L'approche prioritaire pour assurer la conformité à la norme PCI DSS

La norme de sécurité des données du secteur des cartes de paiement (PCI DSS) fournit une structure détaillée de 12 exigences pour sécuriser les données des titulaires de cartes qui sont stockées, traitées et/ou transmises aux commerçants et autres organisations. De par sa nature exhaustive, la norme fournit une grande quantité d'informations sur la sécurité ; tellement en fait que certaines personnes responsables de la sécurité des données de titulaires de cartes se demandent où démarrer le processus continu vers la conformité. À cette fin, le Conseil des normes de sécurité PCI fournit l'approche prioritaire suivante pour aider les parties prenantes à comprendre où elles peuvent agir pour réduire le risque plus tôt dans le processus de conformité. Aucune étape seule dans l'approche prioritaire ne fournira une sécurité complète ni ne garantira la conformité à la norme PCI DSS, mais suivre ses directives aidera les parties prenantes à accélérer le processus de sécurisation des données des titulaires de cartes.

POINTS SAILLANTS

Aide les commerçants à identifier les cibles ayant le risque de sécurité le plus élevé

Crée un langage commun autour de la mise en œuvre de la norme PCI DSS et des efforts d'évaluation

Les étapes importantes permettent aux commerçants de démontrer la progression du processus de conformité

Qu'est-ce que l'approche prioritaire ?

L'approche prioritaire fournit six étapes de sécurité qui aideront les commerçants et d'autres organisations à se protéger de manière incrémentielle contre les plus gros facteurs de risque et les menaces grandissantes pendant qu'ils progressent sur le chemin de la conformité PCI DSS. L'approche prioritaire et ses étapes importantes (décrites en page 2) sont prévues pour obtenir les avantages suivants :

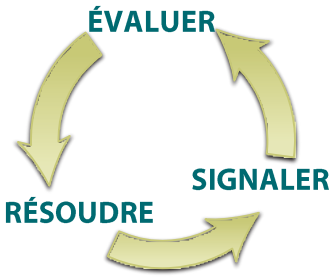
- Feuille de route qu'une organisation peut utiliser pour répondre aux risques par ordre de priorité
- Approche pragmatique permettant des « succès rapides »
- Prend en charge la planification financière et opérationnelle
- Promeut des indicateurs de progression objectifs et mesurables
- Favorise la cohérence parmi les évaluateurs

Mai 2016

Objectifs de l'approche prioritaire ?

L'approche prioritaire fournit une feuille de route pour les activités de conformité basées sur le risque lié au stockage, traitement et/ou transmission des données de titulaires de carte. La feuille de route aide à établir la priorité des efforts pour réaliser la conformité, établir des étapes importantes, réduire le risque de violation des données des titulaires de carte plus tôt dans le processus de conformité, mais aussi aider les acquéreurs à mesurer de manière objective les activités de conformité et de réduction du risque pour les commerçants, les prestataires de services et autres. L'approche prioritaire a été établie après avoir factorisé les données de violations réelles et pris en compte le feedback d'évaluateurs de sécurité qualifiés, d'enquêteurs judiciaires et de membres du Comité de direction du Conseil des normes de sécurité PCI. Elle n'est pas conçue en tant que substitut, raccourci ou mesure d'urgence vers la conformité à la norme PCI DSS, ni en tant que cadre universel obligatoire applicable par chaque entreprise. L'approche prioritaire est adéquate pour les commerçants qui sont soumis une évaluation sur site ou utilisent le questionnaire SAQ D.

LA CONFORMITÉ À LA NORME PCI DSS EST UN PROCESSUS CONTINU



FONDATEURS DE PCI SSC

ORGANISATIONS PARTICIPANTES

Commerçants, banques, opérateurs, développeurs et points de vente

STIPULATION D'EXONÉRATION

Pour arriver à être en conformité avec la norme PCI DSS, une organisation doit parvenir à respecter TOUTES les exigences applicables de la norme PCI DSS, quel que soit l'ordre dans lequel elle y parvient, et que l'organisation suive l'approche prioritaire pour la norme PCI DSS ou non. Ce document ne modifie et n'abrège ni la norme PCI DSS ni aucune de ses exigences, et il est susceptible de changement sans préavis.

Le PCI SSC ne peut être tenu responsable des erreurs ou dommages de toute sorte résultant de l'utilisation des informations contenues dans le présent document. Le PCI SSC n'offre aucune garantie et ne fait aucune déclaration concernant les informations fournies dans les présentes, et le PCI SSC n'assume aucune responsabilité concernant l'utilisation ou la mauvaise utilisation de ces informations.

Étapes importantes pour la priorité des efforts de conformité à la norme PCI DSS

L'approche prioritaire inclut six étapes importantes. La matrice ci-dessous récapitule les objectifs et intentions de haut niveau pour chaque étape. Le reste de ce document trace les étapes importantes pour chacune des 12 conditions de la norme PCI DSS et leurs sous-conditions.

Étape	Objectifs
1	**Supprimer les données d'identification sensibles et limiter la conservation des données.** Cette étape cible une zone de risque clé pour les entités ayant subi un incident de sécurité. N'oubliez pas : si les données d'identification sensibles et les autres données du titulaire ne sont pas stockées, les effets d'un incident de sécurité seront grandement réduits. Il est inutile de stocker ce dont on n'a pas besoin !
2	**Protéger les systèmes et les réseaux, et être prêt à répondre à chaque intrusion dans le système.** Cette étape vise le contrôle des points d'accès à la plupart des incidents de sécurité, ainsi que les processus pour y répondre.
3	**Sécuriser les applications de carte de paiement.** Cette étape vise le contrôle des applications, des processus d'application, et des serveurs d'application. Toute faiblesse dans l'un de ces secteurs peut faire des systèmes une proie facile pour les incidents de sécurité, et faciliter l'obtention de données de titulaire.
4	**Surveiller et contrôler l'accès à vos systèmes.** Les contrôles de cette étape vous permettent de savoir le qui, le quoi, le quand et le comment des individus qui accèdent à votre réseau et à votre environnement de données du titulaire.
5	**Protéger les données des titulaires de cartes stockées.** Pour les organisations ayant analysé leurs processus d'entreprise et déterminé qu'elles devaient stocker des numéros de compte principaux, l'étape cinq vise les mécanismes de protection clés pour le stockage de ces données.
6	**Finaliser les derniers efforts de conformité et s'assurer que tous les contrôles sont en place.** L'objectif de l'étape six est de compléter les exigences du PCI DSS est de finaliser tous les processus, politiques et procédures lié(e)s restant(e)s nécessaires pour protéger l'environnement des données de titulaire.

