PCI (Payment Card Industry)
Data Security Standard

Conditions et procédures d'évaluation de sécurité

Version 2.0

Octobre 2010

Modifications apportées au document

Date	Version	Description	Pages
Octobre 2008	*1.2*	*Afin de présenter la v1.2 de la norme PCI DSS comme les « Conditions et procédures d'évaluation de sécurité PCI DSS », élimination des redondances entre les documents et changements d'ordre général et spécifique par rapport à la v1.1 des* Procédures d'audit de sécurité PCI DSS. *Pour des informations complètes, consulter le document* PCI Data Security Standard – Récapitulatif des changements entre les versions 1.2.1 et 2.0 de la norme PCI DSS.	
Juillet 2009	*1.2.1*	*Ajout d'une phrase supprimée par erreur entre les v1.1 et v1.2 de la norme PCI DSS.*	*5*
		Correction de « ensuite » par « que » dans les procédures de test 6.3.7.a et 6.3.7.b.	*32*
		Suppression des marques grisées des colonnes « En place » et « Pas en place » dans la procédure de test 6.5.b.	*33*
		Pour le document Fiche de contrôles compensatoires – Exemple complété, correction de vocabulaire en haut de page pour dire « Se référer à cette fiche pour définir des contrôles compensatoires pour toute condition indiquée comme « en place » par le biais des contrôles compensatoires. »	*64*
Octobre 2008	*2.0*	*Mise à jour et application des changements depuis la v1.2.1. Pour plus de détails, consulter* « PCI DSS – Récapitulatif des changements entre les versions 1.2.1 et 2.0 de la norme PCI DSS »	

Table des matières

Introduction et présentation de la norme PCI DSS

La norme PCI (Payment Card Industry) DSS (Data Security Standard) a été développée dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. La norme PCI DSS sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données des titulaires de cartes. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de service, ainsi que toutes les autres entités qui stockent, traitent ou transmettent des données de titulaires de cartes. La norme PCI DSS consiste en un ensemble de conditions minimum pour la protection des données de titulaires de cartes et peut être renforcée de contrôles et pratiques supplémentaires pour réduire encore davantage les risques. Les 12 conditions de la norme PCI DSS sont détaillées ci-dessous.

PCI DSS – Présentation détaillée

Création et gestion d'un réseau sécurisé	1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données des titulaires de cartes de crédit	3. Protéger les données de titulaire de carte stockées 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
Gestion d'un programme de gestion des vulnérabilités	5. Utiliser des logiciels antivirus et les mettre à jour régulièrement 6. Développer et gérer des systèmes et des applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître 8. Affecter un ID unique à chaque utilisateur d'ordinateur 9. Restreindre l'accès physique aux données des titulaires de cartes
Surveillance et tests réguliers des réseaux	10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes 11. Tester régulièrement les processus et les systèmes de sécurité
Gestion d'une politique de sécurité des informations	12. Gérer une politique de sécurité des informations pour l'ensemble du personnel.

Le présent document, intitulé *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS*, combine les 12 conditions de la norme PCI DSS et les procédures de test correspondantes en un outil d'évaluation de sécurité. Il est conçu pour être utilisé au cours des évaluations de conformité PCI DSS, dans le cadre du processus de validation d'une entité. Les sections suivantes détaillent les directives et meilleures pratiques afin d'aider les entités à se préparer à une évaluation PCI DSS, à la mener à bien et à en rapporter les résultats. Les conditions PCI DSS et les procédures de test commencent **page 19.**

Le site Web du PCI Security Standards Council (PCI SSC) (www.pcisecuritystandards.org) contient un certain nombre de ressources supplémentaires, notamment :

- Attestations de conformité
- *Navigation dans la norme PCI DSS : comprendre l'objectif des conditions*
- Glossaire *des termes, abréviations et acronymes PCI DSS et PA-DSS*
- Questions fréquentes (FAQ)
- Suppléments d'information et directives

Consulterwww.pcisecuritystandards.org pour plus d'informations.

***Remarque** : les suppléments d'information complètent la norme PCI DSS et identifient des considérations et recommandations supplémentaires pour remplir les conditions PCI DSS, sans changer, éliminer ni supplanter la norme PCI DSS ni aucune de ses conditions.*

Informations relatives aux conditions d'application de la norme PCI DSS

La norme PCI DSS s'applique partout où des données de compte sont stockées, traitées ou transmises. *Les données de compte* regroupent les *données du titulaires de cartes* plus les *données d'authentification sensibles,* indiquées ci-dessous :

Les données du titulaires de cartes comprennent :	***Les données d'authentification sensibles comprennent :***
▪ Numéro de compte primaire (PAN) ▪ Nom du titulaire de la carte ▪ Date d'expiration ▪ Code service	▪ Données de bande magnétique complètes ou leur équivalent sur une puce ▪ CAV2/CVC2/CVV2/CID ▪ Codes/blocs PIN

Le numéro de compte primaire est le facteur déterminant de l'applicabilité des conditions PCI DSS. Les conditions PCI DSS sont applicables si un PAN est stocké, traité ou transmis. Si le PAN n'est pas stocké, traité ni transmis, les conditions PCI DSS ne s'appliquent pas.

Si le nom du titulaires de cartes, le code de service, et/ou la date d'expiration sont stockés, traités ou transmis avec le PAN, ou existent d'une façon ou d'une autre dans l'environnement des données du titulaires de cartes, ils doivent être protégés conformément à toutes les conditions PCI DSS ***sauf*** les conditions 3.3 et 3.4, qui s'appliquent uniquement au PAN.

La norme PCI DSS représente un ensemble minimum d'objectifs de contrôle qui peut être renforcé par des lois et règlements locaux, régionaux ou sectoriels. En outre, la législation ou la réglementation peuvent exiger une protection spécifique des informations personnelles identifiables ou d'autres éléments de données (par exemple, le nom du titulaires de cartes), ou définir les pratiques de divulgation d'une entité, relatives aux informations concernant le consommateur. La législation relative à la protection des données des consommateurs, à la confidentialité, au vol d'identité, ou à la sécurité des données en est un exemple. La norme PCI DSS ne supplante pas les lois locales ou régionales, réglementations gouvernementales ou autres obligations légales.

Le tableau suivant présente un certain nombre d'éléments courants des données des titulaires de cartes et des données d'authentification sensibles, indique si le stockage de chaque élément de données est autorisé ou interdit, et précise si chaque élément de données doit être protégé. Ce tableau n'est pas exhaustif, mais il est présenté de manière à illustrer les différents types de conditions qui s'appliquent à chaque élément de données.

		Élément de données	Stockage autorisé	Rendre illisibles les données de compte stockées selon la condition 3.4
Données de compte	**Données du titulaire de la carte**	Numéro de compte primaire (PAN)	Oui	Oui
		Nom du titulaire de la carte	Oui	Non
		Code service	Oui	Non
		Date d'expiration	Oui	Non
	Données d'authentification sensibles [1]	Données complètes de la bande magnétique [2]	Non	Stockage interdit selon condition 3.2
		CAV2/CVC2/CVV2/CID	Non	Stockage interdit selon condition 3.2
		Code/bloc PIN	Non	Stockage interdit selon condition 3.2

Les conditions 3.3 et 3.4 de la norme PCI DSS ne s'appliquent qu'au PAN. Si le PAN est stocké avec d'autres données du titulaires de cartes, seul le PAN doit être rendu illisible selon la condition 3.4 de la norme PCI DSS.

La norme PCI DSS ***s'applique uniquement*** si les PAN sont stockés, traités et/ou transmis.

1 *Une fois le processus d'autorisation terminé, les données d'authentification sensibles ne doivent plus être stockées (même si elles sont cryptées).*

2 *Données de piste complètes extraites de la bande magnétique, données équivalentes de la puce, ou d'un autre support.*

Relation entre PCI DSS et PA-DSS

L'utilisation d'une application, conforme à la norme PA-DSS en elle-même, n'en fait pas une entité conforme aux normes PCI DSS, car elle doit être mise en œuvre dans un environnement respectant ces normes, conformément au Guide de mise en œuvre de la norme PA-DSS remis par le fournisseur d'applications de paiement (d'après l'exigence 13.1 de la norme PA-DSS).

Les conditions de la norme PA-DSS sont issues des *conditions et procédures d'évaluation de sécurité PCI DSS* (le présent document). La norme PA-DSS **Error! Hyperlink reference not valid.**détaille ce qu'une application de paiement doit prendre en charge pour permettre la conformité d'un client à la norme PCI DSS.

Les applications de paiement sécurisées, lorsqu'elles sont mises en œuvre dans un environnement conforme aux normes PCI DSS, réduisent autant que possible le risque que des failles de la sécurité compromettent les données de bande magnétique, les codes et valeurs de validation de carte (CAV2, CID, CVC2, CVV2), les codes et les blocs PIN, ainsi que la fraude nuisible résultant de ces failles.

Voici quelques exemples sur la façon dont les applications de paiement peuvent faire obstacle à la conformité :

- stockage des données de bande magnétique et/ou équivalent sur la puce sur le réseau du client après autorisation ;
- applications nécessitant que les clients désactivent d'autres fonctions requises par les normes PCI DSS, telles que les programmes antivirus ou les pare-feu, afin que l'application de paiement fonctionne correctement ;
- utilisation par les fournisseurs de méthodes non sécurisées pour se connecter à l'application lors d'une intervention d'assistance au client.

La norme PA-DSS s'applique aux fournisseurs de logiciels et autres qui développent des applications de paiement stockant, traitant ou transmettant des données de titulaires de cartes dans le cadre d'une autorisation ou d'un règlement, lorsque ces applications de paiement sont vendues, distribuées ou cédées sous licence à des tiers.

Noter ce qui suit concernant l'applicabilité de la norme PA-DSS :

- La norme ***PA-DSS*** s'applique aux applications de paiement généralement vendues et installées « prêtes à l'emploi », sans modification de la part des fournisseurs de logiciels.
- La norme PA-DSS ***NE s'applique PAS*** aux applications de paiement développées par des commerçants et des prestataires de services si elles sont utilisées en interne uniquement (ni vendues, ni distribuées ni cédées sous licence à un tiers), puisque de telles applications de paiement seraient couvertes par la conformité normale du prestataire de services/commerçant aux normes PCI DSS.

Pour des directives détaillées afin de déterminer si la norme PA-DSS concerne une application de paiement donnée, consulter les Conditions et procédures d'évaluation de sécurité de la norme PA-DSS, disponibles sur www.pcisecuritystandards.org.

Champ d'application de l'évaluation de la conformité aux conditions de la norme PCI DSS

Les conditions de sécurité de la norme PCI DSS s'appliquent à tous les composants du système. Dans le cadre de la norme PCI DSS, les « composants du système » désignent tout composant réseau, serveur ou application inclus dans, ou connectés à, l'environnement des données des titulaires de cartes. Les « composants du système » comprennent également tous les composants de virtualisation comme les machines, commutateurs/routeurs, outils, applications/bureaux virtuels ainsi que les hyperviseurs. L'environnement des données de titulaires de cartes est constitué d'individus, de processus et de technologies qui stockent, traitent ou transmettent les données de titulaires de cartes ou des données sensibles d'authentification. Les composants réseau comprennent notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans fil, les équipements réseau et d'autres appareils de sécurité. Les types de serveur comprennent, sans s'y limiter : les serveurs Web, d'application, de base de données, d'authentification, de messagerie, proxy, NTP (Network Time Protocol) et DNS (Domain Name Server). Les applications comprennent toutes les applications achetées et personnalisées, y compris les applications internes et externes (par exemple Internet).

La première étape d'une évaluation PCI DSS est de correctement déterminer le champ d'application de la vérification. Au moins une fois par an, et avant l'évaluation annuelle, l'entreprise évaluée doit confirmer l'exactitude de son champ d'application PCI DSS en identifiant tous les emplacements et flux des données de titulaires de cartes et s'assurer qu'ils sont compris dans le champ d'application. Pour confirmer l'exactitude et l'adéquation du champ d'application PCI DSS, procéder comme suit :

- L'entreprise évaluée identifie et documente l'existence de toutes les données de titulaires de cartes dans son environnement, afin de vérifier qu'aucune donnée de titulaires de cartes n'existe en dehors de l'environnement actuellement défini (CDE).
- Une fois tous les emplacements de données de titulaires de cartes identifiés et documentés, l'entreprise utilise les résultats pour vérifier que le champ d'application PCI DSS est approprié (par exemple, les résultats peuvent être un diagramme ou un inventaire des emplacements des données de titulaires de cartes).
- L'entreprise tient compte des données de titulaires de cartes qui se trouvent dans le champ d'application de l'évaluation PCI DSS et font partie du CDE, sauf si lesdites données sont supprimées ou transférées/regroupées dans le CDE actuellement défini.
- L'entreprise conserve la documentation montrant comment le champ d'application PCI DSS a été confirmé et les résultats, pour l'examen de l'évaluateur et/ou pour référence au cours de l'activité annuelle de confirmation du champ d'application PCI DSS.

Segmentation réseau

La segmentation réseau, ou isolation, de l'environnement des données des titulaires de cartes par rapport au reste du réseau de l'entreprise n'est pas une condition de la norme PCI DSS. Cette approche est cependant vivement recommandée dans la mesure où elle contribue à réduire :

- le champ d'application de l'évaluation PCI DSS ;
- les coûts de l'évaluation PCI DSS ;
- les coûts et les difficultés liés à la mise en œuvre et à la gestion des contrôles PCI DSS ;

- les risques pour une entreprise (réduits grâce au regroupement des données des titulaires de cartes dans un nombre plus restreint de sites mieux contrôlés).

Sans une segmentation réseau adéquate (parfois appelée « réseau plat »), l'ensemble du réseau est inclus dans le champ d'application de l'évaluation PCI DSS. La segmentation réseau peut être réalisée par le biais d'un certain nombre de moyens physiques ou logiques, pare-feu réseau internes correctement configurés et routeurs associés à des listes de contrôle d'accès strictes ou autres technologies qui restreignent l'accès à un segment particulier du réseau.

Pour limiter le champ d'application de l'environnement des données des titulaires de cartes, il est important d'identifier clairement les besoins de l'entreprise et les processus liés au stockage, au traitement ou à la transmission des données des titulaires de cartes. Le regroupement des données des titulaires de cartes dans un nombre d'emplacements aussi restreint que possible, en éliminant les données superflues et en consolidant les données nécessaires, peut impliquer la refonte des pratiques commerciales traditionnelles.

La documentation des flux de données des titulaires de cartes par le biais d'un schéma de flux des données permet de comprendre parfaitement tous les flux de données des titulaires de cartes et de s'assurer que toute segmentation réseau isole correctement l'environnement des données des titulaires de cartes.

Si une segmentation réseau est mise en place et doit servir à réduire le champ d'application de l'évaluation PCI DSS, l'évaluateur doit s'assurer qu'elle convient bien à cette fin. À un niveau supérieur, la segmentation réseau isole les systèmes qui stockent, traitent ou transmettent les données des titulaires de cartes des autres systèmes. Toutefois, l'adéquation d'une implémentation spécifique de la segmentation réseau peut varier considérablement et dépend de facteurs tels que la configuration d'un réseau, les technologies déployées et d'autres contrôles susceptibles d'être mis en œuvre.

L'Annexe D : Segmentation et échantillonnage des installations de l'entreprise et des composants du système fournit d'autres informations sur l'effet de la segmentation réseau et de l'échantillonnage sur le champ d'application de l'évaluation PCI DSS.

Technologie sans fil

Si la technologie sans fil est utilisée pour stocker, traiter ou transmettre les données des titulaires de cartes (par exemple, transactions des points de vente et « line busting » [ou élimination des files d'attente aux points de paiement]), ou si un réseau local (WLAN) sans fil est connecté à l'environnement des données des titulaires de cartes ou en fait partie (par exemple, s'il n'est pas clairement séparé par un pare-feu), les conditions de la norme PCI DSS et les procédures de test pour les environnements sans fil s'appliquent et doivent être exécutées (par exemple, conditions 1.2.3, 2.1.1 et 4.1.1). Avant de mettre en œuvre la technologie sans fil, une entreprise doit soigneusement évaluer la nécessité de déployer cette technologie par rapport aux risques induits. Le déploiement de la technologie sans fil ne doit être envisagé que pour la transmission de données non sensibles.

Prestataires tiers/Sous-traitance

Pour les prestataires de services qui doivent subir une évaluation sur site annuelle, la validation de conformité doit s'appliquer à tous les composants du système de l'environnement des données des titulaires de cartes.

Un prestataire de services ou un commerçant peuvent faire appel à un prestataire tiers pour le stockage, le traitement ou la transmission des données des titulaires de cartes en son nom, ou pour la gestion de composants tels que les routeurs, les pare-feu, les bases de données, la sécurité physique et/ou les serveurs. Dans ce cas, la sécurité de l'environnement des données des titulaires de cartes peut s'en trouver affectée.

