distance. L'authentification à deux facteurs *depuis le réseau interne* peut aussi être considérée comme un contrôle compensatoire de l'accès administrateur non-console lorsque la transmission des mots de passe cryptés ne peut pas être prise en charge. L'authentification à deux facteurs peut être un contrôle compensatoire acceptable si : (1) elle satisfait l'intention de l'exigence initiale en résolvant les risques d'interception des mots de passe administrateur en texte clair, et (2) elle est correctement configurée et mise en œuvre dans un environnement sécurisé.
 - c) Les exigences existantes des normes PCI DSS peuvent être associées à de nouveaux contrôles et constituer alors un contrôle compensatoire. Par exemple, si une société n'est pas en mesure de rendre les données de titulaire de carte illisibles conformément à l'exigence 3.4 (par exemple, par cryptage), un contrôle compensatoire pourrait consister en un dispositif ou un ensemble de dispositifs, d'applications et de contrôles qui assurent : (1) la segmentation du réseau interne; (2) le filtrage des adresses IP ou MAC; et (3) l'authentification à deux facteurs à partir du réseau interne.
4. Être proportionnel aux risques supplémentaires qu'implique le non-respect de l'exigence PCI DSS.

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

Annexe C : Fiche de contrôles compensatoires

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

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

Numéro et définition des exigences :

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

Fiche de contrôles compensatoires – Exemple complété

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

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

	Renseignements requis	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité avec l'exigence initiale.	<i>La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « racine ». La société XYZ ne peut pas gérer le nom d'utilisateur « racine » ni consigner toutes les activités de chaque utilisateur « racine ».</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 renseignements d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière.</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 renseignements 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 « racine » et à exécuter des actions sous ce compte, tout en permettant de consigner leurs activités dans le répertoire du journal SU. Il est ainsi possible de suivre les actions de chaque utilisateur par le biais du compte SU.</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 « racine ».</i>
6. Maintenance	Définir les processus et les contrôles en place pour la maintenance 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 racines sans que leurs activités soient consignées ou suivies.</i>