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données du titulaire						
1.1 Établir et mettre en œuvre des normes de configuration des pare-feu et des routeurs comprenant les éléments suivants :						
1.1.1 Processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs						6
1.1.2 Diagramme du réseau actuel qui identifie toutes les connexions entre l'environnement de données de titulaires de carte et les autres réseaux, y compris tout réseau sans fil	1					
1.1.3 Diagramme actuel montrant le flux des données de titulaires de carte dans les systèmes et les réseaux	1					
1.1.4 Conditions relatives au pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne		2				
1.1.5 Description des groupes, des rôles et des responsabilités pour la gestion des composants du réseau						6
1.1.6 Documentation de la justification professionnelle et approbation de l'utilisation de tous les services, protocoles et ports autorisés, y compris la documentation des fonctions de sécurité mises en œuvre pour les protocoles considérés comme étant non sécurisés.		2				
1.1.7 Exigence d'analyse des règles concernant les pare-feu et les routeurs au moins tous les six mois						6
1.2 Créer des configurations de pare-feu et de routeur qui limitent les connexions entre les réseaux non approuvés et tous les composants de système dans l'environnement des données de titulaires de carte. *Remarque : Un « réseau non approuvé » est tout réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.*						
1.2.1 Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données de titulaires de carte et, particulièrement, refuser tout autre trafic.		2				
1.2.2 Sécuriser et synchroniser les fichiers de configuration des routeurs.		2				
1.2.3 Installer des pare-feu de périmètre entre tous les réseaux sans fil et l'environnement des données de titulaires de carte, et configurer ces pare-feu pour refuser ou, s'il est nécessaire à des fins professionnelles, autoriser uniquement le trafic entre l'environnement sans fil et l'environnement de données de titulaires de carte.		2				
1.3 Interdire l'accès public direct entre Internet et tout composant du système dans l'environnement des données des titulaires de cartes.						
1.3.1 Déployer une DMZ pour limiter le trafic entrant aux seuls composants de système fournissant des services, protocoles et ports autorisés, accessibles au public.		2				
1.3.2 Limiter le trafic Internet entrant aux adresses IP dans la DMZ.		2				
1.3.3 Mise en œuvre des mesures anti-usurpation pour détecter et pour empêcher les adresses IP de source frauduleuse de pénétrer sur le réseau. (Par exemple, bloquer le trafic originaire d'Internet avec une adresse de source interne).		2				

1.3.4 Ne pas autoriser le trafic sortant non autorisé de l'environnement des données de titulaires de carte vers Internet.	**2**	
1.3.5 Les connexions « établies » sont les seules autorisées sur le réseau.	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
1.3.6 Placer les composants de système qui stockent les données de titulaires de carte (comme une base de données) dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés.		**2**				
1.3.7 Ne pas divulguer les adresses IP et les informations d'acheminement confidentielles à des parties non autorisées. *Remarque : Quelques-unes des méthodes permettant de dissimuler les adresses IP sont présentées ci-après :* • *Traduction d'adresse réseau (Network Address Translation, NAT) ;* • *Protéger les serveurs contenant des données de titulaires de carte derrière des serveurs proxy/pare-feu ;* • *Retrait ou filtrage des annonces d'acheminement pour les réseaux privés employant des adresses enregistrées ;* • *Utilisation interne de l'espace d'adresse RFC1918 au lieu d'adresses enregistrées.*		**2**				
1.4 Installer un logiciel de pare-feu personnel ou une fonctionnalité équivalente sur tout appareil informatique portable (y compris les appareils appartenant à la société et/ou à l'employé) qui se connecte à Internet en dehors du réseau (par exemple, les ordinateurs portables utilisés par les employés) et qui permet également un accès au CDE. Les configurations de pare-feu (ou fonctionnalité équivalente) comprennent ce qui suit : • Des réglages de configuration spécifiques sont définis. • Un pare-feu personnel (ou fonctionnalité équivalente) fonctionne activement. • Le pare-feu personnel (ou fonctionnalité équivalente) ne peut pas être altéré par les utilisateurs des appareils informatiques portables.		**2**				
1.5 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des pare-feu sont documentées, utilisées et connues de toutes les parties concernées.		**2**				
Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur						
2.1 Changer systématiquement les paramètres par défaut définis par le fournisseur ou désactiver les comptes par défaut inutiles avant d'installer un système sur le réseau. Cette pratique s'applique à TOUS les mots de passe par défaut, y compris mais sans s'y limiter, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, les comptes d'application et de système, les terminaux de point de vente (POS), les applications de paiement, les chaînes de communauté de protocoles de gestion de réseau simple [SNMP], etc.		**2**				
2.1.1 Pour les environnements sans fil connectés à l'environnement des données de titulaires de carte ou qui transmettent des données de titulaires de carte, changer TOUS les paramètres par défaut définis par le fournisseur à l'installation, notamment les clés de cryptage sans fil, les mots de passe et les chaînes de communauté SNMP.		**2**				

2.2 Élaborer des normes de configuration pour tous les composants de système. S'assurer que ces normes couvrent toutes les vulnérabilités de la sécurité et sont compatibles avec toutes les normes renforçant les systèmes en vigueur dans le secteur. Les sources des normes renforçant les systèmes en vigueur dans le secteur, comprennent, sans s'y limiter, les organismes suivants : • Center for Internet Security (CIS – Centre de sécurité Internet) • International Organization for Standardization (ISO – Organisation des normes internationales) • SysAdmin Audit Network Security (SANS) Institute (Institut SANS) • National Institute of Standards Technology (NIST – Institut national des standards et de la technologie).	**3**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
2.2.1 N'appliquer qu'une fonction principale par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents. (Par exemple, les serveurs Web, les serveurs de bases de données et les serveurs DNS doivent être déployés sur des serveurs distincts). *Remarque : Lorsque des technologies de virtualisation sont utilisées, n'appliquer qu'une fonction primaire par composant de système virtuel.*			3			
2.2.2 Activer uniquement les services, protocoles, démons, etc., nécessaires pour le fonctionnement du système.			3			
2.2.3 Implémenter les fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaire et jugé comme non sécurisé. *Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial.*		2				
2.2.4 Configurer les paramètres de sécurité du système pour empêcher les actes malveillants.			3			
2.2.5 Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus.			3			
2.3 Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste. *Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial.*		2				
2.4 Maintenir un inventaire des composants de système qui se trouvent dans le champ d'application de la norme PCI DSS.		2				
2.5 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres par défaut du fournisseur et des autres paramètres de sécurité sont documentés, utilisés et connus de toutes les parties concernées.		2				
2.6 Les fournisseurs d'hébergement partagé doivent protéger l'environnement hébergé et les données de titulaires de carte de chaque entité. Ces fournisseurs doivent satisfaire aux conditions spécifiques décrites dans l'Annexe A1 : Autres clauses de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.			3			
Condition 3 : Protéger les données de titulaires de carte						
3.1 Garder le stockage de données de titulaires de carte à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données, qui comprennent au moins les mesures suivantes pour le stockage des données de titulaires de carte (CHD) : • Limiter la quantité des données stockées et les délais de conservation selon les conditions requises par les conditions légales, réglementaires et/ou commerciales ; • Des conditions de conservation spécifiques pour les données de titulaires de carte ; • Des processus pour la suppression sécurisée des données devenues inutiles ; • Un processus trimestriel pour l'identification et la suppression sécurisée des données de titulaires de carte stockées excédant les conditions de conservation définies.	1					

3.2 Ne stocker aucune donnée d'identification sensible après autorisation (même cryptée). Si des données d'identification sensibles sont reçues, rendre toutes les données irrécupérables à la fin du processus d'autorisation. Il est permis aux émetteurs et aux sociétés qui prennent en charge les services d'émissions de stocker des données d'identification sensibles si : • Une justification commerciale existe et • Les données sont stockées de manière sécurisée. Les données d'identification sensibles sont mentionnées dans les conditions 3.2.1 à 3.2.3 suivantes :	**1**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
3.2.1 Ne pas stocker la totalité du contenu d'une quelconque piste (sur la bande magnétique au verso d'une carte, sur une puce ou ailleurs) après l'autorisation. Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique. Remarque : Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique suivants : • le nom du titulaire de la carte ; • Le numéro de compte primaire (PAN) ; • La date d'expiration ; • Le code de service Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.	1					
3.2.2 Ne pas stocker le code ou la valeur de vérification de carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement, utilisé pour vérifier les transactions carte absente) après l'autorisation.	1					
3.2.3 Ne pas stocker de code d'identification personnelle (PIN) ou de bloc PIN crypté après l'autorisation.	1					
3.3 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel, dont le besoin commercial est légitime, puisse voir plus que les six premiers/les quatre derniers chiffres du PAN. *Remarque : Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données de titulaires de carte, par exemple, pour les reçus des points de vente (POS).*					5	
3.4 Rendre le PAN illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes : • Hachage unilatéral s'appuyant sur une méthode cryptographique robuste (la totalité du PAN doit être hachée) ; • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ; • Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ; • Cryptographie robuste associée aux processus et procédures de gestion des clés. *Remarque : Il s'agit d'un effort relativement peu important pour un individu malveillant de reconstruire les données du PAN d'origine, s'il a à la fois accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachées et tronquées du même PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être en place pour garantir que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.*					5	
3.4.1 Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès logique doit être géré séparément et indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales, ou des justificatifs génériques de connexion au réseau). Les clés de décryptage ne doivent pas être associées à des comptes d'utilisateur. *Remarque : En outre, cette condition s'applique à toutes les autres conditions de gestion des clés et de cryptage PCI DSS.*					5	