Si des sociétés sous-traitent le stockage, le traitement ou la transmission des données des titulaires de cartes auprès de prestataires de services tiers, le rapport de conformité (ROC, Report on Compliance) doit décrire le rôle de chaque prestataire de services et identifier clairement les conditions qui s'appliquent à l'entité évaluée et celles qui s'appliquent au prestataire de services. Il existe deux options de validation de la conformité des prestataires de services tiers :

1) Ils peuvent subir une évaluation PCI DSS de leur propre chef et fournir à leurs clients la preuve de leur conformité.
2) S'ils choisissent de ne pas subir une évaluation PCI DSS de leur propre chef, leurs services devront être examinés en même temps que les évaluations PCI DSS de chacun de leurs clients.

Pour plus d'informations, se reporter au premier point du paragraphe « Pour l'examen des prestataires de services gérés (MSP, Managed Service Providers) » dans le point 3 de la section « Instructions et contenu du Rapport sur la conformité » ci-dessous.

En outre, les commerçants et les prestataires de services doivent gérer et contrôler la conformité à la norme PCI DSS de tous les prestataires tiers qui ont accès aux données des titulaires de cartes auxquels ils sont associés. *Pour plus d'informations, se reporter à la condition 12.8 du présent document.*

Échantillonnage des installations de l'entreprise et des composants du système

L'échantillonnage n'est pas une condition de la norme PCI DSS. Toutefois, après avoir considéré le champ d'application global et la complexité de l'environnement évalué, l'évaluateur peut sélectionner de manière indépendante des échantillons des installations de l'entreprise et des composants du système afin d'évaluer la conformité aux conditions PCI DSS. Ces échantillons doivent d'abord être définis pour les installations de l'entreprise puis pour les composants du système, au sein de chaque installation sélectionnée. Les échantillons doivent être représentatifs de tous les types de sites des installations de l'entreprise et des types de composants du système, au sein des installations sélectionnées. Les échantillons doivent être suffisamment importants pour donner à l'évaluateur la garantie que les contrôles sont appliqués comme prévu.

L'échantillonnage des installations de l'entreprise et des composants du système pour une évaluation ne réduit pas le champ d'application de l'environnement des données des titulaires de carte, ni l'applicabilité des conditions de la norme PCI DSS. Que l'échantillonnage soit ou non utilisé, les conditions de la norme PCI DSS s'appliquent à la totalité de l'environnement des données des titulaires de carte. Si l'échantillonnage est utilisé, chaque échantillon doit être évalué par rapport à toutes les conditions applicables de la norme PCI DSS. L'échantillonnage des conditions PCI DSS elles-mêmes n'est pas autorisé.

Les exemples d'installations d'entreprise comprennent, sans s'y limiter : les bureaux d'entreprise, les sites en franchise, les installations de traitement, les centres de données et autres types d'installations à des sites différents. L'échantillonnage doit inclure les composants du système au sein de chaque installation de l'entreprise. Par exemple, pour chaque installation de l'entreprise, il convient d'inclure divers systèmes d'exploitation, fonctions et applications liés au domaine évalué.

Au sein de chaque installation de l'entreprise, l'évaluateur peut choisir les serveurs Sun exécutant le navigateur Apache WWW, les serveurs Windows exécutant Oracle, les systèmes mainframe exécutant les applications traditionnelles de traitement de cartes, les serveurs de transfert de données exécutant HP-UX et les serveurs Linux exécutant MYSQL. Si toutes les applications s'exécutent à partir d'un système d'exploitation

unique (par exemple, Windows 7 ou Solaris 10), l'échantillon doit tout de même inclure diverses applications (par exemple, serveurs de bases de données, serveurs Web et serveurs de transfert de données).

Lorsqu'ils choisissent des échantillons d'installations d'entreprise et de composants de système de manière indépendante, les évaluateurs doivent prendre en compte les facteurs suivants :

- S'il existe des processus et contrôles standards, opérationnels et de sécurité PCI DSS centralisés, en place, garantissant la cohérence et que chaque installation de l'entreprise/composant du système doit suivre, l'échantillon peut être plus petit que si aucun processus/contrôle n'est en place. L'échantillon doit être assez important pour donner à l'évaluateur une garantie raisonnable que toutes les installations de l'entreprise et composants du système sont configurés conformément aux processus standards.
- S'il existe plus d'un type de processus de sécurité et/ou opérationnel en place (par exemple pour divers types d'installations de l'entreprise/composants du système), l'échantillon doit être assez important pour intégrer les installations de l'entreprise/composants du système sécurisés par chaque type de processus.
- S'il n'existe pas de processus et contrôles PCI DSS standards en place et que chaque installation de l'entreprise et composant du système sont gérés par des processus non standards, l'échantillon doit être plus important pour que l'évaluateur ait la garantie que chaque installation de l'entreprise/composant du système a mis en œuvre les conditions de la norme PCI DSS de la manière appropriée.

Lorsque l'échantillonnage est utilisé, l'évaluateur doit, pour chaque échantillon :

- documenter la justification de la technique d'échantillonnage et de la taille de l'échantillon ;
- documenter et valider les processus et contrôles PCI DSS standardisés, utilisés pour déterminer la taille de l'échantillon ;
- expliquer dans quelle mesure l'échantillon est approprié et représentatif de la population globale.

Se référer également à :
Annexe D : Échantillonnage des installations de l'entreprise et des composants du système.

Les évaluateurs doivent revalider la justification de l'échantillonnage pour chaque évaluation. Si l'échantillonnage est utilisé, divers échantillons des installations de l'entreprise et des composants du système doivent être sélectionnés pour chaque évaluation.

Contrôles compensatoires

Une fois par an, tous les contrôles compensatoires doivent être documentés, examinés et validés par l'évaluateur, puis inclus dans le Rapport sur la conformité qui est envoyé, conformément à *l'annexe B : Contrôles compensatoires* et à *l'Annexe C : Fiche de contrôles compensatoires.*

Pour chaque contrôle compensatoire, la fiche de contrôles compensatoires *(Annexe C)* **doit** être complétée. Par ailleurs, les résultats des contrôles compensatoires doivent être documentés dans le Rapport sur la conformité, dans la section de la condition PCI DSS correspondante.

Pour plus d'informations sur les « contrôles compensatoires », consulter les *annexes B* et *C* mentionnées ci-dessus.

Instructions et contenu du Rapport sur la conformité

Ce document doit être utilisé comme modèle pour la création du *Rapport sur la conformité*. L'entité évaluée doit respecter les conditions respectives de chaque marque de carte de paiement en matière de rapports pour s'assurer que chaque marque connaît l'état de conformité de l'entité. Contacter chaque marque de carte de paiement pour déterminer ses instructions et ses conditions en matière de rapports.

Contenu et format des rapports

Lorsque l'évaluateur complète un Rapport sur la conformité, il doit suivre ces instructions relatives au contenu et au format des rapports :

1. **Résumé**

   Indiquer les éléments suivants :

   - Décrire l'activité Carte de paiement de l'entité, notamment :
     - son rôle professionnel avec les cartes de paiement, à savoir comment et pourquoi elle stocke, traite et/ou transmet les données des titulaires de cartes ;

       Remarque : *il ne s'agit pas ici de copier/coller le contenu du site Web de l'entité, mais de personnaliser la description de manière à démontrer que l'évaluateur comprend bien le rôle de l'entité et sa gestion des paiements.*
     - comment elle traite les paiements (directement, indirectement, etc.) ;
     - les types de réseaux de paiement qu'elle dessert, notamment les transactions carte absente (par exemple, ordre de paiement par e-mail/téléphone (MOTO), e-Commerce), ou les transactions carte présente ;
     - toutes les entités auxquelles elle se connecte pour le traitement ou la transmission des paiements, notamment les relations entre les processeurs.
   - Le schéma détaillé de la topographie réseau de l'entité (obtenu auprès de l'entité même ou créé par l'évaluateur) indiquant :
     - les connexions entrantes et sortantes du réseau ;
     - les composants stratégiques au sein de l'environnement des données des titulaires de cartes, notamment les dispositifs de points de vente, les systèmes, les bases de données et les serveurs Web, le cas échéant ;
     - d'autres composants de paiement nécessaires, le cas échéant.

2. Description du domaine d'activité et de l'approche adoptée

Décrire la portée, conformément aux instructions décrites dans la section Champ d'application de l'évaluation de ce document, notamment les éléments suivants :

- Documenter la manière dont l'évaluateur a validé l'exactitude du champ d'application PCI DSS pour l'évaluation, notamment :
  - les méthodes ou procédés utilisés pour identifier et documenter toutes les existences de données de titulaires de cartes ;
  - la méthode d'évaluation et de documentation des résultats ;
  - la méthode de vérification de l'efficacité et de la précision des méthodes utilisées ;
  - et indiquer que l'évaluateur valide l'exactitude et l'adéquation du champ d'application.
- L'environnement sur lequel porte l'évaluation (par exemple, connexions pour le traitement, réseau intranet et points d'accès Internet du client)
- Si une segmentation réseau est en place et a été utilisée pour réduire la portée de l'examen PCI DSS, expliquer rapidement cette segmentation et la manière dont l'évaluateur l'a validée
- Si l'échantillonnage a été utilisé durant l'évaluation, pour chaque ensemble d'échantillons (d'installations de l'entreprise/de composants du système) utilisés, documenter les éléments suivants :
  - population totale ;
  - nombre d'éléments échantillonnés ;
  - justification du choix de l'échantillon ;
  - description des processus et contrôles de sécurité et opérationnels PCI DSS standardisés, utilisés pour déterminer la taille de l'échantillon et de la manière dont ils ont été validés ;
  - dans quelle mesure l'échantillon est approprié et représentatif de la population globale ;
  - description de tous les emplacements ou environnements, où sont stockées, traitées ou transmises les données des titulaires de cartes, qui ont été EXCLUS du champ d'application de la vérification et en expliquer le motif.
- Indiquer toutes les entités détenues à 100 % qui doivent être mises en conformité avec la norme PCI DSS et si elles sont examinées séparément ou dans le cadre de cette évaluation
- Répertorier toutes les entités internationales qui doivent être mises en conformité avec la norme PCI DSS et si elles sont examinées séparément ou dans le cadre de cette évaluation
- Indiquer tous les réseaux locaux sans fil et/ou les applications de paiement sans fil (par exemple, les terminaux de points de vente) qui sont connectés à l'environnement des données des titulaires de cartes ou qui pourraient en affecter la sécurité, et décrire la sécurité mise en place pour ces environnements sans fil
- La version du document Conditions et procédures d'évaluation de sécurité de la norme PCI DSS sur lequel s'est appuyée l'évaluation

3. Détails concernant l'environnement examiné

Inclure les détails suivants dans cette section :

- Un schéma de chaque élément de la liaison de communication, notamment réseau local (LAN), réseau étendu (WAN) ou Internet.
- Description de l'environnement des données des titulaires de cartes, par exemple :
  - documenter la transmission et le traitement des données des titulaires de cartes, notamment l'autorisation, la collecte, le règlement, le rejet de débit et d'autres flux éventuels ;
  - liste des fichiers et des tables dans lesquels sont stockées les données des titulaires de cartes, étayée par un inventaire créé (ou obtenu auprès du client) et conservé par l'évaluateur parmi les documents relatifs à cette mission. Pour chaque stockage de données de titulaires de cartes (fichier, table, etc.), cet inventaire doit inclure les éléments suivants :
    - la liste de tous les éléments de données des titulaires de cartes stockées,
    - la méthode de sécurisation des données,
    - la méthode de journalisation de l'accès au stockage de données.
- Liste du matériel et des logiciels stratégiques utilisés dans l'environnement des données des titulaires de cartes, accompagnée de la description de la fonction/de l'utilisation de chacun de ces éléments.
- Liste des prestataires de services et autres tiers avec lesquels l'entité partage les données des titulaires de cartes.

  Remarque : *ces entités doivent satisfaire aux conditions de la condition 12.8 de la norme PCI DSS*.
- Liste des applications de paiement tierces utilisées, accompagnée de leur numéro de version, et indication de leur validation éventuelle conformément à la norme PA-DSS. Même si une application de paiement a été validée conformément à la norme PA-DSS, l'évaluateur doit tout de même vérifier qu'elle a été déployée dans le respect de l'environnement et de la norme PCI DSS, et conformément au *Guide de mise en œuvre de la norme* PA-DSS *préparé par le fournisseur de l'application en question.*

  Remarque : *l'utilisation d'applications validées conformément à la norme PA-DSS n'est pas exigée par la norme PCI DSS. Consulter chaque marque de carte de paiement pour comprendre ses conditions en matière de conformité avec la norme PA-DSS.*
- Liste des individus interrogés, leur organisation, leur titre et les sujets abordés.
- Liste de la documentation vérifiée.
- Pour l'examen des prestataires de services gérés (MSP, Managed Service Providers), l'évaluateur doit clairement identifier les conditions qui s'appliquent au MSP (et qui sont incluses dans l'examen) et celles qui en sont exclues et relèvent de la responsabilité des clients du MSP pour être incluses dans leurs examens. Inclure des informations sur les adresses IP du MSP qui sont analysées dans le cadre des analyses trimestrielles des vulnérabilités et celles qui relèvent de la responsabilité des clients du MSP pour être incluses dans leurs propres analyses trimestrielles.

4. Coordonnées et date du rapport

Inclure :

- les coordonnées du commerçant ou prestataire de services, et de l'évaluateur ;
- la période de l'évaluation – spécifier la durée et la période à laquelle l'évaluation a eu lieu ;
- date du rapport.

5. Résultats des analyses trimestrielles

- Résumer les quatre résultats des analyses trimestrielles les plus récentes dans le Résumé ainsi que dans les commentaires indiqués dans la condition 11.2.

  Remarque : *quatre analyses trimestrielles réussies ne sont pas obligatoires pour l'attestation de conformité PCI DSS initiale, si l'évaluateur vérifie que :*

  1) *l'analyse la plus récente a été réussie,*
  2) *l'entreprise possède des politiques et procédures documentées exigeant des analyses trimestrielles en progrès,*
  3) *il a été remédié à toutes les vulnérabilités notées au cours de l'analyse initiale, fait démontré par une nouvelle analyse.*

  Pendant les années qui suivent la vérification PCI DSS initiale, quatre analyses trimestrielles réussies ont été réalisées.

- L'analyse doit couvrir toutes les adresses IP accessibles depuis l'extérieur (par Internet) qui existent au sein de l'entité, conformément au *Guide de programme des prestataires de services d'analyse (ASV) PCI.*

6. Conclusions et observations

Récapituler dans la section Résumé toutes les conclusions qui ne pourraient pas être consignées dans le Rapport sur la conformité standard.

Tous les évaluateurs *doivent :*

- se référer au modèle intitulé Conditions et procédures d'évaluation de sécurité détaillées de la norme PCI DSS pour consigner dans le rapport des descriptions et des conclusions détaillées sur chaque condition et sous-condition ;
- s'assurer que toutes les réponses S.O ont été clairement expliquées ;
- passer en revue et documenter tous les contrôles compensatoires envisagés pour conclure qu'un contrôle est bien en place.

Pour plus d'informations sur les « contrôles compensatoires », consulter la section Contrôles compensatoires ci-dessus et *les annexes B* et *C*.

Revalidation des éléments en instance

Un rapport « contrôles en place » est requis pour vérifier la conformité. Le rapport est considéré non conforme s'il contient des « éléments en instance », ou des éléments qui seront complétés ultérieurement. Le commerçant/prestataire de services doit résoudre ces questions avant que la validation puisse être achevée. Une fois ces points résolus par le commerçant/prestataire de services, l'évaluateur doit procéder de nouveau à l'évaluation afin de valider la résolution et vérifier que toutes les conditions sont satisfaites. Après cette nouvelle validation, l'évaluateur génèrera

un nouveau Rapport sur la conformité, en vérifiant que l'environnement des données des titulaires de cartes est parfaitement conforme, et il soumettra ce rapport conformément aux instructions (décrites ci-dessous).

Étapes de mise en conformité avec la norme PCI DSS

1. Compléter le Rapport sur la conformité (ROC) conformément aux instructions décrites précédemment dans la section « Instructions et contenu du Rapport sur la conformité ».
2. S'assurer que les analyses des vulnérabilités ont été réalisées avec succès par un prestataire de services d'analyse agréé (ASV, Approved Scanning Vendor) par PCI SSC et se procurer auprès de ce dernier la preuve de l'exécution réussie de ces analyses.
3. Compléter l'intégralité de l'attestation de conformité, pour les prestataires de services ou les commerçants, selon le cas. Les attestations de conformité sont disponibles sur le site Web du PCI SSC (www.pcisecuritystandards.org).
4. Envoyer le Rapport sur la conformité, la preuve de l'analyse réussie et l'Attestation de conformité, ainsi que toute autre documentation requise, à l'acquéreur (dans le cas de commerçants), à la marque de carte de paiement ou à tout autre demandeur (dans le cas de prestataires de services).