3.5 Documenter et mettre en œuvre des procédures pour protéger les clés utilisées pour sécuriser les données de titulaires de carte stockées contre la divulgation et l'utilisation illicites : *Remarque : Cette condition s'applique également aux clés utilisées pour crypter les données de titulaires de carte stockées et elle s'applique aux clés de cryptage de clé utilisées pour protéger les clés de cryptage de données – ces clés de cryptage de clés doivent être au moins aussi robustes que la clé de cryptage de données.*	

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
3.5.1 Condition supplémentaire pour les prestataires de services uniquement : Conserver une description documentée de l'architecture cryptographique qui comprend ce qui suit : • Détails de tous les algorithmes, protocoles et clés utilisés pour protéger les données de titulaires de carte, y compris la robustesse des clés et la date d'expiration • Description de l'utilisation de chaque clé • Inventaire des HSM et autres SCD dans le cadre de la gestion des clés *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*					5	
3.5.2 Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible.					5	
3.5.3 Stocker les clés secrètes et privées utilisées pour crypter/décrypter les données de titulaires de carte sous l'une (ou sous plusieurs) des formes suivantes à tout moment : • Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stockée séparément de la clé de cryptage de données. • Dans un périphérique cryptographique sécurisé (comme un module de sécurité matériel (hôte) ou un dispositif de point d'interaction approuvé PTS) • En tant que deux composants de clé ou partages de clé de pleine longueur au moins, conformément à la méthode acceptée par l'industrie *Remarque : Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes.*					5	
3.5.4 Stocker les clés cryptographiques dans aussi peu d'emplacements que possible.					5	
3.6 Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données des titulaires de cartes, notamment ce qui suit : *Remarque : De nombreuses normes du secteur pour la gestion des clés sont disponibles auprès de diverses ressources, notamment NIST, que vous trouverez à l'adresse suivante : http://csrc.nist.gov.*						
3.6.1 Génération de clés cryptographiques robustes					5	
3.6.2 Sécuriser la distribution des clés cryptographiques					5	
3.6.3 Sécuriser le stockage des clés cryptographiques					5	
3.6.4 Changements de clé cryptographique pour les clés ayant atteint la fin de leur cryptopériode (par exemple, après la fin d'une période définie et/ou après la production d'une certaine quantité de cryptogrammes par une clé donnée), comme l'a défini le fournisseur de l'application associée ou le propriétaire de la clé, et selon les meilleures pratiques et directives du secteur (par exemple, la publication spéciale NIST 800-57).					5	

	3.6.5 Retrait ou remplacement des clés (par exemple, en les archivant, détruisant, et/ou en les révoquant), si nécessaire lorsque le degré d'intégrité d'une clé est affaibli (par exemple, départ d'un employé ayant connaissance du texte clair d'une clé) ou lorsque des clés sont susceptibles d'avoir été compromises. Remarque : Si les clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, en utilisant une clé de cryptage de clé). Les clés cryptographiques archivées doivent être utilisées uniquement pour un décryptage ou une vérification.	**5**

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
3.6.6 Si des opérations de gestion manuelle de clés cryptographiques en texte clair sont utilisées, elles doivent être gérées par le fractionnement des connaissances et un double contrôle. Remarque : La génération, la transmission, le chargement, le stockage et la destruction de clés sont quelques-uns des exemples d'interventions de gestion manuelle des clés.					5	
3.6.7 Prévention de la substitution non autorisée des clés cryptographiques.					5	
3.6.8 Condition selon laquelle les opérateurs chargés de la gestion de clés cryptographiques reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités en tant que telles.					5	
3.7 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.					5	
Condition 4 : Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts						
4.1 Utiliser une cryptographie robuste et des protocoles de sécurité afin de protéger les données de titulaires de carte sensibles lors de leur transmission sur des réseaux publics ouverts, y compris : • Seuls des clés et certificats approuvés sont acceptés. • Le protocole utilisé prend uniquement en charge les versions ou configurations sécurisées. • La force du cryptage est appropriée pour la méthodologie de cryptage employée. *Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial. Voici quelques exemples, parmi d'autres, de réseaux publics ouverts :* • *Internet,* • *Technologies sans fil, y compris 802.11 et Bluetooth* • *Les technologies cellulaires, par exemple, Système global pour les communications mobiles (GSM), Accès multiple de division de code (CDMA)* • *GPRS (General Packet Radio Service).* • *Communications par satellite.*		2				
4.1.1 S'assurer que les réseaux sans fil, sur lesquels sont transmises les données de titulaires de carte ou qui sont connectés à l'environnement des données de titulaires de carte, utilisent les meilleures pratiques du secteur pour appliquer un cryptage robuste pour l'authentification et la transmission.		2				
4.2 Ne jamais envoyer de PAN non protégés à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple e-mail, messagerie instantanée, SMS, chat, etc.).		2				
4.3 S'assurer que les politiques de sécurité et les procédures opérationnelles pour le cryptage des données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.		2				
Condition 5 : Utiliser des logiciels ou des logiciels antivirus et les mettre à jour régulièrement						
5.1 Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).		2				

5.1.1 S'assurer que tous les programmes anti-virus sont capables de détecter et d'éliminer tous les types de logiciel malveillant connus, et d'assurer une protection efficace.	**2**	
5.1.2 Pour les systèmes considérés comme n'étant pas affectés par les logiciels malveillants, effectuer des évaluations régulières pour identifier et évaluer l'évolution de la menace posée par les logiciels malveillants afin de confirmer que ces	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
5.2 S'assurer que tous les mécanismes antivirus sont maintenus comme suit : • Maintenus à jour • Effectuent régulièrement des scans • Génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS.		**2**				
5.3 S'assurer que les mécanismes anti-virus fonctionnement de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps. *Remarque : Les solutions anti-virus peuvent être désactivées temporairement uniquement s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la protection anti-virus doit être désactivée dans un but spécifique, cette désactivation doit donner lieu à une autorisation formelle. Des mesures de sécurité supplémentaires doivent également être mises en œuvre pour la période de temps pendant laquelle la protection anti-virus n'est pas active.*		**2**				
5.4 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la protection contre les logiciels malveillants sont documentées, utilisées et connues de toutes les parties concernées.		**2**				
Condition 6 : Développer et maintenir des systèmes et des applications sécurisés						
6.1 Établir un processus pour identifier les vulnérabilités de la sécurité, en utilisant des sources externes de bonne réputation pour la sécurité des informations concernant la vulnérabilité et affecter un classement du risque (par exemple « élevé », « moyen » ou « faible ») aux vulnérabilités de sécurité nouvellement découvertes. *Remarque : Le classement des risques doit se baser sur les meilleures pratiques du secteur, ainsi que sur la prise en compte de l'impact potentiel. Par exemple, les critères de classement des vulnérabilités peuvent inclure la prise en compte du score de base CVSS et/ou la classification par le fournisseur et/ou le type de système affecté.* *Les méthodes d'évaluation de vulnérabilité et d'affectation des classements de risque varieront selon l'environnement de l'organisation et la stratégie d'évaluation des risques. Le classement de risque doit, au minimum, identifier toutes les vulnérabilités considérées comme posant un « risque élevé » pour l'environnement. En plus du classement de risque, les vulnérabilités peuvent être considérées comme « critiques » si elles constituent une menace imminente pour l'environnement, ont un impact critique sur les systèmes et/ou si elles sont susceptibles de compromettre l'application si elles ne sont pas résolues. Les exemples de systèmes critiques peuvent inclure les systèmes de sécurité, les dispositifs et systèmes ouverts au public, les bases de données et autres systèmes qui stockent, traitent ou transmettent des données de titulaires de carte.*			**3**			
6.2 S'assurer que tous les logiciels et les composants de système sont protégés de vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation. *Remarque : Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.*			**3**			

6.3 Développer des applications logicielles internes et externes (y compris l'accès administratif aux applications par le Web) conformément aux points suivants : • Conformément à la norme PCI DSS (par exemple, authentification et connexion sécurisées) • Basés sur les normes/meilleures pratiques du secteur. • Incorporer la sécurité des informations au cours du cycle de vie de la conception d'un logiciel. *Remarque : ce point s'applique à tous les logiciels développés à l'interne, ainsi qu'aux logiciels sur mesure ou personnalisés qui sont développés par un tiers.*	**3**	
6.3.1 Supprimer les comptes de développement, de test et/ou les comptes d'application personnalisés, les ID d'utilisateur et des mots de passe avant l'activation des applications ou leur mise à la disposition des clients.	**3**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
6.3.2 Examiner le code d'application personnalisé avant la mise en production ou la mise à la disposition des clients afin d'identifier toute vulnérabilité de codage éventuelle (à l'aide de processus manuels ou automatiques) pour inclure au moins les points suivants : • Les modifications de code sont examinées par des individus autres que l'auteur initial du code et par des individus compétents en la matière de techniques d'analyse de code et de pratiques de codage sécurisées. • Les examens de code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé • Les corrections appropriées sont implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. *Remarque : Cette condition s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de conception du système. Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers. Les applications Web destinées au public font également l'objet de contrôles supplémentaires afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par la condition 6.6 de la norme PCI DSS.*			**3**			
6.4 Suivre les processus et procédures de contrôle des changements pour toutes les modifications apportées à des composants de système. Ces processus doivent inclure les points suivants :			**3**			
6.4.1 Séparer les environnements de test/développement des environnements de production et appliquer la séparation à l'aide de contrôles d'accès.			**3**			
6.4.2 Séparation des obligations entre les environnements de développement/test et de production.			**3**			
6.4.3 Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.			**3**			
6.4.4 Suppression des données et comptes de tests dans les composants de système avant que le système ne devienne actif/passe en phase de production.			**3**			
6.4.5 Les procédures de contrôle de changement doivent inclure ce qui suit :						**6**
6.4.5.1 Documentation de l'impact.						**6**
6.4.5.2 Documentation du changement approuvée par les parties autorisées.						**6**
6.4.5.3 Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système.						**6**
6.4.5.4 Procédures de suppression.						**6**
6.4.6 Suite à un changement important, toutes les conditions pertinentes PCI DSS doivent être mises en œuvre sur tous les systèmes et réseaux, qu'ils soient nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant. *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*						**6**

6.5 Adresser les vulnérabilités de code les plus fréquentes dans les processus de développement de logiciel, afin d'inclure les éléments suivants : • Former les développeurs au moins une fois par an pour perfectionner leurs techniques de codage sécurisé, afin qu'ils sachent notamment comment éviter les vulnérabilités de codage courantes. • Développer des applications basées sur les directives de codage sécurisé. *Remarque : Les vulnérabilités décrites aux points 6.5.1 à 6.5.10 faisaient partie des meilleures pratiques du secteur au moment de la publication de cette version de la norme PCI DSS. Cependant, comme les meilleures pratiques de gestion de la vulnérabilité du secteur sont actualisées (par exemple, le guide OWASP, le Top 25 SANS CWE, le codage sécurisé CERT, etc.), se reporter aux meilleures pratiques actuelles pour ces conditions.*	**3**	
Remarque : Les conditions 6.5.1 à 6.5.6, ci-dessous, s'appliquent à toutes les applications (internes ou externes).		

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
6.5.1 Attaques par injection, notamment les injections de commandes SQL. Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.			3			
6.5.2 Saturation de la mémoire tampon			3			
6.5.3 Stockage cryptographique non sécurisé			3			
6.5.4 Communications non sécurisées			3			
6.5.5 Traitement inapproprié des erreurs			3			
6.5.6 Toutes les vulnérabilités à « haut risque », identifiées dans le processus d'identification de vulnérabilité (selon la condition 6.1 de la norme PCI DSS).			3			
Remarque : Les conditions 6.5.7 à 6.5.10, ci-dessous, s'appliquent aux applications Web et aux interfaces d'application (internes ou externes) :						
6.5.7 Attaques Cross-Site Scripting (XSS)			3			
6.5.8 Contrôle d'accès inapproprié (comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, le survol de répertoire et la non-restriction de l'accès utilisateur aux fonctions).			3			
6.5.9 Attaques CSRF (Cross-site request forgery)			3			
6.5.10 Rupture dans la gestion des authentifications et des sessions			3			
6.6 Pour les applications Web destinées au public, traiter les nouvelles menaces et vulnérabilités de manière continue et veiller à ce que ces applications soient protégées contre les attaques connues à l'aide de l'une des méthodes suivantes : • Examen des applications Web destinées au public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuelles, au moins une fois par an et après toute modification. *Remarque : Cette évaluation est différente des scans de vulnérabilité effectués pour la condition 11.2.* • Installer une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) devant les applications web destinées au public pour vérifier continuellement tout le trafic.			3			
6.7 S'assurer que les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de la sécurité des systèmes et applications sont documentées, utilisées et connues de toutes les parties concernées.			3			
Condition 7 : Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître						
7.1 Restreindre l'accès aux composants du système et aux données des titulaires de cartes aux seuls individus qui doivent y accéder pour mener à bien leur travail.						
7.1.1 Définir les besoins d'accès pour chaque rôle, y compris : • Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste ; • Le niveau de privilège requis (par exemple utilisateur, administrateur, etc.) pour accéder aux ressources.				4		
7.1.2 Restreindre l'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail				4		

7.1.3 Affecter l'accès basé sur la classification et la fonction professionnelles de chaque employé.	4	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
7.1.4 Demander l'approbation documentée des parties responsables spécifiant les privilèges requis.				4		
7.2 Établir des systèmes de contrôle d'accès pour les composants de système qui limitent l'accès aux seuls utilisateurs qui doivent accéder aux données et qui est configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés. Ces systèmes de contrôle d'accès doivent inclure les éléments suivants :						
7.2.1 Couverture de tous les composants de système				4		
7.2.2 L'octroi de privilèges aux individus repose sur leur classification et leur fonction				4		
7.2.3 Configuration par défaut du paramètre « Refuser tout ».				4		
7.3 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.				4		
Condition 8 : Affecter un ID unique à chaque utilisateur d'ordinateur						
8.1 Définir et mettre en œuvre des politiques et des procédures pour assurer la gestion appropriée de l'identification des utilisateurs pour les utilisateurs non consommateurs et pour les administrateurs sur tous les composants de système comme suit :						
8.1.1 Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants de système ou aux données de titulaires de carte.		2				
8.1.2 Contrôler l'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiants.		2				
8.1.3 Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société.		2				
8.1.4 Supprimer/Désactiver les comptes d'utilisateur inactifs dans un délai de 90 jours.		2				
8.1.5 Gérer les ID utilisés par les parties tierces pour accéder, prendre en charge ou maintenir les composants de système par accès à distance comme suit : • Activés uniquement pendant la période de temps nécessaire et désactivés lorsqu'ils ne sont pas utilisés. • Surveillés lorsqu'ils sont utilisés.		2				
8.1.6 Limiter les tentatives d'accès répétées en verrouillant l'ID d'utilisateur après six tentatives au maximum.		2				
8.1.7 Régler la durée de verrouillage sur 30 minutes au minimum ou jusqu'à ce que l'administrateur active l'ID d'utilisateur.		2				
8.1.8 Si une session reste inactive pendant plus de 15 minutes, demander à l'utilisateur de s'authentifier de nouveau pour réactiver le terminal ou la session.		2				
8.2 En plus de l'affectation d'un ID unique, s'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants de système en employant au moins une des méthodes suivantes pour identifier tous les utilisateurs : • Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; • Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; • Quelque chose que vous détenez, comme une mesure biométrique.		2				