Conditions et procédures d'évaluation de sécurité détaillées de la norme PCI DSS

Les informations suivantes définissent les en-têtes des colonnes du tableau *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS* :

- **Conditions de la norme PCI DSS** – Cette colonne définit la norme DSS (Data Security Standard) et indique les conditions à satisfaire pour se mettre en conformité avec la norme PCI DSS. La conformité sera validée au regard de ces conditions.
- **Procédures de test** – Cette colonne indique les processus que l'évaluateur doit suivre pour valider que les conditions de la norme PCI DSS sont « en place ».
- **En place** – L'évaluateur doit se référer à cette colonne pour donner une brève description des contrôles validés comme étant « en place » pour chaque condition, y compris celle des contrôles déterminés comme en place à la suite de contrôles compensatoires, ou en raison d'une condition « sans objet ».

  Remarque : *cette colonne ne doit pas être utilisée pour les éléments qui ne sont pas encore en place ou pour les éléments en instance à compléter ultérieurement.*
- Pas en place **– L'évaluateur doit se référer à cette colonne pour donner une brève description des contrôles qui ne sont pas en place. Notez qu'un rapport non conforme ne doit pas être envoyé à une marque de carte de paiement ou à l'acquéreur à moins que celui-ci n'en ait fait la demande explicite. Consulter les attestations de conformité disponibles sur le site Web du PCI SSC (www.pcisecuritystandards.org), pour y trouver davantage d'instructions sur les rapports non conformes.**
- **Date cible/Commentaires** – Pour les contrôles qui ne sont « pas en place », l'évaluateur peut préciser la date cible à laquelle le commerçant ou le prestataire de services doivent avoir les contrôles « en place ». Les remarques ou commentaires éventuels peuvent être portés ici.

Création et gestion d'un réseau sécurisé

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

Les pare-feu sont des dispositifs qui contrôlent le trafic autorisé entre le réseau d'une entreprise (interne) et les réseaux non approuvés (externes), ainsi que le trafic entrant et sortant dans des zones plus sensibles du réseau approuvé interne d'une société. L'environnement des données des titulaires de cartes est un exemple de zone plus sensible au sein du réseau approuvé d'une entreprise.

Un pare-feu examine l'ensemble du trafic réseau et bloque les transmissions qui ne satisfont pas aux critères de sécurité définis.

Tous les systèmes doivent être protégés contre les accès non autorisés depuis un réseau non approuvé, que ce soit en entrée via Internet (par exemple e-commerce, accès des employés à Internet à partir de leurs navigateurs, accès des employés à la messagerie électronique, connexions dédiées telles que les connexions interentreprises) ou bien via les réseaux sans fil ou d'autres sources. Les chemins d'accès de/vers des réseaux non approuvés, en apparence insignifiants, peuvent souvent constituer des chemins d'accès non protégés à des systèmes critiques. Les pare-feu sont des mécanismes de protection essentiels sur tout réseau informatique.

D'autres composants du système peuvent assurer une fonctionnalité pare-feu, à condition de remplir les conditions minimum des pare-feu indiquées dans la condition 1. Lorsque d'autres composants du système sont utilisés dans l'environnement des données de titulaires de cartes pour assurer une fonctionnalité pare-feu, ces dispositifs doivent être inclus dans le champ d'application de l'évaluation de la condition 1.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
1.1Définir des normes de configuration des pare-feu et des routeurs incluant les éléments suivants :	**1.1**Obtenir et vérifier les normes de configuration des pare-feu et des routeurs et autres documents spécifiés ci-dessous pour vérifier que les normes sont bien satisfaites. Procéder comme suit :			
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	**1.1.1**Vérifier qu'un processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs est en place.			
1.1.2 Schéma de réseau actuel indiquant toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil	**1.1.2.a** Vérifier qu'il existe un schéma de réseau actuel (par exemple, illustrant les flux des données des titulaires de cartes) et que celui-ci indique toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil.			
	1.1.2.bVérifier que le schéma est tenu à jour.			
1.1.3 Exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne	**1.1.3.a** Vérifier que les normes de configuration des pare-feu comprennent l'exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée et la zone de réseau Internet.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	1.1.3.b Vérifier que le schéma de réseau actuel est conforme aux normes de configuration des pare-feu.			
1.1.4 Description des groupes, des rôles et des responsabilités pour la gestion logique des composants réseau	**1.1.4** Vérifier que les normes de configuration des pare-feu et des routeurs comprennent la description des groupes, des rôles et des responsabilités pour la gestion logique des composants réseau.			
1.1.5 Documentation et justification professionnelle de l'utilisation de tous les services, protocoles et ports autorisés, y compris la documentation des fonctions de sécurité mises en œuvre pour les protocoles considérés comme étant non sécurisés. Les protocoles FTP, Telnet, POP3, IMAP et SNMP sont des exemples de services, protocoles ou ports non sécurisés, mais ne sont pas les seuls.	**1.1.5.a** Vérifier que les normes de configuration des pare-feu et des routeurs comprennent la liste documentée des services, protocoles et ports nécessaires à la conduite des activités de l'entreprise, par exemple les protocoles HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer), SSH (Secure Shell) et VPN (Virtual Private Network).			
	1.1.5.b Identifier les services, les protocoles et les ports non sécurisés autorisés, et vérifier qu'ils sont nécessaires et que les fonctions de sécurité sont documentées et mises en œuvre en examinant les normes de configuration des pare-feu et des routeurs ainsi que les paramètres de chaque service.			
1.1.6 Nécessité d'examiner les règles des pare-feu et des routeurs au moins tous les six mois	**1.1.6.a** Vérifier que les normes de configuration des pare-feu et des routeurs exigent l'examen des règles des pare-feu et des routeurs au moins tous les six mois.			
	1.1.6.b Obtenir et examiner la documentation pour vérifier que les règles sont passées en revue au moins tous les six mois.			
1.2 Créer une configuration de pare-feu qui limite les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données des titulaires de cartes. ***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** Examiner les configurations des pare-feu et des routeurs pour vérifier que les connexions entre les réseaux non approuvés et les composants du système dans l'environnement des données des titulaires de cartes sont restreintes comme suit :			
1.2.1 Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données des titulaires de cartes.	**1.2.1.a** Vérifier que le trafic entrant et sortant est limité au trafic nécessaire à l'environnement des données des titulaires de cartes et que les restrictions sont documentées.			
	1.2.1.b Vérifier que tous les autres trafics entrants et sortants sont			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	explicitement refusés, par exemple à l'aide d'une instruction « refuser tout » explicite ou d'un refus implicite après une instruction d'autorisation.			
1.2.2 Sécuriser et synchroniser les fichiers de configuration des routeurs.	**1.2.2** Vérifier que les fichiers de configuration des routeurs sont sécurisés et synchronisés. Par exemple, les fichiers de configuration d'exécution (utilisés pour l'exécution normale des routeurs) et les fichiers de configuration de démarrage (utilisés au redémarrage des machines) ont les mêmes configurations sécurisées.			
1.2.3 Installer des pare-feu de périmètre entre tous les réseaux sans fil et l'environnement des données des titulaires de cartes, et configurer ces pare-feu pour refuser ou contrôler le trafic (si celui-ci est nécessaire à des fins professionnelles) de l'environnement sans fil vers l'environnement des données des titulaires de cartes.	**1.2.3** Vérifier que des pare-feu de périmètre sont installés entre tous les réseaux sans fil et les systèmes stockant les données des titulaires de cartes, et que ceux-ci refusent ou contrôlent le trafic (si celui-ci est nécessaire à des fins professionnelles) de l'environnement sans fil vers l'environnement des données des titulaires de cartes.			
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** Examiner les configurations des pare-feu et des routeurs – y compris sans s'y limiter, le routeur interne (parfois appelé « choke router ») au niveau d'Internet, le routeur et le pare-feu DMZ, le segment DMZ des titulaires de cartes, le routeur du périmètre et le segment du réseau interne des titulaires de cartes – afin de déterminer qu'il n'existe aucun accès direct entre Internet et les composants du système dans le segment du réseau interne des titulaires de cartes, comme décrit en détails ci-dessous.			
1.3.1 Déployer une zone démilitarisée pour limiter le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public.	**1.3.1** Vérifier qu'une zone démilitarisée est déployée pour limiter le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public.			
1.3.2 Limiter le trafic Internet entrant aux adresses IP dans la zone démilitarisée.	**1.3.2** Vérifier que le trafic Internet entrant est limité aux adresses IP dans la zone démilitarisée.			
1.3.3 N'autoriser aucune connexion directe entrante ou sortante de trafic entre Internet et l'environnement des	**1.3.3** Vérifier qu'aucune connexion directe entrante ou sortante n'est autorisée pour le trafic entre Internet et l'environnement des données des titulaires de cartes.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
données des titulaires de cartes.				
1.3.4 Ne pas autoriser le passage des adresses internes d'Internet dans la zone démilitarisée.	**1.3.4** Vérifier que les adresses internes ne peuvent pas passer d'Internet dans la zone démilitarisée**.**			
1.3.5 Ne pas autoriser le trafic sortant non autorisé de l'environnement des données des titulaires de cartes vers Internet.	**1.3.5** Vérifier que le trafic sortant de l'environnement des données des titulaires de cartes vers Internet est expressément autorisé.			
1.3.6 Implémenter le contrôle avec état, également appelé « filtrage des paquets dynamique » (seules les « connexions établies » sont autorisées sur le réseau).	**1.3.6** Vérifier que le pare-feu effectue un contrôle avec état (filtrage des paquets dynamique) (seules les connexions établies doivent être autorisées, et seulement si elles sont associées à une session précédemment établie).			
1.3.7 Placer les composants du système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone de réseau interne, isolée de la zone démilitarisée et des autres réseaux non approuvés.	**1.3.7** Vérifier que les composants du système qui stockent les données de titulaires de cartes se trouvent dans une zone de réseau interne, isolée de la zone démilitarisée et des autres réseaux non approuvés.			
1.3.8 Ne pas divulguer les adresses IP et les informations d'acheminement confidentielles à des tiers non autorisés. ***Remarque :*** *Voici quelques exemples de méthodes pour dissimuler les*	**1.3.8.a** Vérifier que des moyens sont en place pour prévenir la divulgation d'adresses IP et d'informations d'acheminement confidentielles des réseaux internes sur Internet.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
adresses IP : ▪ *traduction d'adresse réseau (Network Address Translation – NAT) ;* ▪ *protéger les serveurs contenant des données de titulaires de cartes derrière des serveurs proxy/pare-feu ou des caches de contenu ;* ▪ *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.*	**1.3.8.b** Vérifier que toute divulgation d'adresses IP et d'informations d'acheminement confidentielles à des entités externes est autorisée.			
1.4 Installer un logiciel pare-feu personnel sur tout ordinateur portable et/ou ordinateur appartenant à un employé équipé d'une connexion directe à Internet (par exemple, ordinateurs portables utilisés par les employés), qui est utilisé pour accéder au réseau de l'entreprise.	**1.4.a** Vérifier qu'un logiciel pare-feu personnel est installé et activé sur les ordinateurs portables et/ou les ordinateurs appartenant aux employés équipés d'une connexion directe à Internet (par exemple, ordinateurs portables utilisés par les employés), qui sont utilisés pour accéder au réseau de l'entreprise.			
	1.4.b Vérifier que le logiciel pare-feu personnel est configuré par l'entreprise selon des normes spécifiques et que cette configuration ne peut pas être modifiée par les utilisateurs d'ordinateurs portables.			

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

Les individus malveillants (à l'intérieur ou à l'extérieur d'une entreprise), utilisent souvent les mots de passe et autres paramètres par défaut du fournisseur pour s'infiltrer dans les systèmes en vue de les endommager. Ces mots de passe et paramètres sont bien connus des communautés de pirates et sont facilement détectables à partir d'informations publiques.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
2.1 Changer systématiquement les paramètres par défaut définis par le fournisseur **avant** d'installer un système sur le réseau ; par exemple, inclure des mots de passe et des chaînes de communauté SNMP (Simple Network Management Protocol), et éliminer les comptes qui ne sont pas nécessaires.	**2.1** Choisir un échantillon de composants du système et essayer de se connecter (avec l'aide de l'administrateur système) aux périphériques avec les comptes et mots de passe définis par défaut par le fournisseur, afin de vérifier que ceux-ci ont bien été changés (Se référer aux manuels du fournisseur et aux sources disponibles sur Internet pour rechercher les comptes/mots de passe définis par le fournisseur).			
2.1.1 Pour les environnements sans fil connectés à l'environnement des données des titulaires de cartes ou la transmission de données des titulaires de cartes, modifier les paramètres par défaut définis par le fournisseur des équipements sans fil, notamment les mots de passe, les chaînes de communauté SNMP et les clés de cryptage sans fil par défaut.	**2.1.1** Vérifier les points suivants, concernant les paramètres par défaut du fournisseur pour les environnements sans fil :			
	2.1.1.a Vérifier que les clés de cryptage par défaut ont été modifiées à l'installation et qu'elles sont changées à chaque fois qu'un employé qui les connaît quitte l'entreprise ou change de poste.			
	2.1.1.b Vérifier que les chaînes de communauté SNMP par défaut sur les périphériques sans fil ont été modifiées.			
	2.1.1.c Vérifier que les mots de passe/locutions de passage par défaut des points d'accès ont été modifiés.			
	2.1.1.d Vérifier que le firmware des périphériques sans fil est mis à jour de manière à prendre en charge un cryptage robuste pour l'authentification et la transmission sur les réseaux sans fil.			
	2.1.1.e Vérifier que les autres paramètres par défaut liés à la sécurité, définis par le fournisseur des équipements sans fil, ont été changés, le cas échéant.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
2.2 Élaborer des normes de configuration pour tous les composants du 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)	**2.2.a** Examiner les normes de configuration du système de l'organisation pour tous les types de composants du système et vérifier que ces normes sont compatibles avec les normes de renforcement en vigueur dans le secteur.			
	2.2.b Vérifier que les normes de configuration du système sont mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités, comme indiqué dans la condition 6.2.			
	2.2.c Vérifier que les normes de configuration du système sont appliquées lorsque de nouveaux systèmes sont configurés.			
	2.2.d Vérifier que les normes de configuration du système comprennent chaque élément indiqué ci-dessous (aux points 2.2.1 – 2.2.4).			
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 principale par composant de système virtuel.*	**2.2.1.a** Sur un échantillon de composants du système, vérifier qu'une seule fonction principale par serveur est implémentée.			
	2.2.1.b Si des technologies de virtualisation sont utilisées, vérifier que seule une fonction principale est déployée par composant de système ou dispositif virtuels.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
2.2.2 N'activer que les services, protocoles, démons, etc., nécessaires et sécurisés pour le fonctionnement du système. Mettre en œuvre les fonctions de sécurité pour tout service, protocole ou démon nécessaires et considérés comme non sécurisés, par exemple, utiliser des technologies sécurisées du type SSH, S-FTP, SSL ou IPSec VPN, pour protéger les services non sécurisés comme NetBIOS, le partage de fichiers, Telnet, FTP, etc.	**2.2.2.a** Sur un échantillon de composants du système, examiner les démons, les protocoles et les services activés du système. Vérifier que seuls les services ou protocoles nécessaires sont activés.			
	2.2.2.b Identifier tous services, démons ou protocoles activés et non sécurisés. Vérifier que leur utilisation se justifie et que des fonctions de sécurité sont documentées et déployées.			
2.2.3 Configurer les paramètres de sécurité du système pour empêcher les actes malveillants.	**2.2.3.a** Interroger les administrateurs système et/ou les responsables de la sécurité pour vérifier qu'ils connaissent les paramètres de sécurité courants des composants du système.			
	2.2.3.b Vérifier que les paramètres de sécurité courants sont inclus dans les normes de configuration du système.			
	2.2.3.c Sur un échantillon de composants du système, vérifier que les paramètres de sécurité courants sont correctement définis.			
2.2.4 Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus.	**2.2.4.a** Sur un échantillon de composants du système, vérifier que toutes les fonctionnalités qui ne sont pas nécessaires (par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers, etc.) sont supprimées.			
	2.2.4.b. Vérifier que les fonctions activées sont documentées et prennent en charge une configuration sécurisée.			
	2.2.4.c. Vérifier que seule la fonctionnalité documentée est présente sur les composants de système échantillonnés.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
2.3 Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste. Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion sur le Web et autres accès administratifs non-console.	**2.3** Sur un échantillon de composants du système, s'assurer que l'accès administratif non-console est crypté en :			
	2.3.a Observant un administrateur se connecter à chaque système pour vérifier qu'une méthode de cryptage robuste est appelée avant que l'administrateur ne soit invité à taper son mot de passe.			
	2.3.b Passant en revue les services et les fichiers de paramètres sur les systèmes pour déterminer que Telnet et d'autres commandes de connexion à distance ne sont pas disponibles pour un usage interne.			
	2.3.c Vérifiant que l'accès administrateur aux interfaces de gestion Web est crypté au moyen d'une méthode de cryptage robuste.			
2.4 Les fournisseurs d'hébergement partagé doivent protéger l'environnement hébergé et les données des titulaires de cartes de chaque entité. Ces fournisseurs doivent satisfaire aux exigences spécifiques décrites dans *l'Annexe A : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.*	**2.4** Exécuter les procédures de test **A.1.1** à **A.1.4** décrites dans *l'Annexe A : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé* pour l'évaluation PCI DSS des fournisseurs d'hébergement partagé, afin de vérifier que les fournisseurs d'hébergement partagé protègent l'environnement hébergé et les données de leurs entités (commerçants et prestataires de services).			