8.2.1 Utiliser une cryptographie robuste, rendre tous les justificatifs d'authentification (tels que les mots/phrases de passe) illisibles pendant la transmission et le stockage sur tous les composants de système.	**2**	
8.2.2 Vérifier l'identité de l'utilisateur avant de modifier tout justificatif d'authentification, par exemple, lors des réinitialisations de mot de passe, la délivrance de nouveaux jetons ou la création de nouvelles clés.	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
8.2.3 Les mots de passe/locutions de passage doivent respecter les critères suivants : • Exiger une longueur minimale d'au moins sept caractères ; • Comporter à la fois des caractères numériques et des caractères alphabétiques. Autrement, les mots de passe/locutions de passage doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.		2				
8.2.4 Modifier les mots de passe/locutions de passage utilisateur au moins tous les 90 jours.		2				
8.2.5 Interdire à un individu de soumettre un nouveau mot de passe/locution de passage identique à l'un de quatre derniers mots de passe/locutions de passage utilisés.		2				
8.2.6 Définir des mots de passe/locutions de passage pour la première utilisation et suite à la réinitialisation pour une valeur unique pour chaque utilisateur et changer immédiatement après la première utilisation.		2				
8.3 Sécuriser tous les accès administratifs non-console et tous les accès distants au CDE par authentification à plusieurs facteurs. *Remarque : L'authentification à plusieurs facteurs requiert d'utiliser au moins deux des trois méthodes d'authentification (voir la condition 8.2 pour les descriptions des méthodes d'authentification). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à plusieurs facteurs.*						
8.3.1 Incorporer l'authentification à plusieurs facteurs pour tous les accès non-console dans CDE pour les membres du personnel dotés d'un accès administratif. *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*		2				
8.3.2 Incorporer une authentification à plusieurs facteurs pour tous les accès réseau à distance (utilisateur et administrateur, y compris l'accès des parties tierces dans un souci d'assistance ou de maintenance) provenant de l'extérieur du réseau de l'entité.		2				
8.4 Documenter et communiquer les politiques et les procédures d'authentification à tous les utilisateurs, y compris : • Des directives concernant la sélection de justificatifs d'authentification robustes ; • Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ; • Des instructions stipulant qu'il ne faut pas réutiliser les mots de passe ayant déjà été utilisés ; • Des instructions expliquant comment changer les mots de passe si l'on				4		
8.5 Ne pas utiliser de méthode d'authentification par groupe, partagé ou de mots de passe d'ID génériques comme suit : • Les ID d'utilisateur génériques sont désactivés ou supprimés. • Les ID d'utilisateur partagés n'existent pas pour les fonctions d'administration du système et les autres fonctions critiques. • Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration du moindre composant du système.				4		

8.5.1 Condition supplémentaire pour les prestataires de services uniquement : Les prestataires de services ayant un accès à distance aux installations des clients (par exemple, pour l'assistance des systèmes ou des serveurs de POS) doivent utiliser un justificatif d'authentification unique (tel qu'un mot/phrase de passe) pour chaque client. *Remarque : Cette condition n'est pas prévue pour s'appliquer aux fournisseurs*	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
8.6 Lorsque les autres mécanismes d'authentification sont utilisés (par exemple, des jetons de sécurité logiques ou physiques, des cartes électroniques, certificats, etc.) l'utilisation de ces mécanismes doit être assignée comme suit : • Les mécanismes d'authentification doivent être affectés à un compte individuel et non pas partagés par de multiples comptes. • Les contrôles logiques et/ou physiques doivent être en place pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès.				4		
8.7 Tous les accès à n'importe quelle base de données contenant des données de titulaires de carte (y compris les accès par les applications, administrateurs et autres utilisateurs) sont restreints comme suit : • Tous les accès d'utilisateur, demandes d'utilisateur et actions d'utilisateur sur les bases de données ont lieu au moyen de méthodes de programmation. • Seuls les administrateurs de bases de données ont la possibilité d'accéder directement aux bases de données ou d'effectuer des demandes sur les bases de données. • Les ID d'application pour les applications de base de données peuvent uniquement être utilisés par les applications (et non par des utilisateurs individuels ou d'autres processus).				4		
8.8 S'assurer que les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont documentées, utilisées et connues de toutes les parties concernées.				4		
Condition 9 : Restreindre l'accès physique aux données de titulaires de carte						
9.1 Utiliser des contrôles d'accès aux installations appropriés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de carte.		2				
9.1.1 Installer des caméras vidéo ou des mécanismes de contrôle d'accès pour contrôler l'accès physique des individus aux zones sensibles. Examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi. *Remarque : Par « zones sensibles », nous entendons tout centre de données, salle de serveur ou zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaires de carte. Cette définition exclut les zones face au public où seuls les terminaux de point de vente sont présents, tels que les zones de caisse dans un magasin.*		2				
9.1.2 Mettre en œuvre des contrôles physiques et/ou logiques pour restreindre l'accès physique aux prises réseau accessibles au public. Par exemple, les prises de réseau situées dans les zones publiques et les zones accessibles aux visiteurs doivent être désactivées et uniquement activées lorsque l'accès au réseau est accepté de manière explicite. Autrement, des processus doivent être mis en œuvre pour assurer que les visiteurs sont accompagnés à tout moment dans les zones contenant des prises réseau actives.		2				
9.1.3 Restreindre l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans fil.		2				

9.2 Développer des procédures pour distinguer facilement le personnel du site des visiteurs, en incluant : • L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple) ; • En changeant les conditions d'accès ; • La révocation ou l'élimination de l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à expiration (telle que les badges d'identification).			**5**
9.3 Contrôler l'accès physique du personnel du site aux zones sensibles comme suit : • L'accès doit être autorisé et basé sur les fonctions professionnelles individuelles. • L'accès est immédiatement révoqué à la cessation de fonction de l'employé et tous les mécanismes d'accès physique, tels que les clés, cartes d'accès, etc., sont rendus ou désactivés.	**2**		