Protection des données des titulaires de cartes de crédit

Condition 3 : Protéger les données de titulaires de cartes stockées

Les méthodes de protection, telles que le cryptage, la troncature, le masquage et le hachage, sont des composants stratégiques de la protection des données des titulaires de cartes. Si un intrus parvient à contourner les autres contrôles de sécurité et à accéder aux données cryptées, il ne pourra pas les lire ni les utiliser s'il n'a pas les clés cryptographiques appropriées. D'autres méthodes efficaces de protection des données stockées doivent être envisagées pour limiter les risques. Par exemple, pour minimiser les risques, éviter de stocker les données des titulaires de cartes à moins que cela ne soit absolument nécessaire, tronquer les données des titulaires de cartes si un PAN complet n'est pas requis et éviter d'envoyer un PAN non protégé par les technologies pour utilisateur final, comme les e-mails ou les messageries instantanées.

Pour obtenir la définition d'une « cryptographie robuste » et d'autres termes relatifs à PCI DSS, consulter le *Glossaire des termes, abréviations et acronymes PCI DSS.*

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
3.1 Garder le stockage de données de titulaires de cartes à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données, comme suit.	**3.1** Obtenir et passer en revue les politiques et procédures et processus de l'entreprise relatifs à la conservation et l'élimination des données, et procéder comme suit :			
3.1.1 Appliquer une politique de conservation et d'élimination des données qui comprenne : ▪ la limitation de la quantité de données stockées et du délai de conservation restreints aux obligations professionnelles, légales et réglementaires ; ▪ des processus pour l'élimination sécurisée des données devenues inutiles ; ▪ des conditions de conservation	**3.1.1.a** Vérifier que les politiques et les procédures comprennent des dispositions légales, réglementaires et professionnelles sur la conservation des données, notamment des conditions spécifiques sur la conservation des données des titulaires de cartes (par exemple, ces données doivent être conservées pendant une période X pour des raisons professionnelles Y) ;			
	3.1.1.b Vérifier que les politiques et les procédures comprennent des dispositions sur l'élimination des données qui ne sont plus requises à des fins légales, réglementaires ou professionnelles, notamment la suppression des données des titulaires de cartes.			
	3.1.1.c Vérifier que les politiques et procédures couvrent l'ensemble du stockage de données de titulaires de cartes.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
spécifiques pour les données de titulaires de cartes ; ▪ un processus trimestriel automatique ou manuel pour l'identification et l'élimination sécurisée des données de titulaires de cartes stockées excédant les conditions de conservation définies.	**3.1.1.d** Vérifier que toutes les politiques et procédures comprennent au moins un des éléments suivants : Un processus programmé (automatique ou manuel) pour supprimer, au moins une fois par trimestre, les données de titulaires de cartes stockées, excédant les conditions définies dans la politique de conservation des données. L'obligation d'une vérification, au moins trimestrielle, afin de contrôler que les données de titulaires de cartes stockées n'excèdent pas les conditions définies dans la politique de conservation des données.			
	3.1.1.e Sur un échantillon de composants de système stockant des données de titulaires de cartes, vérifier que les données stockées n'excèdent pas les conditions définies dans la politique de conservation des données.			
3.2 Ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée). Les données concernées sont mentionnées dans les conditions 3.2.1 à 3.2.3 suivantes : ***Remarque :*** *les émetteurs et les sociétés qui prennent en charge les services d'émissions peuvent stocker des données d'authentification sensibles si ceci est justifié du point de vue professionnel et que ces données sont stockées de manière sécurisée.*	**3.2.a** Dans le cas des émetteurs et des sociétés qui prennent en charge les services d'émission et stockent des données d'authentification sensibles, vérifier que ce stockage est justifié du point de vue professionnel et que ces données sont protégées.			
	3.2.b Pour toutes les autres entités, si des données d'authentification sensibles sont reçues et supprimées, obtenir et passer en revue les processus de suppression des données pour vérifier que ces dernières sont irrécupérables.			
	3.2.c Pour chaque élément de données d'authentification sensibles ci-dessous, procéder comme suit :			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
3.2.1 Ne jamais stocker la totalité du contenu d'une quelconque piste (sur la bande magnétique au verso d'une carte, sur une puce ou ailleurs). Ces données sont également appelées 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.*	**3.2.1** Sur un échantillon de composants du système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que la totalité du contenu d'une quelconque piste de la bande magnétique au verso d'une carte ou sur une puce, n'est en aucun cas stockée : ▪ les données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ les fichiers d'historique ; ▪ les fichiers trace ; ▪ plusieurs schémas de bases de données ; ▪ le contenu des bases de données.			
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.	**3.2.2** Sur un échantillon de composants du système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que le code ou la valeur de vérification de carte à trois ou quatre chiffres figurant au recto de la carte de paiement, ou dans l'espace réservé à la signature, (données CVV2, CVC2, CID, CAV2) n'est en aucun cas stocké : ▪ les données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ les fichiers d'historique ; ▪ les fichiers trace ; ▪ plusieurs schémas de bases de données ; ▪ le contenu des bases de données.			
3.2.3 Ne pas stocker de code PIN (Personal Identification Number) ni de bloc PIN crypté.	**3.2.3** Sur un échantillon de composants du système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que les codes et blocs PIN cryptés ne sont en			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	aucun cas stockés : ▪ les données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ les fichiers d'historique ; ▪ les fichiers trace ; ▪ plusieurs schémas de bases de données ; ▪ le contenu des bases de données.			
3.3 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés). ***Remarques :*** ▪ *cette condition ne s'applique pas aux employés et autres parties qui ont un besoin professionnel légitime 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 des titulaires de cartes, par exemple, pour les reçus des points de vente (POS).*	**3.3** Obtenir et examiner les politiques écrites, et passer en revue l'affichage des PAN (par exemple, à l'écran, sur les reçus papier) afin de vérifier que les numéros de comptes principaux (PAN) sont masqués lors de l'affichage des données des titulaires de cartes, sauf pour les utilisateurs qui ont un besoin professionnel légitime de voir l'intégralité du PAN.			
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 forte (la totalité du PAN doit être haché) ; ▪ troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ; ▪ des tokens et pads d'index (les pads	**3.4.a** Obtenir et passer en revue la documentation relative au système utilisé pour protéger le PAN, notamment le fournisseur, le type de système/processus et les algorithmes de cryptage (le cas échéant). Vérifier que le PAN est rendu illisible à l'aide de l'une des méthodes suivantes : ▪ hachage unilatéral s'appuyant sur une méthode cryptographique robuste ; ▪ une troncature ; ▪ tokens et pads d'index, les pads devant être stockés de manière sécurisée ; ▪ cryptographie robuste associée à des processus et des procédures de gestion des clés.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
doivent être stockés de manière sécurisée) ; ▪ cryptographie robuste associée à des processus et des 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 hachée et tronquée du même PAN sont présentes dans l'environnement de l'entreprise, des contrôles supplémentaires doivent être en place pour garantir que les versions hachée et tronquée ne peuvent pas être corrélées pour reconstituer le PAN d'origine.*	**3.4.b** Examiner plusieurs tables ou fichiers d'un échantillon de référentiels de données afin de vérifier que le PAN est rendu illisible (en d'autres termes, qu'il n'est pas stocké en texte clair).			
	3.4.c Examiner un échantillon de support amovible (par exemple, bandes de sauvegarde) pour s'assurer que le PAN est rendu illisible.			
	3.4.d Examiner un échantillon des journaux d'audit pour confirmer que le PAN est bien illisible ou supprimé des journaux.			
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 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). Les clés de décryptage ne doivent pas être liées à des comptes d'utilisateur.	**3.4.1.a** Si un cryptage par disque est utilisé, vérifier que l'accès logique aux systèmes de fichiers cryptés est implémenté par le biais d'un mécanisme indépendant des mécanismes des systèmes d'exploitation natifs (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales).			
	3.4.1.b Vérifier que les clés cryptographiques sont stockées de manière sécurisée (par exemple, sur des supports amovibles correctement protégés avec des contrôles d'accès stricts).			
	3.4.1.c Vérifier que les données des titulaires de cartes sur les supports amovibles sont cryptées où qu'elles soient stockées. ***Remarque :*** *si le cryptage de disque n'est pas utilisé pour crypter les supports amovibles, les données stockées sur ce support devront être rendues illisibles par une autre méthode.*			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
3.5 Protéger les clés utilisées pour protéger les données de titulaires de cartes de la divulgation et de l'utilisation illicites : ***Remarque :*** *cette exigence s'applique également aux clés de cryptage de clés 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*.	**3.5** Vérifier les processus de protection des clés de cryptage utilisées pour le cryptage des données des titulaires de cartes contre la divulgation et l'utilisation illicite en procédant comme suit :			
3.5.1 Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible.	**3.5.1** Passer en revue les listes d'accès utilisateur afin de vérifier que l'accès aux clés est restreint aux opérateurs strictement nécessaires.			
3.5.2 Stocker les clés cryptographiques de manière sécurisée dans aussi peu d'emplacements et de formes que possible.	**3.5.2.a** Passer en revue les fichiers de configuration des systèmes pour vérifier que les clés sont stockées dans un format crypté et que les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données.			
	3.5.2.b Identifier les emplacements de stockage des clés pour vérifier que celles-ci sont stockées dans aussi peu d'endroits et sous aussi peu de formes que possible.			
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 le NIST, à l'adresse suivante : http://csrc.nist.gov.*	**3.6.a** Vérifier l'existence de procédures de gestion des clés pour les clés de cryptage des données de titulaires de cartes.			
	3.6.b Pour les prestataires de services seulement : si le prestataire de services partage des clés avec ses clients pour la transmission de données de titulaires de cartes, vérifier qu'il leur fournit la documentation nécessaire avec les instructions sur la manière de sécuriser la transmission, le stockage et la mise à jour des clés conformément aux conditions 3.6.1 à 3.6.8 ci-dessous.			
	3.6.c Passer en revue les procédures de gestion des clés et procéder comme suit :			
3.6.1 Génération de clés cryptographiques robustes	**3.6.1** Vérifier que des procédures de gestion des clés sont mises en œuvre pour la production de clés robustes.			
3.6.2 Sécuriser la distribution des clés cryptographiques	**3.6.2** Vérifier que des procédures de gestion des clés sont mises en œuvre pour une distribution de clés sécurisée.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
3.6.3 Sécuriser le stockage des clés cryptographiques	**3.6.3** Vérifier que des procédures de gestion des clés sont mises en œuvre pour le stockage de clés sécurisé.			
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).	**3.6.4** Vérifier que des procédures de gestion de clés sont mises en œuvre pour appliquer les changements de clés périodiques à la fin de la cryptopériode définie.			
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.*	**3.6.5.a** Vérifier que des procédures de gestion des clés sont mises en œuvre pour supprimer les clés lorsque leur intégrité a été affaiblie.			
	3.6.5.b Vérifier que des procédures de gestion des clés sont mises en œuvre pour requérir le remplacement des clés soupçonnées d'avoir été compromises, ou si ce fait est avéré.			
	3.6.5.c Si des clés cryptographiques retirées ou remplacées sont conservées, vérifier qu'elles ne sont pas utilisées pour des opérations de cryptage.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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 (par exemple, exigeant deux ou trois personnes, chacune connaissant uniquement sa propre fraction de la clé, pour reconstituer la clé entière). ***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.*	**3.6.6** Vérifier que les procédures de gestion manuelle de clés en texte clair exigent un fractionnement des connaissances et un double contrôle.			
3.6.7 Prévenir la substitution non autorisée des clés cryptographiques.	**3.6.7** Vérifier que des procédures de gestion des clés sont mises en œuvre pour empêcher la substitution non autorisée des clés.			
3.6.8 Exiger des opérateurs chargés de la gestion de clés cryptographiques qu'ils reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités.	**3.6.8** Vérifier que des procédures de gestion des clés sont mises en œuvre pour exiger des opérateurs chargés de la gestion de clés cryptographiques qu'ils reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités.			

Condition 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts

Les informations sensibles doivent être cryptées pendant leur transmission sur des réseaux accessibles à des individus malveillants. Les réseaux sans fil mal configurés et les vulnérabilités dans les protocoles traditionnels de cryptage et d'authentification sont les cibles permanentes des individus malveillants qui profitent de ces faiblesses pour obtenir un accès privilégié aux environnements des données des titulaires de cartes.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
4.1 Utiliser des protocoles de sécurité et de cryptographie robustes (par exemple, SSL/TLS, IPSEC, SSH, etc.) afin de protéger les données sensibles des titulaires de cartes durant la transmission sur des réseaux publics ouverts. *Voici quelques exemples de réseaux publics ouverts couverts par la norme PCI DSS :* ▪ Internet ▪ technologies sans fil ▪ communications GSM (Global System for Mobile) ▪ GPRS (General Packet Radio Service)	**4.1** Vérifier l'utilisation de protocoles sécurisés chaque fois que les données des titulaires de cartes sont transmises ou reçues sur des réseaux publics ouverts. Vérifier qu'un cryptage robuste est utilisé pendant la transmission des données, comme suit :			
	4.1.a À la réception de transactions, choisir un échantillon et examiner les transactions pendant qu'elles s'exécutent afin de vérifier que les données des titulaires de cartes sont cryptées pendant le transfert.			
	4.1.b Vérifier que seuls des clés/certificats approuvés sont acceptés.			
	4.1.c Vérifier que le protocole est déployé de manière à n'utiliser que des configurations sécurisées et qu'il ne prend en charge aucune version ni configuration non sécurisées.			
	4.1.d Vérifier que le niveau de cryptage approprié est mis en œuvre pour la méthodologie de cryptage employée (Vérifier les recommandations/meilleures pratiques du fournisseur).			
	4.1.e Pour les implémentations SSL/TLS : ▪ vérifier que la mention HTTPS apparaît dans l'adresse URL (Universal Record Locator) dans le navigateur ; ▪ vérifier qu'aucune donnée de titulaires de cartes n'est requise lorsque la mention HTTPS n'apparaît pas dans l'URL.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
4.1.1 S'assurer que les réseaux sans fil sur lesquels sont transmises les données des titulaires de cartes ou qui sont connectés à l'environnement des données des titulaires de cartes mettent en œuvre les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste pour l'authentification et la transmission. ***Remarque :*** *l'utilisation du protocole WEP comme contrôle de sécurité est interdit depuis le 30 juin 2010.*	**4.1.1** Pour les réseaux sans fil sur lesquels sont transmises les données des titulaires de cartes ou qui sont connectés à l'environnement des données des titulaires de cartes, vérifier que les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont mises en œuvre pour appliquer un cryptage robuste pour l'authentification et la transmission.			
4.2 Ne jamais envoyer de PAN non protégé à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple e-mail, messagerie instantanée, chat).	**4.2.a** Vérifier que le PAN est rendu illisible ou protégé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie pour les utilisateurs finaux.			
	4.2.b Vérifier l'existence d'une politique interdisant la transmission de PAN non protégés à l'aide de technologies de messagerie pour les utilisateurs finaux.			

Gestion d'un programme de gestion des vulnérabilités

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

Des logiciels malicieux, généralement appelés « programmes malveillants », par exemple virus, vers et chevaux de Troie, sont infiltrés dans le réseau dans le cadre d'activités professionnelles approuvées, notamment l'échange d'e-mails et l'accès à Internet des employés ainsi que l'utilisation de périphériques de stockage et d'ordinateurs portables. Les vulnérabilités des systèmes peuvent alors être exploitées à des fins malveillantes. Des logiciels antivirus doivent être installés sur tous les systèmes régulièrement affectés par des programmes malveillants afin de les protéger contre les menaces logicielles actuelles et futures.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
5.1 Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).	**5.1** Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que des logiciels antivirus sont déployés et, le cas échéant, qu'une technologie de protection antivirus est en place.			
5.1.1 S'assurer que tous les programmes antivirus sont capables de détecter et d'éliminer tous les types de logiciels malveillants connus, et de constituer une protection efficace contre ce fléau.	**5.1.1** Sur un échantillon de composants du système, vérifier que tous les programmes antivirus détectent et éliminent tous les types de logiciels malveillants connus (par exemple, virus, chevaux de Troie, vers, spyware, adware et dissimulateurs d'activités), et constituent une protection efficace contre ces fléaux.			
5.2 S'assurer que tous les mécanismes antivirus sont à jour, en cours d'exécution et génèrent des journaux d'audit.	**5.2** Vérifier que tous les logiciels antivirus sont à jour, en cours d'exécution et génèrent des journaux en procédant comme suit :			
	5.2.a Obtenir et passer en revue la politique, et vérifier qu'elle stipule la mise à jour des logiciels antivirus et des définitions de virus.			
	5.2.b Vérifier que l'installation principale du logiciel est configurée pour la mise à jour automatique et l'exécution d'analyses à intervalles réguliers.			
	5.2.c Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que les mises à jour automatiques et les analyses à intervalles réguliers sont activées.			

	5.2.d Sur un échantillon de composants du système, vérifier que la génération des journaux des logiciels antivirus est activée et que ceux-ci sont conservés conformément à la condition 10.7 de la norme PCI DSS.			

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

Des individus sans scrupules peuvent exploiter les points faibles de la sécurité pour obtenir un accès privilégié aux systèmes. Bon nombre de ces vulnérabilités sont résolues par les correctifs de sécurité développés par les fournisseurs. Ceux-ci doivent être installés par les entités chargées de la gestion des systèmes. Tous les systèmes stratégiques doivent être dotés des correctifs logiciels appropriés les plus récents afin d'empêcher l'exploitation et l'altération des données des titulaires de cartes par des individus et des logiciels malveillants.

Remarque : *Les correctifs logiciels appropriés sont ceux qui ont été suffisamment évalués et testés pour déterminer qu'ils ne présentent aucun conflit avec les configurations de sécurité existantes. De nombreuses vulnérabilités peuvent être évitées dans les applications développées en interne grâce à l'utilisation de processus de développement système standard et de techniques de codage sécurisées.*

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
6.1 S'assurer que tous les logiciels et les composants du système sont dotés des derniers correctifs de sécurité développés par le fournisseur, afin de les protéger des vulnérabilités connues. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation. ***Remarque :*** *une entreprise peut envisager la mise en œuvre d'une approche en fonction du risque pour définir la priorité des correctifs à installer. Par exemple, en accordant aux infrastructures stratégiques (par exemple, bases de données, périphériques et systèmes orientés public) une priorité supérieure à celle des périphériques internes moins cruciaux, de sorte que les systèmes et les périphériques hautement prioritaires soient traités dans un délai d'un mois, tandis que les périphériques et systèmes moins stratégiques le soient dans un délai de trois mois.*	**6.1.a** Sur un échantillon de composants du système et de logiciels associés, comparer la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur, afin de vérifier que les correctifs les plus récents disponibles sont installés.			
	6.1.b Passer en revue les politiques relatives à l'installation des correctifs de sécurité afin de s'assurer qu'elles stipulent l'installation de tous les nouveaux correctifs de sécurité stratégiques dans un délai d'un mois.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
6.2 Établir un processus pour identifier et assigner une catégorie de risque aux nouvelles vulnérabilités de sécurité découvertes. ***Remarques :*** ▪ *Le classement des risques doit se baser sur les meilleures pratiques du secteur. Par exemple, les critères de classement des vulnérabilités à « haut » risque peuvent comprendre un score CVSS (Common Vulnerability Scoring System, système de notation de vulnérabilité commun) de 4.0 ou plus, et/ou un correctif proposé par le fournisseur, classé comme « critique », et/ou une vulnérabilité affectant un composant essentiel du système.* ▪ *Le classement des vulnérabilités tel qu'il est défini au point 6.2 est considéré comme une meilleure pratique jusqu'au 30 juin 2012, après quoi ce sera une obligation.*	**6.2.a** Interroger le personnel responsable afin de vérifier que les processus d'identification des nouvelles vulnérabilités de la sécurité sont mis en œuvre et que ces dernières reçoivent un classement de risque. (Au minimum, les vulnérabilités les plus critiques, de risque le plus élevé, doivent être classées comme « à haut risque »).			
	6.2.b Vérifier que les processus pour identifier les nouvelles vulnérabilités de sécurité comprennent l'utilisation de sources externes d'information sur la vulnérabilité de sécurité			
6.3 Développer des applications logicielles (internes et externes, y compris l'accès administratif aux applications par le Web) conformément à la norme PCI DSS (par exemple, authentification et connexion sécurisées), basées sur les meilleures pratiques du secteur. Intégrer la sécurité des informations à tout le cycle de vie du développement de logiciel. Ces processus doivent inclure ce qui suit :	**6.3.a** Se procurer les processus écrits de développement de logiciel et les examiner pour vérifier que les processus respectent les normes du secteur et/ou les meilleures pratiques.			
	6.3.b Examiner les processus écrits de développement de logiciel pour vérifier que la sécurité des informations est intégrée à tout le cycle de vie.			
	6.3.c Examiner les processus écrits de développement de logiciel pour vérifier que les applications logicielles sont développées conformément à la norme PCI DSS.			
	6.3.d En examinant les processus écrits de développement de logiciel et les entretiens des développeurs de logiciels, vérifier que :			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
6.3.1 La suppression des comptes d'application personnalisés, des noms d'utilisateur et des mots de passe avant l'activation des applications ou leur mise à la disposition des clients.	**6.3.1** Les comptes d'application personnalisés, les noms d'utilisateur et les mots de passe sont supprimés avant la mise en production du système ou sa mise à la disposition des clients.			
6.3.2 L'examen du code personnalisé avant sa mise en production ou sa mise à la disposition des clients afin d'identifier toute vulnérabilité éventuelle du codage. ***Remarque :*** *cette condition s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de développement du système.* *Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers. Les applications Web font également l'objet de contrôles supplémentaires si elles sont orientées public afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par la condition 6.6 de la norme PCI DSS.*	**6.3.2.a** Obtenir et passer en revue les politiques afin de vérifier que toutes les modifications apportées au code personnalisé d'application sont examinées (manuellement ou automatiquement), comme suit : ▪ Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. ▪ Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé (voir la condition 6.5 de la norme PCI DSS). ▪ 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 la publication.			
	6.3.2.b Sélectionner un échantillon de modifications apportées récemment à une application personnalisée et vérifier que le code correspondant est examiné conformément aux instructions décrites au point 6.3.2 ci-dessus.			
6.4 Suivre les processus et procédures de contrôle des changements pour toutes les modifications apportées à des composants du système. Ces processus doivent inclure ce qui suit :	**6.4** D'après l'examen des processus de contrôle du changement, les entretiens avec les administrateurs système et réseau et l'examen des données pertinentes (documentation sur la configuration réseau, données de production et de tests, etc.) vérifier que :			
6.4.1 Séparation des environnements de développement/test et de production.	**6.4.1** Les environnements de test/développement sont distincts de l'environnement de production, et il existe un contrôle d'accès pour garantir la séparation.			
6.4.2 Séparation des obligations entre les environnements de développement/test et de production.	**6.4.2** Il existe une séparation entre les missions des collaborateurs affectés aux environnements de développement/test et celles des personnels affectés à l'environnement de production.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
6.4.3 Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.	**6.4.3** Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.			
6.4.4 Suppression des données et comptes de tests avant que les systèmes de production ne deviennent actifs.	**6.4.4** Les données de test et les comptes sont supprimés avant que le système de production ne devienne actif.			
6.4.5 Procédures de contrôle de modifications pour la mise en œuvre de correctifs de sécurité et de modifications du logiciel. Les procédures doivent inclure ce qui suit :	**6.4.5.a** Vérifier que les procédures de contrôle des modifications liées à la mise en œuvre des correctifs de sécurité et des modifications logicielles sont documentées et stipulent les points 6.4.5.1 à 6.4.5.4 ci-dessous.			
	6.4.5.b Sur un échantillon de composants du système et de correctifs de sécurité/changements récents, associer ces modifications à la documentation du contrôle des changements correspondante. Pour chaque modification étudiée, procéder comme suit :			
6.4.5.1 Documentation de l'impact	**6.4.5.1** Vérifier que la documentation de l'impact est comprise dans la documentation de contrôle des changements, et ce pour chaque changement inclus dans l'échantillon.			
6.4.5.2 Documentation du changement approuvée par les responsables appropriés.	**6.4.5.2** Vérifier qu'une approbation documentée par les responsables existe pour chaque modification échantillonnée.			
5.4.5.3 Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système.	**6.4.5.3.a** Pour chaque changement échantillonné, vérifier que le test de fonctionnalité a été exécuté pour vérifier que le changement ne compromet pas la sécurité du système.			
	6.4.5.3.b Pour les modifications de code personnalisé, vérifier la conformité à la condition 6.5 de la norme PCI DSS de toutes les mises à jour avant leur mise en production.			
6.4.5.4 Procédures de suppression.	**6.4.5.4** Vérifier que des procédures de suppression sont préparées pour chaque changement inclus dans l'échantillon.			
6.5 Développer des applications basées sur les directives de codage sécurisé. Prévenir les vulnérabilités de codage courantes dans les processus de	**6.5.a** Se procurer et examiner les processus de développement de logiciel. Vérifier que le processus exige la formation aux techniques de codage sécurisé pour les développeurs, selon les directives et les meilleures pratiques du secteur.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
développement de logiciel, afin d'inclure les éléments suivants : ***Remarque :*** *les vulnérabilités décrites aux points 6.5.1 à 6.5.9 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.*	**6.5.b** Interroger un panel de développeurs et obtenir la preuve qu'ils disposent des connaissances nécessaires en techniques de codage sécurisé.			
	6.5.c. Vérifier la mise en place de processus garantissant, au minimum, la non-vulnérabilité des applications aux éléments suivants :			
6.5.1 Attaques par injection, notamment les injection de commandes SQL. Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.	**6.5.1** Attaques par injection, notamment les injection de commandes SQL (valider l'entrée pour vérifier que les données utilisateur ne peuvent pas modifier le sens des commandes et des requêtes, utiliser des requêtes paramétrées, etc.).			
6.5.2 Saturation de la mémoire tampon	**6.5.2** Saturation de la mémoire tampon (valider les limites de la mémoire tampon et tronquer les chaînes d'entrée).			
6.5.3 Stockage cryptographique non sécurisé	**6.5.3** Stockage cryptographique non sécurisé (prévient les défauts cryptographiques).			
6.5.4 Communications non sécurisées	**6.5.4** Communications non sécurisées (crypter correctement toutes les communications authentifiées et sensibles).			
6.5.5 Traitement inapproprié des erreurs	**6.5.5** Traitement inapproprié des erreurs (ne pas laisser échapper d'informations par les messages d'erreurs)			
6.5.6 Toutes les vulnérabilités à « haut risque », identifiées dans le processus d'identification de vulnérabilité (selon la condition 6.2 de la norme PCI DSS). ***Remarque :*** *cette condition est considérée comme une meilleure pratique jusqu'au 30 juin 2012, après quoi ce sera une obligation.*	**6.5.6** Toutes les vulnérabilités de niveau « élevé », identifiées par la condition 6.2 de la norme PCI DSS.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
Remarque : *les conditions 6.5.7 à 6.5.9, ci-dessous, s'appliquent aux applications Web et aux interfaces d'application (internes ou externes) :*				
6.5.7 Script intersite (XSS)	**6.5.7** Attaques par script intersite (XSS) (valider tous les paramètres avant l'inclusion, utiliser un mécanisme d'échappement sensible au contexte, etc.).			
6.5.8 Contrôle d'accès inapproprié (comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, et survol de répertoire)	**6.5.8** Contrôle d'accès inapproprié comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, et survol de répertoire (authentifier correctement les utilisateurs et nettoyer les entrées. Ne soumettre en aucun cas les références à des objets internes aux utilisateurs).			
6.5.9 Attaques CSRF (Cross-site request forgery)	**6.5.9** Attaques CSRF (Cross-site request forgery) (ne pas se fier aux éléments d'authentification et tokens automatiquement soumis par les navigateurs).			
6.6 Pour les applications Web orientées public, traiter les nouvelles menaces et vulnérabilités de manière régulière 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 orientées public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuels, au moins une fois par an et après toute modification ▪ Installation d'un pare-feu pour applications Web devant les applications Web orientées public	**6.6** Pour *les applications* Web orientées public, s'assurer que l'*une* des méthodes ci-dessous est en place comme suit : ▪ Vérifier que les applications Web orientées public sont examinées (à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité automatiques ou manuels) de la manière suivante : - au moins une fois par an ; - après toute modification ; - par une société spécialisée dans la sécurité des applications ; - toutes les vulnérabilités sont corrigées ; - l'application est réévaluée après les corrections. ▪ Vérifier qu'un pare-feu pour applications Web est en place devant les applications Web orientées public et les attaques via Internet. ***Remarque :*** *« une société spécialisée dans la sécurité des applications »* *peut être une société tiers ou* *une organisation interne, tant que les examinateurs se spécialisent dans la sécurité des applications et peuvent démontrer leur indépendance vis-à-vis de l'équipe de développement.*			

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître

Pour veiller à ce que les données stratégiques ne soient accessibles qu'au personnel autorisé, des systèmes et des processus doivent être mis en place pour restreindre l'accès à ces données aux seuls individus qui doivent les connaître et en fonction de leurs responsabilités professionnelles.

En d'autres termes, les droits d'accès ne sont accordés qu'au plus petit nombre de données nécessaires et en fonction des tâches à effectuer.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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. Les restrictions d'accès doivent inclure ce qui suit :	**7.1** Se procurer et examiner la politique écrite de contrôle des données et vérifier que le politique comprend ce qui suit :			
7.1.1 Restriction des droits d'accès accordés aux ID d'utilisateur privilégiés en octroyant les privilèges les plus faibles qui sont nécessaires pour la réalisation du travail	**7.1.1** S'assurer que les droits d'accès accordés aux ID d'utilisateur privilégiés sont les plus faibles nécessaires à la réalisation des obligations professionnelles.			
7.1.2 L'octroi des privilèges se fait sur la base de la classification et de la fonction professionnelles de chaque employé	**7.1.2** S'assurer que les privilèges sont octroyés aux individus sur la base de leur classification et de leur fonction professionnelles (cette approche est également appelée « contrôle d'accès en fonction du rôle » (ou RBAC, Role-Based Access Control).			
7.1.3 Obligation d'une approbation documentée par les responsables spécifiant les privilèges requis.	**7.1.3** Confirmer que l'approbation documentée par les responsables est requise (par écrit ou par voie électronique) pour tout accès, et qu'elle spécifie les privilèges requis.			
7.1.4 Mise en œuvre d'un système de contrôle d'accès automatique	**7.1.4** Confirmer que les contrôles d'accès sont mis en œuvre par le biais d'un système de contrôle d'accès automatisé.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
7.2 Définir un système de contrôle d'accès pour les composants de systèmes comptant plusieurs utilisateurs, qui limite 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. Ce système de contrôle d'accès doit inclure les éléments suivants :	**7.2** Passer en revue les paramètres du système et la documentation du fournisseur pour vérifier qu'un système de contrôle d'accès est déployé comme suit :			
7.2.1 Couverture de tous les composants du système	**7.2.1** Confirmer que les systèmes de contrôle d'accès sont en place sur tous les composants du système.			
7.2.2 L'octroi de privilèges aux individus repose sur leur classification et leur fonction professionnelles	**7.2.2** Confirmer que les systèmes de contrôle d'accès sont configurés pour octroyer les privilèges aux individus en fonction de leur classification et fonction professionnelles.			
7.2.3 Configuration par défaut du paramètre « Refuser tout » ***Remarque :*** *sur certains systèmes de contrôle d'accès, le paramètre « Autoriser tout » est configuré par défaut. Par conséquent, l'accès est autorisé à tous, à moins qu'une règle écrite ne précise explicitement le refus de l'accès.*	**7.2.3** Confirmer que les systèmes de contrôle d'accès intègrent un paramètre par défaut « Refuser tout ».			

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

En affectant un identifiant (ID) unique à chaque utilisateur, on s'assure que chacun sera personnellement responsable de ses actes. Les actions sur des données et des systèmes stratégiques peuvent alors être exécutées par des utilisateurs clairement identifiés et habilités à le faire.