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
9.4 Mettre en œuvre des procédures pour identifier et autoriser les visiteurs. Les procédures doivent inclure les points suivants :						
9.4.1 Les visiteurs sont autorisés avant d'entrer et accompagnés en permanence dans les zones où sont traitées et conservées les données de titulaires de carte.					5	
9.4.2 Les visiteurs sont identifiés et un badge ou une autre forme d'identification leur est remis avec une date limite d'utilisation, qui distingue clairement les visiteurs du personnel du site.					5	
9.4.3 Les visiteurs doivent rendre le badge ou l'autre forme d'identification physique avant de quitter les locaux ou à la date d'expiration.					5	
9.4.4 Un registre des visites est utilisé pour maintenir un suivi d'audit de l'activité des visiteurs aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de carte. Y consigner le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son accès physique. Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi.					5	
9.5 Assurer la sécurité physique de tous les supports.					5	
9.5.1 Ranger les sauvegardes sur support en lieu sûr, de préférence hors des locaux de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an.					5	
9.6 Assurer un contrôle strict de la distribution interne ou externe de tout type de support, notamment ce qui suit :						
9.6.1 Classer les supports afin de déterminer la sensibilité des données qu'ils contiennent.					5	
9.6.2 Envoyer les supports par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis.					5	
9.6.3 S'assurer que les responsables approuvent le déplacement de tout support déplacé d'une zone sécurisée (en particulier s'ils sont distribués à des individus).					5	
9.7 Assurer un contrôle strict du stockage et de l'accessibilité des supports.						
9.7.1 Tenir de manière appropriée les journaux d'inventaire de tous les supports et effectuer un inventaire des supports au moins une fois par an.					5	
9.8 Détruire les supports lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou légales comme suit :						
9.8.1 Déchiqueter, brûler ou réduire en pâte les documents papier de sorte que les données de titulaires de carte ne puissent pas être reconstituées. Sécuriser les conteneurs de stockage utilisés pour les documents qui doivent être détruits.	1					
9.8.2 Rendre les données de titulaires de carte sur support électronique irrécupérables de sorte que les informations ne puissent pas être reconstituées.	1					
9.9 Protéger les dispositifs qui capturent les données de carte de paiement par interaction physique directe avec la carte des manipulations malveillantes et des substitutions. *Remarque : Ces conditions s'appliquent aux dispositifs de lecture de carte utilisés dans les transactions pour lesquelles la carte est présente (c'est-à-dire, une lecture de piste ou de puce) au point de vente. Cette condition n'est pas destinée à être appliquée pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.*						

9.9.1 Maintenir une liste d'appareils à jour. La liste doit inclure les points suivants : • Marque et modèle de l'appareil ; • L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve l'appareil) ; • Le numéro de série de l'appareil ou autre méthode d'identification unique.	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
9.9.2 Inspecter régulièrement la surface des appareils pour voir si elle présente des signes de manipulations malveillantes (par exemple, l'ajout de copieur de carte sur l'appareil), ou de substitution (par exemple, en inspectant le numéro de série ou autre caractéristique de l'appareil pour vérifier qu'il n'a pas été substitué par un appareil frauduleux). *Remarque : Les exemples de signes qu'un appareil aurait pu être la victime de manipulations malveillantes ou substituées comprennent les fixations de câble ou de dispositifs inattendus à l'appareil, les étiquettes de sécurité manquantes ou modifiées, un boîtier cassé ou de couleur différente, ou un changement du numéro de série ou autres marques externes.*		2				
9.9.3 Assurer la formation du personnel afin qu'il soit conscient des tentatives de manipulation malveillantes ou de remplacement des appareils. La formation doit inclure les points suivants : • Vérifier l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils. • Ne pas installer, remplacer ou renvoyer l'appareil sans vérification. • Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues). • Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité).		2				
9.10 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.					5	
Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte						
10.1 Implémenter des cheminements d'audit pour relier tous les accès aux composants de système à chaque utilisateur individuel.				4		
10.2 Mettre en œuvre des journaux d'audit automatiques pour tous les composants du système afin de reconstituer les événements suivants :						
10.2.1 Tous les accès des utilisateurs individuels aux données de titulaires de carte				4		
10.2.2 Toutes les actions exécutées par tout utilisateur avec des droits racine ou				4		
10.2.3 Accès à toutes les vérifications à rebours				4		
10.2.4 Tentatives d'accès logique non valides				4		
10.2.5 L'utilisation et les modifications des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation de privilèges, et toutes les modifications, additions ou suppressions aux				4		
10.2.6 Initialisation, interruption ou pause des journaux d'audit				4		
10.2.7 Création et suppression d'objets au niveau système				4		
10.3 Consigner dans les journaux d'audit au moins les entrées suivantes pour chaque événement :						
10.3.1 Identification de l'utilisateur				4		
10.3.2 Type d'événement				4		

10.3.3 Date et heure	**4**	
10.3.4 Indication de succès ou d'échec	**4**	
10.3.5 Origine de l'événement	**4**	
10.3.6 Identité ou nom des données, du composant du système ou de la ressource	**4**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
10.4 À l'aide d'une technologie de synchronisation temporelle, synchroniser tous les systèmes d'horloge et temporels critiques et s'assurer que les éléments suivants sont mis en œuvre pour l'acquisition, la distribution et l'enregistrement du temps. *Remarque : Le protocole Network Time Protocol (NTP -Protocole d'Heure Réseau) est un exemple de technologie de synchronisation temporelle.*				4		
10.4.1 L'heure des systèmes critiques est correcte et la même pour tous.				4		
10.4.2 Les données temporelles sont protégées.				4		
10.4.3 Les paramètres temporels sont reçus de sources temporelles reconnues par le secteur.				4		
10.5 Protéger les journaux d'audit de sorte qu'ils ne puissent pas être modifiés.						
10.5.1 Limiter l'affichage des vérifications à rebours aux utilisateurs qui en ont besoin				4		
10.5.2 Protéger les fichiers de vérifications à rebours contre toute modification non autorisée.				4		
10.5.3 Sauvegarder rapidement les fichiers de vérifications à rebours sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer.				4		
10.5.4 Inscrire les journaux pour les technologies orientées vers l'extérieur sur un serveur de journal interne centralisé et sécurisé, ou sur un dispositif de support.				4		
10.5.5 Analyser les journaux à l'aide d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte).				4		
10.6 Examiner les journaux et les évènements de sécurité de tous les composants de système pour identifier les anomalies ou les activités suspectes. *Remarque : Des outils de journalisation, d'analyse et d'alerte peuvent être utilisés pour respecter cette condition.*						
10.6.1 Examiner les points suivants au moins une fois par jour : • Tous les événements de sécurité • Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD • Les journaux de tous les composants critiques du système • Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.)				4		
10.6.2 Examiner régulièrement les journaux de tous les autres composants de système conformément aux politiques et à la stratégie de gestion des risques de l'organisation, ainsi que le détermine l'évaluation de risque annuelle de l'organisation.				4		
10.6.3 Suivi des exceptions et des anomalies identifiées pendant le processus d'examen.				4		
10.7 Conserver l'historique des audits pendant une année au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, à fin d'analyse (par exemple, disponibles en ligne, dans des archives ou pouvant être restaurés à partir d'une sauvegarde).				4		

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
10.8 Condition supplémentaire pour les prestataires de services uniquement : Implémenter un processus pour détecter et signaler à temps les pannes des systèmes de contrôle de sécurité critiques, y compris, mais sans s'y limiter, les pannes relatives aux : • Pare-feu • IDS/IPS • FIM • Antivirus • Contrôles d'accès physiques • Contrôles d'accès logiques • Mécanismes de journalisation d'audit • Contrôles de segmentation (le cas échéant) *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*				4		
10.8.1 Condition supplémentaire pour les prestataires de services uniquement : Intervenir face aux pannes de contrôles de sécurité critiques en temps opportun. Les processus de résolution des pannes de contrôles de sécurité doivent comprendre : • Rétablissement des fonctions de sécurité • Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité • Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause fondamentale • Identification et résolution des problèmes de sécurité survenus pendant la panne • Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité • Implémentation des contrôles pour prévenir la répétition d'une telle panne • Reprise de la surveillance des contrôles de sécurité				4		
10.9 S'assurer que les politiques de sécurité et les procédures opérationnelles pour le contrôle de tous les accès aux ressources du réseau et aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.				4		
Condition 11 : Tester régulièrement les processus et les systèmes de sécurité						
11.1 Mettre en œuvre des processus pour tester la présence de points d'accès sans fil (802.11) ; détecter et identifier tous les points d'accès sans fil autorisés et non autorisés sur une base trimestrielle. *Remarque : Les analyses de réseau sans fil, les inspections logiques/physiques des composants de système et de l'infrastructure, le contrôle d'accès réseau (NAC) ou les systèmes de détection et/ou de prévention d'intrusions sans fil sont quelques exemples de méthodes pouvant être utilisées pour ce processus. Quelles que soient les méthodes utilisées, elles doivent être suffisantes pour détecter et identifier les appareils autorisés ainsi que les appareils non autorisés.*				4		
11.1.1 Maintenir un registre des points d'accès sans fil autorisés comprenant une justification commerciale documentée.				4		