Remarque : *ces obligations concernent tous les comptes, y compris ceux des points de vente, avec une capacité administrative, et tous les comptes utilisés pour voir ou accéder aux données de titulaires de carte ou pour accéder à des systèmes comportant ce type de données. Cependant, les conditions 8.1, 8.2 et 8.5.8 à 8.5.15 ne sont pas destinées aux comptes utilisateurs au sein d'une application de paiement de point de vente, qui n'ont accès qu'à un numéro de carte à la fois afin de permettre une transaction unique (comme les comptes de caisse).*

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
8.1 Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants du système ou aux données de titulaires de cartes.	**8.1** Vérifier que tous les utilisateurs ont un ID unique pour accéder aux composants du système ou aux données de titulaires de cartes.			
8.2 Outre l'affectation d'un ID unique**,** employer au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs : ▪ quelque chose de connu, comme un mot de passe ou une locution de passage ; ▪ quelque chose de détenu, comme un dispositif token ou une carte à puce ; ▪ quelque chose concernant l'utilisateur, comme une mesure biométrique.	**8.2** Pour vérifier que les utilisateurs sont authentifiés à l'aide d'un ID unique et une autre méthode d'authentification (par exemple, un mot de passe) afin d'accéder à l'environnement des données de titulaires de cartes, procéder comme suit : ▪ Obtenir et examiner la documentation qui décrit les méthodes d'authentification utilisées. ▪ Pour chaque type de méthode d'authentification employée et pour chaque type de composant du système, observer une authentification pour vérifier qu'elle se déroule conformément aux méthodes d'authentification décrites.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
8.3 Intégrer l'authentification à deux facteurs pour l'accès à distance (accès au niveau du réseau depuis l'extérieur du réseau) des employés, des administrateurs et de tiers au réseau (par exemple, authentification à distance et service de renseignements par téléphone (RADIUS) avec tokens ; système de contrôle d'accès au contrôleur d'accès du terminal (TACACS) avec tokens ; ou autres technologies permettant une authentification à deux facteurs). ***Remarque :*** *l'authentification à deux facteurs exige d'utiliser deux des trois méthodes d'authentification (voir la condition 8.2 pour la description des méthodes d'authentification). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à deux facteurs.*	**8.3** Pour vérifier qu'une authentification à deux facteurs est utilisée pour tout accès réseau à distance, observer un employé (par exemple un administrateur) se connectant à distance au réseau, et vérifier que deux des trois méthodes d'authentification sont utilisées.			
8.4 Rendre tous les mots de passe illisibles pendant la transmission et le stockage sur tous les composants du système à l'aide d'une méthode de cryptographie robuste.	**8.4.a** Sur un échantillon de composants du système, passer en revue les fichiers de mots de passe pour vérifier que les mots de passe sont illisibles pendant la transmission et le stockage.			
	8.4.b Pour les prestataires de services seulement, passer en revue les fichiers de mots de passe pour vérifier que les mots de passe des clients sont cryptés.			
8.5 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 du système comme suit :	**8.5** Examiner les procédures et interroger le personnel pour vérifier que des procédures sont mises en œuvre pour l'identification des utilisateurs et la gestion de l'authentification, en procédant comme suit :			
8.5.1 Contrôler l'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiant.	**8.5.1** Sélectionner un échantillon d'ID d'utilisateur, qui comprend aussi bien des administrateurs que des utilisateurs ordinaires. Vérifier que chaque utilisateur est autorisé à utiliser le système conformément à la politique en procédant comme suit :			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	▪ Obtenir et examiner un formulaire d'autorisation pour chaque ID. ▪ Vérifier que les ID d'utilisateur inclus dans l'échantillon sont implémentés conformément au formulaire d'autorisation (notamment les privilèges spécifiés et obtention de toutes les signatures exigées), en suivant les informations du formulaire d'autorisation vers le système.			
8.5.2 Vérifier l'identité des utilisateurs avant de réinitialiser leur mot de passe.	**8.5.2** Examiner les procédures relatives aux mots de passe et observer le personnel en charge de la sécurité afin de s'assurer, lorsqu'un utilisateur demande la réinitialisation de son mot de passe par téléphone, par e-mail, via Internet ou toute autre méthode n'impliquant pas un face-à-face, que son identité est vérifiée au préalable.			
8.5.3 Définir des mots de passe initiaux uniques pour chaque utilisateur et les modifier immédiatement après la première utilisation.	**8.5.3** Examiner les procédures relatives aux mots de passe et observer le personnel en charge de la sécurité pour vérifier que les mots de passe initiaux de chaque nouvel utilisateur, et les mots de passe réinitialisés des utilisateurs existants sont uniques pour chaque utilisateur et qu'ils sont modifiés après leur première utilisation.			
8.5.4 Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société.	**8.5.4** Sélectionner un échantillon d'employés qui ont quitté la société au cours des six derniers mois, et passer en revue les listes d'accès utilisateur actuelles pour vérifier que leurs ID ont été désactivés ou supprimés.			
8.5.5 Supprimer/désactiver les comptes d'utilisateur inactifs au moins tous les 90 jours.	**8.5.5** Vérifier que les comptes inactifs depuis plus de 90 jours sont supprimés ou désactivés.			
8.5.6 Activer les comptes utilisés par les fournisseurs pour un accès à distance pendant la période nécessaire seulement. Surveiller les compte d'accès à distance du fournisseur pendant leur utilisation.	**8.5.6.a** Vérifier que les comptes utilisés par les fournisseurs pour l'accès, la maintenance et l'entretien des composants du système sont désactivés et qu'ils ne sont activés que lorsqu'une intervention du fournisseur est nécessaire.			
	8.5.6.b Vérifier que les compte d'accès à distance du fournisseur sont surveillés pendant leur utilisation.			
8.5.7 Communiquer les politiques et procédures d'authentification à tous les utilisateurs qui ont accès aux données de titulaires de cartes.	**8.5.7** Interroger les utilisateurs d'un échantillon d'ID d'utilisateur pour vérifier qu'ils connaissent les politiques et les procédures d'authentification.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
8.5.8 Ne pas utiliser de comptes, de mots de passe ni d'autres méthodes d'authentification collectifs, partagés ou génériques.	**8.5.8.a** Sur un échantillon de composants du système, passer en revue les listes d'ID d'utilisateur pour vérifier les points suivants : ▪ les ID d'utilisateur et les comptes génériques sont désactivés ou supprimés ; ▪ il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ; ▪ aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration d'aucun composant du système.			
	8.5.8.b Passer en revue les politiques/procédures d'authentification pour vérifier que les mots de passe ou autres méthodes d'authentification collectifs et partagés sont interdits de façon explicite.			
	8.5.8.c Interroger les administrateurs système pour vérifier qu'ils ne distribuent aucun mot de passe ni autre méthode d'authentification, collectifs ou partagés, même si on le leur demande.			
8.5.9 Modifier les mots de passe utilisateur au moins tous les 90 jours.	**8.5.9.a** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les mots de passe utilisateur sont configurés de manière à demander aux utilisateurs de modifier leur mot de passe au moins tous les 90 jours.			
	8.5.9.b Pour les prestataires de services seulement, examiner les processus internes et la documentation des clients/utilisateurs pour s'assurer que les mots de passe utilisateur non client doivent être changés régulièrement et qu'il est demandé aux utilisateurs non clients de changer régulièrement leurs mots de passe, avec indication de la fréquence et des circonstances de ce changement.			
8.5.10 Exiger des mots de passe comportant au moins sept caractères.	**8.5.10.a** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les mots de passe utilisateur sont configurés pour comporter au moins sept caractères.			
	8.5.10.b Pour les prestataires de services seulement, examiner les processus internes et la documentation des clients/utilisateurs pour s'assurer qu'il est demandé aux utilisateurs non clients de définir des mots de passe comportant un nombre de caractères			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	minimal.			
8.5.11 Définir des mots de passe comportant des caractères alphanumériques.	**8.5.11.a** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les mots de passe sont configurés pour comporter des caractères alphanumériques.			
	8.5.11.b Pour les prestataires de services seulement, examiner les processus internes et la documentation des clients/utilisateurs pour s'assurer qu'il est demandé aux utilisateurs non clients de définir des mots de passe comportant des caractères alphanumériques.			
8.5.12 Interdire à un utilisateur de soumettre un nouveau mot de passe identique à l'un de ses quatre derniers mots de passe.	**8.5.12.a** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier qu'ils exigent que les nouveaux mots de passe ne puissent pas être identiques aux quatre derniers mots de passe utilisés.			
	8.5.12.b Pour les prestataires de services seulement, examiner les processus internes et la documentation des clients/utilisateurs pour vérifier que les nouveaux mots de passe des utilisateurs non clients ne puissent pas être identiques aux quatre derniers utilisés.			
8.5.13 Limiter les tentatives d'accès répétées en verrouillant l'ID d'utilisateur après six tentatives au maximum.	**8.5.13.a** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les paramètres d'authentification sont configurés pour exiger le verrouillage d'un compte d'utilisateur après six tentatives de connexion non valides au maximum.			
	8.5.13.b Pour les prestataires de services seulement, examiner les processus internes et la documentation des clients/utilisateurs pour vérifier que les comptes des utilisateurs non clients sont provisoirement verrouillés après six tentatives d'accès non valides au maximum.			
8.5.14 Régler la durée de verrouillage sur 30 minutes au moins ou jusqu'à ce que l'administrateur active l'ID d'utilisateur.	**8.5.14** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les mots de passe sont configurés pour exiger qu'un compte d'utilisateur, une fois verrouillé, reste à cet état 30 minutes au moins ou jusqu'à ce qu'un administrateur système réinitialise le			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	compte.			
8.5.15 Si une session reste inactive pendant plus de 15 minutes, demander à l'utilisateur de se réauthentifier pour réactiver le terminal ou la session.	**8.5.15** Sur un échantillon de composants du système, obtenir et contrôler les paramètres de configuration du système pour vérifier que les fonctions d'expiration du système/de la session sont réglées sur 15 minutes ou moins.			
8.5.16 Authentifier tous les accès aux bases de données contenant des données de titulaires de cartes. Cette condition concerne les accès des applications, des administrateurs et de tous les autres utilisateurs. Restreindre l'accès direct des utilisateurs ou les requêtes aux bases de données aux seuls administrateurs de bases de données.	**8.5.16.a** Examiner les paramètres de configuration de la base de données et de l'application, et vérifier que tous les utilisateurs s'authentifient avant d'y accéder.			
	8.5.16.b Vérifier que les paramètres de configuration de la base de données et de l'application garantissent que tous les accès d'utilisateurs aux bases de données, toutes les consultations et toutes les actions exécutées dans celles-ci (par exemple, déplacement, copie, suppression d'informations) s'effectuent exclusivement au moyen de méthodes programmées (par exemple, par le biais de procédures stockées).			
	8.5.16.c Vérifier que les paramètres de configuration de la base de données et de l'application restreignent l'accès direct des utilisateurs ou les requêtes aux bases de données aux seuls administrateurs de bases de données.			
	8.5.16.d Examiner les applications de base de données et les ID d'application associés pour vérifier que ces derniers ne peuvent être utilisés que par les applications (et non par des utilisateurs individuels ou d'autres processus).			

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

Dans la mesure où tout accès physique à des données ou à des systèmes hébergeant des données de titulaires de cartes permet à des individus d'accéder à des périphériques ou à des informations, et de supprimer des systèmes ou des copies papier, cet accès doit être restreint de façon appropriée. Dans le cadre de cette condition 9, le terme « personnel du site » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité. Un « visiteur » est défini comme un fournisseur, l'hôte du personnel du site, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée. « Support » se rapporte à tout support papier ou électronique contenant des données de titulaires de cartes.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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 cartes.	**9.1** Vérifier que des contrôles de sécurité physiques sont en place dans chaque salle informatique, centre de données et autres zones physiques qui abritent des systèmes appartenant à l'environnement des données de titulaires de cartes. ▪ Vérifier que l'accès est contrôlé par des lecteurs de badge et autres dispositifs tels que des badges autorisés, des clés et des cadenas. ▪ Observer un administrateur système pendant qu'il tente de se connecter sur les consoles de systèmes choisis de façon aléatoire dans l'environnement des données de titulaires de cartes, et vérifier que ces consoles sont « verrouillées » pour empêcher toute utilisation non autorisée.			
9.1.1 Installer des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès pour surveiller l'accès physique des individus aux zones sensibles. Examiner les données enregistrées et les mettre en corrélation avec d'autres	**9.1.1.a** Vérifier que des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès sont en place pour surveiller les points d'entrée/de sortie des zones sensibles.			
	9.1.1.b Vérifier que les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont protégés contre la falsification ou la désactivation.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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 cartes. Cette définition exclut les zones où ne sont installés que des terminaux de point de vente, tels que les zones de caisse dans un magasin.*	**9.1.1.c** S'assurer que les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont sous surveillance et que les données enregistrées sont conservées pendant trois mois au moins.			
9.1.2 Restreindre l'accès physique aux prises réseau accessibles au public. Par exemple, les zones accessibles aux visiteurs ne doivent pas comporter de prises réseau activées à moins que l'accès réseau ne soit explicitement autorisé.	**9.1.2** Interroger les administrateurs réseau et observer si les prises réseau ne sont activées que lorsque le personnel autorisé sur place a besoin de les utiliser. Il est également possible de vérifier que les visiteurs sont accompagnés à tout moment dans les zones contenant des prises réseau actives.			
9.1.3 Restreindre l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans fil.	**9.1.3** Vérifier que l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans fil est restreint de la manière appropriée.			
9.2 Élaborer des procédures qui aident à faire facilement la distinction entre le personnel du site et les visiteurs, en particulier dans les zones où sont accessibles les données de titulaires de cartes.	**9.2.a** Passer en revue les processus et les procédures d'attribution de badges au personnel du site et aux visiteurs, et vérifier qu'ils incluent ce qui suit : ▪ remise de nouveaux badges ; ▪ changement des conditions d'accès ; ▪ révocation des badges des personnels ne travaillant plus sur le site et des badges visiteurs périmés.			
	9.2.b Vérifier que l'accès au système de badges est restreint au seul personnel autorisé.			
	9.2.c Examiner les badges en cours d'utilisation afin de vérifier qu'ils identifient clairement les visiteurs et qu'il est facile de distinguer ces derniers du personnel du site.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
9.3 S'assurer que tous les visiteurs sont traités de la manière suivante :	**9.3** Vérifier que des contrôles des visiteurs sont en place comme suit :			
9.3.1 Une autorisation d'accès leur est donnée avant de pénétrer dans les zones où sont traitées et conservées les données de titulaires de cartes.	**9.3.1** Observer l'utilisation des badges d'ID des visiteurs afin de vérifier qu'un tel badge ne permet pas d'accéder aux zones physiques où sont stockées les données des titulaires de carte sans être accompagné.			
9.3.2 Ils reçoivent un dispositif physique (par exemple, badge ou dispositif d'accès) doté d'une date d'expiration, qui identifie bien les visiteurs comme ne faisant pas partie du personnel.	**9.3.2.a** Observer les gens au sein de l'établissement afin de vérifier l'utilisation des badges d'ID visiteur et de s'assurer qu'ils permettent de clairement distinguer les visiteurs du personnel du site.			
	9.3.2.b Vérifier que les badges des visiteurs portent une date d'expiration.			
9.3.3 Il leur est demandé de rendre le dispositif physique avant de quitter les locaux ou à la date d'expiration.	**9.3.3** Observer les visiteurs qui quittent les locaux pour vérifier qu'on leur demande bien de remettre leur badge d'identification à la sortie ou à l'expiration du badge.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
9.4 Utiliser un registre des visites pour tenir un contrôle physique de la circulation des visiteurs. 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.	**9.4.a** Vérifier qu'un registre des visites est utilisé pour consigner l'accès physique aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de cartes.			
	9.4.b Vérifier que ce registre comporte le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son accès physique, et que ce document est conservé pendant au moins trois mois.			
9.5 Ranger les sauvegardes sur support en lieu sûr, de préférence hors de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an.	**9.5.a** Observer la sécurité physique du site de stockage afin de s'assurer que le stockage des supports de sauvegarde est sécurisé.			
	9.5.b Vérifier que la sécurité physique du site de stockage est passée en revue au moins une fois par an.			
9.6 Assurer la sécurité physique de tous les supports.	**9.6** Vérifier que les procédures de protection des données de titulaires de cartes comprennent le contrôle de la sécurité physique de tous les supports (entre autres, ordinateurs, supports électroniques amovibles, réseaux, reçus et rapports sur papier, et fax).			
9.7 Assurer un contrôle strict de la distribution interne ou externe de tout type de support, notamment ce qui suit :	**9.7** Vérifier qu'une politique est en place pour le contrôle de la distribution des supports, et que celle-ci couvre tous les supports distribués, y compris ceux qui sont remis aux individus.			
9.7.1 Classer les supports afin de déterminer la sensibilité des données qu'ils contiennent.	**9.7.1** Vérifier que tous les supports sont classés afin de déterminer la sensibilité des données qu'ils contiennent.			
9.7.2 Envoyer les supports par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis.	**9.7.2** Vérifier que tous les supports expédiés à l'extérieur sont consignés et autorisés par les responsables, et qu'ils sont envoyés par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis.			
9.8 S'assurer que les responsables approuvent tous les supports déplacés d'une zone sécurisée (en particulier s'ils sont distribués à des individus).	**9.8** Choisir un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports, et vérifier que les informations de suivi et les autorisations appropriées des responsables y sont consignées.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
9.9 Assurer un contrôle strict du stockage et de l'accessibilité des supports.	**9.9** Obtenir et examiner la politique de contrôle du stockage et de la gestion des supports, et vérifier qu'elle stipule l'inventaire des supports à intervalles réguliers.			
9.9.1 Tenir de manière appropriée les journaux d'inventaire de tous les supports et effectuer un inventaire des supports au moins une fois par an.	**9.9.1** Obtenir et passer en revue le journal d'inventaire des supports pour vérifier qu'un inventaire des supports est réalisé au moins une fois par an.			
9.10 Détruire les supports lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou légales comme suit :	**9.10** Obtenir et examiner la politique de destruction périodique des supports, vérifier qu'elle couvre tous les supports et s'assurer que les points suivants sont respectés :			
9.10.1 Déchiqueter, brûler ou réduire en pâte les documents papier de sorte que les données de titulaires de cartes ne puissent pas être reconstituées.	**9.10.1.a** Vérifier que les documents papier sont déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être reconstitués.			
	9.10.1.b Examiner les conteneurs dans lesquels sont stockées les informations à détruire afin de vérifier qu'ils sont bien protégés. Par exemple, s'assurer que le conteneur portant la mention « À déchiqueter » est doté d'un dispositif de verrouillage empêchant d'accéder à son contenu.			
9.10.2 Rendre les données de titulaires de cartes sur support électronique irrécupérables de sorte que les informations ne puissent pas être reconstituées.	**9.10.2** Vérifier que les données de titulaires de cartes sur support électronique sont rendues irrécupérables à l'aide d'un programme de nettoyage sécurisé, conformément aux normes du secteur en matière d'élimination sécurisée des informations, ou à l'aide de tout autre procédé de destruction physique des supports (par exemple, par démagnétisation).			

Surveillance et test réguliers des réseaux

Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes

Les mécanismes de journalisation et la possibilité de suivre les activités des utilisateurs sont essentiels pour prévenir, détecter ou minimiser l'impact d'une altération des données. La présence de journaux dans tous les environnements permet de suivre de près, d'émettre des alertes et d'analyser les incidents éventuels. En l'absence de journaux retraçant les activités du système, il est très difficile, sinon impossible, de déterminer la cause d'une anomalie.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
10.1 Définir un processus pour associer chaque accès aux composants du système (en particulier les accès avec des droits administrateur, tels que root) à chaque utilisateur individuel.	**10.1** En observant les activités et en interrogeant l'administrateur système, vérifier que les vérifications à rebours des composants du système sont activés et actifs.			
10.2 Mettre en œuvre des vérifications à rebours automatisées pour tous les composants du système afin de reconstituer les événements suivants :	**10.2** Interroger les utilisateurs, examiner les vérifications à rebours et passer en revue les paramètres de ces journaux d'audit pour :			
10.2.1 Tous les accès des utilisateurs aux données des titulaires de cartes	**10.2.1** Vérifier que tous les accès des utilisateurs aux données de titulaires de cartes sont consignés.			
10.2.2 Toutes les actions exécutées par tout utilisateur avec des droits root ou administrateur	**10.2.2** Vérifier que les actions exécutées par tout utilisateur avec des droits root ou administrateur sont consignées.			
10.2.3 Accès à toutes les vérifications à rebours	**10.2.3** Vérifier que les accès à toutes les vérifications à rebours sont consignés.			
10.2.4 Tentatives d'accès logique non valides	**10.2.4** Vérifier que les tentatives d'accès logique non valides sont consignées.			
10.2.5 Utilisation des mécanismes d'identification et d'authentification	**10.2.5** Vérifier que l'utilisation des mécanismes d'identification et d'authentification est consignée.			
10.2.6 Initialisation des journaux d'audit	**10.2.6** Vérifier que l'initialisation des journaux d'audit est consignée.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
10.2.7 Création et suppression d'objets au niveau système	**10.2.7** Vérifier que la création et la suppression d'objets au niveau système sont consignées.			
10.3 Consigner dans les vérifications à rebours au moins les entrées suivantes pour chaque événement :	**10.3** Interroger et observer les utilisateurs pour chaque événement vérifiable (à partir du point 10.2), et :			
10.3.1 Identification de l'utilisateur	**10.3.1** Vérifier que les ID d'utilisateur sont inclus dans les entrées des journaux.			
10.3.2 Type d'événement	**10.3.2** Vérifier que le type d'événement est inclus dans les entrées des journaux.			
10.3.3 Date et heure	**10.3.3**Vérifier que l'horodatage est inclus dans les entrées des journaux.			
10.3.4 Indication de succès ou d'échec	**10.3.4** Vérifier que l'indication de succès ou d'échec est incluse dans les entrées des journaux.			
10.3.5 Origine de l'événement	**10.3.5** Vérifier que l'origine de l'événement est incluse dans les entrées des journaux.			
10.3.6 Identité ou nom des données, du composant du système ou de la ressource affectés	**10.3.6** Vérifier que l'identité ou le nom des données, du composant du système ou de la ressource affectés est inclus dans les entrées des journaux.			
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) est un exemple de technologie de synchronisation temporelle.*	**10.4.a** Vérifier qu'une technologie de synchronisation temporelle est mise en œuvre et active selon les conditions 6.1 et 6.2 de la norme PCI DSS.			
	10.4.b Obtenir et examiner le processus d'acquisition et de distribution et d'enregistrement de l'heure correcte au sein de l'entreprise ainsi que les paramètres systèmes d'horloge sur un échantillon de composants du système. Vérifier que les points suivants sont inclus dans le processus et mis en œuvre :			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
10.4.1 L'heure des systèmes critiques est correcte et la même pour tous.	**10.4.1.a** Vérifier que seuls des serveurs temporels reçoivent des signaux temporels de sources externes et que ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné).			
	10.4.1.b Vérifier que les serveurs temporels centraux désignés se consultent mutuellement pour maintenir l'exactitude de l'heure et que les autres serveurs internes ne reçoivent l'heure que de ces serveurs temporels centraux.			
10.4.2 Les données temporelles sont protégées.	**10.4.2.a** Examiner les configurations du système et des paramètres de synchronisation temporelle afin de vérifier que l'accès aux données temporelles est restreint au seul personnel dont l'accès à ces données est justifié par un besoin professionnel.			
	10.4.2.b Examiner les processus et configurations du système et des paramètres de synchronisation temporelle afin de vérifier que tout changement aux paramètres temporels sur des systèmes critiques est consigné, surveillé et vérifié.			
10.4.3 Les paramètres temporels sont reçus de sources temporelles reconnues par le secteur.	**10.4.3** Vérifier que les serveurs temporels acceptent des mises à jour temporelles de sources externes spécifiques, reconnues par le secteur (afin de prévenir toute tentative malveillante de changer l'horloge). Il est également possible de crypter ces mises à jour avec une clé symétrique, et de créer des listes de contrôle d'accès qui indiquent les adresses IP des machines clientes qui recevront les mises à jour temporelles (afin d'empêcher toute utilisation non autorisée des serveurs d'horloge internes).			
10.5 Protéger les vérifications à rebours de sorte qu'elles ne puissent pas être modifiées.	**10.5** Interroger l'administrateur système et passer en revue les autorisations pour vérifier que les vérifications à rebours sont bien protégées, de sorte qu'elles ne puissent pas être modifiées, comme suit :			
10.5.1 Limiter l'affichage des vérifications à rebours aux utilisateurs qui en ont besoin pour mener à bien leur travail.	**10.5.1** Vérifier que **les** vérifications à rebours sont uniquement accessibles aux individus qui en ont besoin pour mener à bien leur travail.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
10.5.2 Protéger les fichiers de vérifications à rebours contre toute modification non autorisée.	**10.5.2** Vérifier que **les** fichiers de vérifications à rebours existants sont protégés contre toute modification non autorisée par des mécanismes de contrôle d'accès, leur isolation physique et/ou l'isolation du réseau.			
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.	**10.5.3** Vérifier que **les** fichiers de vérifications à rebours sont rapidement sauvegardés sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer.			
10.5.4 Enregistrer les journaux des technologies orientées vers l'extérieur sur un serveur réservé à la journalisation sur le réseau local (LAN) interne.	**10.5.4** Vérifier que **les** journaux des technologies orientées vers l'extérieur (par exemple, sans fil, pare-feu, DNS, messagerie) sont déchargés ou copiés sur un support ou sur un serveur centralisé interne réservé à la journalisation sécurisée.			
10.5.5 Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte).	**10.5.5** Vérifier que les journaux sont analysés à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications en passant en revue les paramètres système ainsi que les fichiers contrôlés et les résultats des activités de contrôle.			
10.6 Passer en revue les journaux relatifs à tous les composants du système au moins une fois par jour. L'examen des journaux doit inclure les serveurs exécutant des fonctions des sécurité, tels que les serveurs IDS (système de détection d'intrusion) et AAA (Authentication, Authorization, and Accounting) (par exemple, RADIUS). ***Remarque :*** *les outils de journalisation, d'analyse et d'alerte peuvent être utilisés conformément à la condition 10.6*.	**10.6.a** Obtenir et examiner les politiques et les procédures de sécurité pour vérifier qu'elles comprennent des procédures d'analyse des journaux de sécurité au moins une fois par jour, et qu'elles exigent le suivi des anomalies.			
	10.6.b En observant et en interrogeant les utilisateurs, vérifier que les journaux relatifs à tous les composants du système sont régulièrement vérifiés.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
10.7 Conserver l'historique des vérifications à rebours pendant une année au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, pour analyse (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde).	**10.7.a** Obtenir et examiner les politiques et les procédures de sécurité, et vérifier qu'elles comprennent des dispositions pour la conservation des journaux, dont elles fixent la période à un an au moins.			
	10.7.b Vérifier que les journaux d'audit sont disponibles pendant un an au moins et que des processus sont en place pour restaurer immédiatement les journaux des trois derniers mois au moins, pour analyse.			

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

Des vulnérabilités sont sans cesse découvertes par des individus malveillants et des chercheurs, et sont introduites avec tout nouveau logiciel. Les composants du système, les processus et les logiciels personnalisés doivent être fréquemment testés afin de s'assurer que les contrôles de sécurité reflètent toujours les nouveaux environnements.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
11.1 Tester la présence de points d'accès sans fil et détecter les points d'accès sans fil non autorisés tous les trimestres. ***Remarque :*** *les analyses de réseau sans fil, les inspections logiques/physiques des composants du 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.* *Quelle que soit la méthode utilisée, elle doit être suffisante pour détecter et identifier tous les dispositifs non autorisés.*	**11.1.a** Vérifier que l'entreprise possède un processus documenté pour détecter et identifier les points d'accès sans fil, tous les trimestres.			
	11.1.b Vérifier que la méthodologie est appropriée et qu'elle permet de détecter et d'identifier tout point d'accès sans fil non autorisé, notamment au moins ce qui suit : ▪ cartes WLAN insérées dans les composants du système ; ▪ dispositifs sans fil portatifs connectés aux composants du système (par exemple, par USB, etc.) ; ▪ dispositifs sans fil branchés sur un port réseau ou à périphérique réseau.			
	11.1.c Vérifier que le processus documenté pour identifier les points d'accès sans fil non autorisés est exécuté au moins chaque trimestre pour tous les composants du système et toutes les installations.			
	11.1.d Si l'on utilise une surveillance automatisée (par exemple systèmes de détection et/ou de prévention d'intrusions sans fil, NAC, etc.), vérifier que la configuration déclenchera des alertes pour le personnel.			
	11.1.e Vérifier que le plan de réponse aux incidents de l'entreprise (condition 12.9) prévoit une réaction en cas de détection de périphériques sans fil non autorisés.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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 du système, modification de la topologie du réseau ou des règles des pare-feu, mise à niveau de produits). ***Remarque :*** *il n'est pas obligatoire que quatre analyses trimestrielles aient été réalisées avec succès pour la vérification de conformité PCI DSS initiale si l'évaluateur vérifie que 1) le résultat de la dernière analyse était réussi, 2) l'entité a documenté les politiques et les procédures exigeant l'exécution d'analyses trimestrielles, et 3) toutes les vulnérabilités relevées dans les résultats ont été corrigées, comme indiqué lors de la réexécution de l'analyse. Pendant les années qui suivent la vérification PCI DSS initiale, quatre analyses trimestrielles réussies doivent avoir été réalisées.*	**11.2** Vérifier que les analyses de vulnérabilité interne et externe sont exécutées comme suit :			
11.2.1 Effectuer des analyses trimestrielles de vulnérabilité interne.	**11.2.1.a** Examiner les rapports d'analyse et vérifier que quatre analyses trimestrielles internes ont eu lieu au cours de la période de 12 mois la plus récente.			
	11.2.1.b Examiner les rapports d'analyse et vérifier que le processus d'analyse comprenne de nouvelles analyses jusqu'à obtenir un résultat satisfaisant ou jusqu'à ce que toutes les vulnérabilités à « haut risque », définies à la condition 6.2 de la norme PCI DSS, aient été résolues.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	11.2.1.c Vérifier que l'analyse a été effectuée par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).			
11.2.2 Des analyses de vulnérabilité externe doivent être effectuées une fois par trimestre par un prestataire de services d'analyse agréé par le PCI SSC (Payment Card Industry Security Standards Council). ***Remarque :*** *des analyses de vulnérabilité externe doivent être effectuées une fois par trimestre par un prestataire de services d'analyse agréé (ASV) par le PCI SSC (Payment Card Industry Security Standards Council). Les analyses réalisées après la modification des réseaux peuvent être effectuées par le personnel interne.*	**11.2.2.a** Examiner les résultats des quatre analyses trimestrielles de vulnérabilité externe les plus récentes et vérifier qu'elles ont toutes eu lieu au cours de la période de 12 mois la plus récente.			
	11.2.2.b Examiner les résultats de chacune des quatre analyses trimestrielles pour s'assurer qu'elles satisfont aux conditions du guide de programme ASV (par exemple, pas de vulnérabilité supérieure à la note 4.0 du CVSS et aucune défaillance automatique).			
	11.2.2.c Examiner les rapports d'analyse pour vérifier que les analyses ont été réalisées par un prestataire de services d'analyse agréé (ASV) par le PCI SSC.			
11.2.3 Effectuer des analyses internes et externes après tout changement d'importance. ***Remarque :*** *les analyses réalisées après un changement peuvent être effectuées par le personnel interne.*	**11.2.3.a** Inspecter la documentation de contrôle des changements et analyser les rapports afin de vérifier que les composants du système assujettis à un changement d'importance ont été analysés.			
	11.2.3.b Examiner les rapports d'analyse et vérifier que le processus d'analyse stipule de nouvelles analyses jusqu'à ce que : ▪ aucune vulnérabilité supérieure à la note 4.0 du CVSS ne soit détectée pour les analyses externes ; ▪ un résultat satisfaisant soit obtenu ou jusqu'à ce que toutes les vulnérabilités à « haut risque », définies dans la condition 6.2 de la norme PCI DSS, aient été résolues, pour les analyses internes.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
	11.2.3.c Confirmer que l'analyse a été effectuée par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).			
11.3 Effectuer des tests de pénétration externe et interne au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement). Ces tests de pénétration doivent inclure ce qui suit :	**11.3.a** Obtenir et passer en revue les résultats du dernier test de pénétration pour vérifier qu'un tel test est effectué au moins une fois par an et après tout changement significatif de l'environnement.			
	11.3.b Vérifier que les vulnérabilités relevées et exploitables ont été corrigées et que les tests ont été réexécutés.			
	11.3.c Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).			
11.3.1 Tests de pénétration de la couche réseau	**11.3.1** Vérifier que les tests de pénétration comprennent des tests de pénétration de la couche réseau. Ces tests doivent inclure les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation.			
11.3.2 Tests de pénétration de la couche application	**11.3.2** Vérifier que les tests de pénétration comprennent des tests de pénétration de la couche application. Les tests doivent comprendre au minimum les vulnérabilités répertoriées dans la condition 6.5.			
11.4 Utiliser des systèmes de détection d'intrusions et/ou des systèmes de prévention d'intrusions pour contrôler l'intégralité du trafic, ainsi que les points critiques, dans l'environnement des données de titulaires de cartes et signaler au personnel tous les soupçons portant sur des altérations potentielles. Tenir à jour tous les moteurs de détection et de prévention des intrusions, les références et les signatures.	**11.4.a** Vérifier l'utilisation de systèmes de détection d'intrusions et/ou de systèmes de prévention d'intrusions pour contrôler l'intégralité du trafic, ainsi que les points critiques, dans l'environnement des données de titulaires de cartes.			
	11.4.b Vérifier que les systèmes de détection et/ou de prévention d'intrusions sont configurés pour alerter le personnel sur des altérations potentielles.			
	11.4.c Examiner les configurations des systèmes de détection et/ou de prévention d'intrusions et confirmer que le matériel correspondant est configuré, géré et mis à jour conformément aux instructions des fournisseurs pour garantir une protection optimale.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
11.5 Déployer des logiciels de contrôle de l'intégrité des fichiers pour alerter le personnel de toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques, et configurer ces logiciels pour effectuer des comparaisons entre les fichiers stratégiques au moins une fois par semaine. ***Remarque :*** *pour le contrôle de l'intégrité des fichiers, les fichiers stratégiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les produits de contrôle de l'intégrité des fichiers sont généralement préconfigurés avec les fichiers stratégiques pour le système d'exploitation associé. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).*	**11.5.a** Vérifier l'utilisation d'outils de contrôle de l'intégrité des fichiers dans l'environnement des données de titulaires de cartes en examinant les paramètres système et les fichiers contrôlés, ainsi que les résultats des activités de contrôle. Exemples de fichiers qui doivent être contrôlés : ▪ exécutables du système ; ▪ exécutables des applications ; ▪ fichiers de configuration et de paramètres ; ▪ fichiers d'historique, d'archive, de journaux et d'audit stockés à un emplacement centralisé.			
	11.5.b Vérifier que les outils sont configurés de manière à alerter le personnel de toute modification non autorisée des fichiers stratégiques et à procéder à de comparaisons de fichiers stratégiques au moins une fois par semaine.			