11.1.2 Mettre en œuvre des procédures de réponse aux incidents au cas où des points d'accès non autorisés sont détectés.	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
11.2 Analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux (par exemple, installation de nouveaux composants de système, modification de la topologie du réseau ou des règles des pare-feu, mise à niveau de produits). *Remarque : De multiples rapports de scan peuvent être combinés pour que le processus de scan trimestriel montre que tous les systèmes ont été scannés et que toutes les vulnérabilités applicables ont été traitées. Une documentation supplémentaire peut être requise pour vérifier que les vulnérabilités qui n'ont pas été résolues sont en phase de l'être.* *Pour la conformité initiale à la norme PCI DSS, il n'est pas obligatoire que quatre scans trimestriels aient été réalisés avec succès si l'évaluateur vérifie que 1) le résultat du dernier scan était réussi, 2) l'entité a documenté les politiques et les procédures exigeant l'exécution de scans trimestriels et 3) toutes les vulnérabilités relevées dans les résultats ont été corrigées, comme indiqué lors de la réexécution du scan. Pour les années qui suivent la vérification PCI DSS initiale, quatre scans trimestriels réussis ont été réalisés.*		**2**				
11.2.1 Effectuer des scans trimestriels de vulnérabilité interne. Résoudre les vulnérabilités et renouveler les scans pour vérifier que toutes les vulnérabilités à « risque élevé » sont résolues conformément à la classe de vulnérabilité de l'entité (selon la condition 6.1). Les analyses doivent être exécutées par un personnel qualifié.		**2**				
11.2.2 Des analyses de vulnérabilité externe doivent être effectuées une fois par trimestre par un prestataire de services de scan agréé par le PCI SSC (Payment Card Industry Security Standards Council -Conseil des normes de sécurité PCI). Recommencer le scan si nécessaire, jusqu'à ce que les scans soient réussis. *Remarque : Les scans de vulnérabilité externe doivent être effectués une fois par trimestre par un prestataire de services de scan agréé (ASV) par le PCI SSC (Payment Card Industry Security Standards Council-Conseil des normes de sécurité PCI). Consulter le Guide de programme ASV publié sur le site Web du PCI SSC pour connaître les responsabilités du client vis-à-vis du scan, la préparation du scan, etc.*		**2**				
11.2.3 Effectuer les scans internes et externes et recommencez si nécessaire, après tout changement d'importance. Les analyses doivent être exécutées par un personnel qualifié.		**2**				
11.3 Mettre en œuvre une méthodologie pour le test de pénétration qui inclut ce qui suit : • Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115) • Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques • Comprend un test depuis l'intérieur et l'extérieur du système • Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée. • Définit les tests de pénétration de couche d'application pour qu'ils comprennent, au minimum les vulnérabilités indiquées dans la Condition 6.5. • Définit les tests de pénétration de couche d'application pour qu'ils comprennent les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation. • Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois • Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation.		**2**				

11.3.1 Effectuer des tests de pénétration externe au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement).	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
11.3.2 Effectuer des tests de pénétration internes au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement).		2				
11.3.3 Les vulnérabilités exploitables découvertes pendant le test de pénétration sont corrigées et les tests sont recommencés pour vérifier les corrections.		2				
11.3.4 Si la segmentation est utilisée pour isoler le CDE des autres réseaux, effectuer des tests de pénétration au moins une fois par an et après toute modification des méthodes/contrôles de segmentation pour vérifier que les méthodes de segmentation sont opérationnelles et efficaces, et isoler tous les systèmes hors champ d'application des systèmes inclus dans le CDE.		2				
11.3.4.1 Condition supplémentaire pour les prestataires de services uniquement : En cas de segmentation, confirmer le champ d'application de la norme PCI DSS en effectuant des tests de pénétration sur les contrôles de segmentation au moins une fois par semestre et après des modifications apportées aux contrôles/méthodes de segmentation. *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*		2				
11.4 Utiliser les techniques d'intrusion-détection et/ou d'intrusion-prévention pour détecter et/ou empêcher les intrusions dans le réseau. Surveiller la totalité du trafic au périmètre de l'environnement de données de titulaires de carte, ainsi qu'aux points critiques de l'environnement des données de titulaires de carte et alerter le personnel en cas de soupçons de compromis. Tenir à jour tous les moteurs d'intrusion-détection et de prévention, les lignes de base et les signatures.		2				
11.5 Déployer des mécanismes de détection des modifications (par exemple, des outils de contrôle de l'intégrité des fichiers) pour alerter le personnel de toute modification non autorisée (y compris des changements, des ajouts et des suppressions) des fichiers critiques du système, des fichiers de configuration ou des fichiers de contenu et configurer le logiciel pour qu'il effectue des comparaisons de fichier critique au moins une fois par semaine. *Remarque : Pour la détection des changements, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les mécanismes de détection des changements tels que les produits de surveillance d'intégrité de fichier sont généralement préconfigurés avec les fichiers critiques pour le système d'exploitation connexe. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).*				4		
11.5.1 Mettre en œuvre un processus pour répondre à n'importe quelle alerte générée par la solution de détection de changement.				4		
11.6 S'assurer que les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sont documentées, utilisées et connues de toutes les parties concernées.				4		

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

12.1 Établir, publier, maintenir et diffuser une politique de sécurité.	**6**
12.1.1 Examiner la politique de sécurité au moins une fois par an et mettre la politique à jour lorsque l'environnement change.	**6**

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
12.2 Mettre en œuvre un processus d'évaluation des risques qui : • Est effectué au moins une fois par an et à la suite des changements significatifs apportés à l'environnement (par exemple acquisition, intégration, déménagement, etc.) • Identifie les actifs critiques, les menaces et vulnérabilités, et • Se solde par une analyse formelle et documentée de risques. Les exemples de méthodologies d'évaluation des risques comprennent entre autres les directives OCTAVE, ISO 27005 et NIST SP 800-30.	1					
12.3 Développer les politiques d'utilisation des technologies critiques et définir l'utilisation adéquate de ces technologies. *Remarque : Les exemples de technologies critiques comprennent notamment l'accès à distance et les technologies sans fil, les ordinateurs portables, les tablettes, les supports électroniques amovibles, l'utilisation d'e-mail et d'Internet.* S'assurer que ces politiques d'utilisation exigent ce qui suit :						6
12.3.1 Approbation explicite des responsables						6
12.3.2 Authentification pour l'utilisation des technologies						6
12.3.3 Liste de tous les périphériques et du personnel disposant d'un accès						6
12.3.4 Une méthode permettant de déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils)						6
12.3.5 Usages acceptables de la technologie						6
12.3.6 Emplacements acceptables des technologies sur le réseau						6
12.3.7 Liste des produits approuvés par la société						6
12.3.8 Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique						6
12.3.9 Activation des technologies d'accès à distance pour les fournisseurs et les partenaires commerciaux, uniquement lorsque c'est nécessaire, avec désactivation immédiate après usage						6
12.3.10 Lors de l'accès du personnel aux données de titulaires de carte au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données de titulaires de carte sur des disques durs locaux et des supports électroniques amovibles, sauf autorisation expresse pour un besoin professionnel défini. Lorsqu'il existe un besoin professionnel autorisé, la politique d'utilisation doit exiger						6
12.4 S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tout le personnel en matière de sécurité.						6
12.4.1 Condition supplémentaire pour les prestataires de services uniquement : L'équipe de direction a défini la responsabilité relative à la protection des données de titulaires de carte et un programme de conformité à la norme PCI DSS, comme suit : • Responsabilité globale pour respecter la conformité à la norme PCI DSS • Définition d'une charte pour un programme de conformité à la norme PCI DSS et des canaux de communication avec la direction *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au*						6

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
12.5 Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations :						6
12.5.1 Définir, documenter et diffuser les politiques et les procédures de sécurité.						6
12.5.2 Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent.						6
12.5.3 Définir, documenter et diffuser les procédures de remontée et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations.		2				
12.5.4 Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la						6
12.5.5 Surveiller et contrôler tous les accès aux données.						6
12.6 Mettre en œuvre un programme formel de sensibilisation à la sécurité pour sensibiliser tout le personnel à la politique et aux procédures de sécurité relatives aux données de titulaires de carte.						6
12.6.1 Former le personnel au moment du recrutement et au moins une fois par an. Remarque : Les méthodes varient selon les postes occupés et le niveau d'accès du personnel aux données de titulaires de carte.						6
12.6.2 Exiger que le personnel reconnaisse au moins une fois par an avoir lu et compris les procédures et la politique de sécurité.						6
12.7 Effectuer une sélection préalable à l'embauche du personnel pour minimiser les risques d'attaques par des sources internes (Ces contrôles devraient inclure, par exemple, les antécédents professionnels, le casier judiciaire, les renseignements de solvabilité et la vérification des références.) *Remarque : Pour le personnel dont l'embauche potentielle concerne des postes tels que celui de caissier dans un magasin, et qui n'a accès qu'à un numéro de carte à la fois à l'occasion du traitement d'une transaction, cette condition n'est qu'une recommandation.*						6
12.8 Maintenir et mettre en œuvre des politiques et des procédures de gestion des prestataires de services avec lesquels les données de titulaires de carte sont partagées, ou qui pourraient affecter la sécurité des données de titulaires de carte comme suit :		2				
12.8.1 Conserver une liste des prestataires de services, y compris une description des services fournis.		2				
12.8.2 Maintenir un accord écrit par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte. *Remarque : La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.*		2				
12.8.3 S'assurer que le processus de sélection des prestataires de services est bien défini, et qu'il inclut notamment des contrôles préalables à l'engagement.		2				
12.8.4 Maintenir un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an.		2				

12.8.5 Maintenir les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation.	**2**	

Conditions de la norme PCI DSS, version 3.2	Étape					
	1	2	3	4	5	6
12.9 Condition supplémentaire pour les prestataires de services uniquement : Les prestataires de services reconnaissent par écrit qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte. *Remarque : La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.*		2				
12.10 Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système.						
12.10.1 Élaborer le plan de réponse aux incidents à mettre en place en cas d'intrusion dans le système. S'assurer que le plan prévoit au moins les points suivants : • Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ; • Les procédures de réponse aux incidents spécifiques ; • Les procédures de continuité et de reprise des affaires ; • Processus de sauvegarde des données ; • Analyse des exigences légales en matière de signalement des incidents ; • Couverture et réponses de tous les composants stratégiques du système ; • Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement.		2				
12.10.2 Examiner et tester le plan au moins une fois par an, y compris les éléments répertoriés dans la condition 12.10.1.		2				
12.10.3 Désigner le personnel spécifique disponible 24 heures sur 24 et sept jours sur sept pour répondre aux alertes.		2				
12.10.4 Organiser la formation appropriée du personnel en charge de la réponse aux violations de la sécurité.		2				
12.10.5 Inclure les alertes des systèmes de surveillance de sécurité, notamment les systèmes d'intrusion-détection, intrusion-prévention, les pare-feu et les systèmes de surveillance de l'intégrité des fichiers.		2				
12.10.6 Définir un processus de modification et de développement du plan de réponse aux incidents en fonction des leçons apprises, et tenir compte de l'évolution du secteur.		2				
12.11 Condition supplémentaire pour les prestataires de services uniquement : Effectuer des vérifications au moins une fois par trimestre pour confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles. Les examens doivent couvrir les processus suivants : • Examens quotidiens des journaux • Examens des règles liées aux pare-feu • Application des normes de configuration aux nouveaux systèmes • Intervention suite aux alertes de sécurité • Modifier les processus de gestion *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*						6

Conditions de la norme PCI DSS, version 3.2	Étape 1	2	3	4	5	6
12.11.1 Condition supplémentaire pour les prestataires de services uniquement : La gestion de la documentation du processus d'examens trimestriels comprend ce qui suit : • Documentation des résultats d'examens • Examiner et valider les résultats par le personnel responsable du programme de conformité à la norme PCI DSS *Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.*						6
Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux prestataires de services d'hébergement partagé						
A1 Protéger les données et l'environnement hébergés de chaque entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité) conformément aux conditions A1.1 à A1.4 : Un prestataire de services d'hébergement doit satisfaire à ces conditions ainsi qu'aux conditions de toutes les autres rubriques pertinentes de la norme PCI DSS. *Remarque : Même si un prestataire de services d'hébergement peut satisfaire à ces conditions, la conformité de l'entité qui a recours au prestataire de services d'hébergement n'est pas garantie. Chaque entité doit se conformer à la norme PCI DSS et doit valider cette conformité comme applicable.*			3			
A1.1 S'assurer que chaque entité ne met en œuvre que les processus qui ont accès à l'environnement des données de titulaires de carte qui la concerne.			3			
A1.2 Restreindre l'accès et les privilèges de chaque entité à son propre environnement de données de titulaires de carte.			3			
A1.3 S'assurer que la journalisation et les vérifications à rebours sont activées, uniques à l'environnement des données de titulaires de carte de chaque entité et conformes à la condition 10 de la norme PCI DSS.			3			
A1.4 Activer les processus d'investigation informatique légale rapide en cas d'incident dans l'environnement d'un commerçant ou d'un prestataire de services.			3			
Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial *Remarque : Cette annexe s'applique à toutes les entités ayant recours au SSL/TLS initial en tant que contrôles de sécurité pour protéger le CDE et/ou le CHD*						
A2.1 Lorsque les terminaux POS POI (et les points de terminaison SSL/TLS auxquels se connecter) utilisent le SSL et/ou le TLS initial, l'entité doit : • Confirmer les dispositifs qui n'ont pas de failles connues pour ces protocoles. Ou : • Disposer d'un plan formel d'atténuation des risques et de migration.		2				
A2.2 Les entités dotées d'implémentations existantes (autres que celles autorisées dans la condition A2.1) et utilisant le SSL et/ou TLS initial doivent disposer d'un plan formel d'atténuation des risques et de migration.		2				

A2.3 Condition supplémentaire pour les prestataires de services uniquement : D'ici le 30 juin 2016, tous les prestataires de services doivent proposer un service sécurisé. *Remarque : D'ici le 30 juin 2016, le prestataire de services doit proposer soit un protocole sécurisé compris dans son offre de services soit un plan documenté d'atténuation des risques et de migration (conformément à la condition A2.2) avec une date cible pour offrir un protocole sécurisé d'ici le 30 juin 2016. Après cette date, tous les prestataires de services doivent offrir un protocole sécurisé pour leurs services.*	**2**	