Gestion d’une politique de sécurité des informations

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

Une politique de sécurité robuste définit la sécurité mise en œuvre à l'échelle de l'entreprise et indique aux employés ce que l'on attend d’eux. Tout le personnel doit être sensibilisé au caractère confidentiel des données et à ses responsabilités dans la protection de ces informations. Dans le cadre de cette condition 12, le terme « personnel » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou ont accès d'une manière ou d'une autre à l'environnement des données des titulaires de cartes.

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
12.1 Définir, publier, gérer et diffuser une politique de sécurité qui remplit les fonctions suivantes :	**12.1** Passer en revue la politique de sécurité des informations et vérifier qu’elle est publiée et diffusée à tout le personnel concerné (mais aussi aux fournisseurs et partenaires commerciaux).			
12.1.1 Satisfait à toutes les conditions de la norme PCI DSS.	**12.1.1** Vérifier que la politique satisfait à toutes les conditions de la norme PCI DSS.			
12.1.2 Inclut un processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques (les directives OCTAVE, ISO 27005 and NIST SP 800-30 sont des exemples de méthodologies d'évaluation du risque).	**12.1.2.a** Vérifier que le processus annuel d'évaluation des risques qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques est documenté.			
	12.1.2.b Examiner la documentation d'évaluation des risques, afin de vérifier que le processus d'évaluation est exécuté au moins une fois par an.			
12.1.3 Comprend au moins un examen annuel avec une mise à jour chaque fois que l’environnement change.	**12.1.3** Vérifier que la politique de sécurité des informations est passée en revue au moins une fois par an et mise à jour le cas échéant, pour tenir compte des modifications apportées aux objectifs de l’entreprise ou à l’environnement de risque.			
12.2 Élaborer des procédures de sécurité opérationnelles quotidiennes conformes aux exigences de cette spécification (par exemple, des procédures de gestion des comptes d’utilisateur et des procédures d’examen des journaux).	**12.2** Examiner les procédures de sécurité opérationnelles quotidiennes. Vérifier qu’elles sont conformes à cette spécification et qu’elles comprennent des procédures administratives et techniques pour chaque condition.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
12.3 Élaborer les 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), utilisation du courrier électronique et d'Internet) et définir l'usage approprié de ces technologies. S'assurer que ces politiques d'utilisation exigent ce qui suit :	**12.3** Obtenir et examiner la politique d'utilisation des technologies stratégiques, et procéder comme suit :			
12.3.1 Approbation explicite des responsables	**12.3.1** Vérifier que les politiques d'utilisation exigent l'approbation explicite des responsables pour l'utilisation des technologies.			
12.3.2 Authentification pour l'utilisation des technologies	**12.3.2** Vérifier que les politiques d'utilisation exigent que l'utilisation de toute technologie soit authentifiée à l'aide d'un ID d'utilisateur et d'un mot de passe, ou toute autre méthode d'authentification (par exemple, token).			
12.3.3 Liste de tous les périphériques et du personnel disposant d'un accès	**12.3.3** Vérifier que les politiques d'utilisation exigent une liste de tous les périphériques et personnel autorisé à utiliser ce matériel.			
12.3.4 Indication sur les périphériques du nom de leur propriétaire, de ses coordonnées et de leur usage	**12.3.4** Vérifier que les politiques d'utilisation exigent que soient indiqués sur les périphériques le nom de leur propriétaire, ses coordonnées et leur usage.			
12.3.5 Usages acceptables de la technologie	**12.3.5** Vérifier que les politiques d'utilisation exigent un usage acceptable de la technologie.			
12.3.6 Emplacements acceptables des technologies sur le réseau	**12.3.6** Vérifier que les politiques d'utilisation exigent des emplacements acceptables des technologies sur le réseau.			
12.3.7 Liste des produits approuvés par la société	**12.3.7** Vérifier que les politiques d'utilisation exigent une liste des produits approuvés par la société.			
12.3.8 Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique	**12.3.8** Vérifier que les politiques d'utilisation exigent la déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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	**12.3.9** Vérifier que les politiques d'utilisation exigent l'activation des technologies d'accès à distance utilisées par les fournisseurs et partenaires commerciaux, uniquement lorsque c'est nécessaire, avec désactivation immédiate après usage.			
12.3.10 Lors de l'accès aux données de titulaires de cartes au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données de titulaires de cartes sur des disques durs locaux et des supports électroniques amovibles, sauf autorisation expresse pour des besoins professionnels.	**12.3.10.a** Vérifier que les politiques d'utilisation interdisent la copie, le déplacement ou le stockage des données de titulaires de cartes sur des disques durs locaux et des supports électroniques amovibles lors de l'accès à ces informations au moyen de technologies d'accès à distance.			
	12.3.10.b Pour le personnel dûment autorisé, vérifier que les politiques d'utilisation exigent la protection des données des titulaires de cartes conformément aux conditions de la norme PCI DSS.			
12.4 S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tout le personnel en la matière.	**12.4** Vérifier que les politiques de sécurité des informations définissent clairement les responsabilités de tout le personnel en la matière.			
12.5 Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations :	**12.5** Vérifier l'assignation formelle de la sécurité des informations à un chef de la sécurité ou tout autre responsable compétent. Obtenir et examiner les politiques et les procédures de sécurité des informations pour vérifier que les responsabilités suivantes en matière de sécurité des données sont assignées de manière spécifique et formelle :			
12.5.1 Définir, documenter et diffuser les politiques et les procédures de sécurité.	**12.5.1** Vérifier que la responsabilité de l'établissement et de la distribution des procédures et politiques de sécurité est formellement attribuée au personnel compétent.			
12.5.2 Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent.	**12.5.2** Vérifier que la responsabilité du contrôle, de l'analyse des alertes de sécurité, et de la diffusion des informations aux chefs de divisions appropriés et au personnel chargé de la sécurité est formellement assignée au personnel compétent.			
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.	**12.5.3** Vérifier que la responsabilité de l'établissement et de la diffusion des politiques et des procédures de remontée et de réponse aux incidents liés à la sécurité est formellement assignée au personnel compétent.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
12.5.4 Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification de comptes	**12.5.4** Vérifier que la responsabilité de l'administration des comptes d'utilisateur et de la gestion des authentifications est formellement assignée au personnel compétent.			
12.5.5 Surveiller et contrôler tous les accès aux données.	**12.5.5** Vérifier que la responsabilité de la surveillance et du contrôle de tous les accès aux données est formellement assignée au personnel compétent.			
12.6 Mettre en œuvre un programme formel de sensibilisation à la sécurité pour sensibiliser les employés à l'importance de la sécurité des données de titulaires de cartes.	**12.6.a** Vérifier qu'un programme formel de sensibilisation à la sécurité de tout le personnel est en place.			
	12.6.b Obtenir et examiner les procédures et la documentation du programme de sensibilisation à la sécurité, et procéder comme suit :			
12.6.1 Sensibiliser 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 des titulaires de cartes.*	**12.6.1.a** Vérifier que le programme de sensibilisation à la sécurité comprend plusieurs méthodes de sensibilisation et de formation du personnel (par exemple, affiches, lettres, mémos, formations sur le Web, réunions et promotions).			
	12.6.1.b Vérifier que le personnel participe à des formations de sensibilisation au moment de son recrutement et au moins une fois par an.			
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.	**12.6.2** Vérifier que le programme de sensibilisation à la sécurité exige que le personnel reconnaisse, par écrit ou par voie électronique, au moins une fois par an, avoir lu et compris la politique de sécurité des informations.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
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.*	**12.7** Interroger le responsable des ressources humaines et vérifier qu'existent, avant toute embauche, des contrôles des antécédents professionnels (dans les restrictions imposées par la loi) pour le personnel qui aura accès aux données des titulaires de cartes ou à l'environnement de ces données.			
12.8 Si les données de titulaires de cartes sont partagées avec des prestataires de services, gérer et mettre en œuvre des politiques et des procédures de gestion de ces derniers, de manière à inclure :	**12.8** Si l'entité partage des données de titulaires de cartes avec des prestataires de services (par exemple, sites de stockage sur bandes de sauvegarde, prestataires de services gérés tels que les prestataires de services d'hébergement sur le Web ou les prestataires de services de sécurité, ou encore les prestataires qui reçoivent des données en vue de la modélisation des fraudes), observer les intervenants, examiner les politiques et les procédures ainsi que les documents justificatifs pour :			
12.8.1 Tenir une liste des prestataires de services.	**12.8.1** Vérifier qu'une liste des prestataires de services est tenue.			
12.8.2 Faire signer aux prestataires de services un accord écrit par lequel ils se reconnaissent responsables de la sécurité des données de titulaires de cartes en leur possession.	**12.8.2** Vérifier que l'accord écrit stipule la reconnaissance par les prestataires de services de leur responsabilité en matière de protection des données de titulaires de cartes.			
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.	**12.8.3** Vérifier que les politiques et les procédures sont décrites et respectées, notamment le contrôle préalable à l'engagement de tout prestataire de services.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
12.8.4 Mettre en place un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an.	**12.8.4** Vérifier que l'entité a mis en place un programme qui contrôle la conformité de ses prestataires de services à la norme PCI DSS au moins une fois par an.			
12.9 Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système.	**12.9** Obtenir et examiner le plan de réponse aux incidents et les procédures associées, et procéder comme suit :			
12.9.1 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 ; ▪ procédures de réponse aux incidents spécifiques ; ▪ 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 ; ▪ la référence ou l'inclusion des procédures de réponse aux incidents des marques de cartes de paiement.	**12.9.1.a** Vérifier que le plan de réponse aux incidents inclut : ▪ les rôles, les responsabilités et les stratégies de communication en cas d'incident, notamment la 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 ; ▪ le processus de sauvegarde des données ; ▪ l'analyse des exigences légales en matière de signalement des incidents (par exemple, le California Bill 1386, qui exige la notification des consommateurs affectés en cas d'incident avéré ou soupçonné pour toute entreprise comptant des résidents en Californie dans sa base de données) ; ▪ la couverture et les réponses de tous les composants stratégiques du système ; ▪ la référence ou l'inclusion des procédures de réponse aux incidents des marques de cartes de paiement.			
	12.9.1.b Examiner la documentation d'un incident ou d'une alerte signalés antérieurement afin de vérifier que les procédures et le plan documenté de réponse aux incidents sont suivis.			

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible/Commentaires
12.9.2 Tester le plan au moins une fois par an.	**12.9.2** Vérifier que le plan est testé au moins une fois par an.			
12.9.3 Désigner le personnel spécifique disponible 24 heures sur 24 et sept jours sur sept pour répondre aux alertes.	**12.9.3** À travers l'observation et l'examen des politiques, vérifier que des équipes de réponse aux incidents sont disponibles 24 heures sur 24 et sept jours sur sept et que toutes les activités non autorisées, la détection des points d'accès sans fil non autorisés, les alertes des systèmes de détection d'incidents et/ou le signalement de toute modification non autorisée du contenu des fichiers ou des systèmes stratégiques sont sous surveillance.			
12.9.4 Organiser la formation appropriée du personnel en charge de la réponse aux violations de la sécurité.	**12.9.4** Vérifier par l'observation et l'examen des politiques, que le personnel chargé de la réponse aux violations de la sécurité reçoit une formation périodique.			
12.9.5 Inclure des alertes des systèmes de détection et de prévention des intrusions, et de contrôle de l'intégrité des fichiers.	**12.9.5** À travers l'observation et l'examen des processus, vérifier que le contrôle et la réponse aux alertes émises par les systèmes de sécurité, y compris la détection des points d'accès sans fil non autorisés, sont prévus dans le plan de réponse aux incidents.			
12.9.6 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.	**12.9.6** À travers l'observation et l'examen des politiques, vérifier qu'un processus est en place pour la modification et le développement du plan de réponse aux incidents en fonction des leçons apprises, et la prise en compte de l'évolution du secteur.			

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

Condition A.1 : Les prestataires de services d'hébergement partagé doivent protéger l'environnement des données de titulaires de cartes

Comme indiqué dans la condition 12.8, tous les prestataires de services qui ont accès aux données de titulaires de cartes (notamment les prestataires de services d'hébergement partagé) doivent respecter la norme PCI DSS. En outre, la condition 2.4 stipule que les prestataires de services d'hébergement partagé doivent protéger les données et l'environnement hébergés de chaque entité. En conséquence, les prestataires de services d'hébergement partagé doivent par ailleurs se conformer aux exigences définies dans cette annexe.

Exigences	Procédures de test	En place	Pas en place	Date cible/Commentaires
A.1 Protéger les données et l'environnement hébergés de entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité), conformément aux conditions A.1.1 à A.1.4 : Un prestataire de services d'hébergement doit satisfaire à ces exigences ainsi qu'aux conditions de toutes les autres sections pertinentes de la norme PCI DSS. ***Remarque :*** *même si un prestataire de services d'hébergement peut satisfaire ces exigences, le respect par l'entité qui a recours au prestataire de services d'hébergement n'est pas garanti. Chaque entité* doit *se conformer à la norme PCI DSS et doit valider cette conformité comme applicable.*	**A.1** Dans le cadre spécifique de l'évaluation d'un prestataire de services d'hébergement partagé au regard de la norme PCI DSS, pour vérifier que ceux-ci protègent les données et l'environnement hébergés des entités (commerçants et prestataires de services), sélectionner un échantillon de serveurs (Microsoft Windows et Unix/Linux) appartenant à quelques commerçants et prestataires de services hébergés représentatifs, et exécuter les points A.1.1 à A.1.4 décrits ci-dessous.			

Exigences	Procédures de test	En place	Pas en place	Date cible/Commentaires
A.1.1 S'assurer que chaque entité ne met en œuvre que les processus qui ont accès à l'environnement des données de titulaires de cartes qui la concerne.	**A.1.1** Si un prestataire de services d'hébergement partagé autorise des entités (par exemple, commerçants ou prestataires de services) à déployer leurs propres applications, vérifier que ces processus sont exécutés avec l'ID unique de l'entité. Par exemple : aucune entité sur le système ne peut utiliser un ID d'utilisateur partagé sur le serveur Web . Tous les scripts CGI utilisés par une entité doivent être créés et exécutés sous l'ID d'utilisateur unique de l'entité.			
A.1.2 Restreindre l'accès et les privilèges de chaque entité à son propre environnement de données de titulaires de cartes.	**A.1.2.a** Vérifier que l'ID d'utilisateur de tout processus d'application n'est pas un utilisateur avec des privilèges (root/admin).			
	A.1.2.b Vérifier que chaque entité (commerçant, prestataire de services) a des autorisations de lecture, d'écriture ou d'exécution uniquement sur les fichiers et les répertoires qui lui appartiennent ou sur les fichiers système nécessaires (restreintes au moyen d'autorisations sur le système de fichiers, de listes de contrôle d'accès, chroot, jailshell, etc.). **Important :** les fichiers d'une entité ne peuvent pas être partagés par groupe.			
	A.1.2.c Vérifier que les utilisateurs d'une entité n'ont pas un accès en écriture aux fichiers binaires d'un système partagé.			
	A.1.2.d Vérifier que l'affichage des entrées des journaux est limité à l'entité propriétaire de ces journaux.			
	A.1.2.e Pour s'assurer que chaque entité ne puisse pas monopoliser des ressources serveur en vue d'exploiter des vulnérabilités (notamment, erreur, concurrence critique et conditions de reprise entraînant, par exemple, la saturation de la mémoire tampon), vérifier que des restrictions sont en place pour l'usage de ces ressources système : ▪ espace disque, ▪ bande passante, ▪ mémoire, ▪ processeur.			

Exigences	Procédures de test	En place	Pas en place	Date cible/Commentaires
A.1.3 S'assurer que la journalisation et les vérifications à rebours sont activées, uniques à l'environnement des données de titulaires de cartes de chaque entité et conformes à la condition 10 de la norme PCI DSS.	**A.1.3** Vérifier que le prestataire de services d'hébergement partagé a activé la journalisation comme suit, pour l'environnement de chaque commerçant et prestataire de services : les journaux sont activés pour les applications tierces courantes ; les journaux sont activés par défaut ; les journaux peuvent être consultés par l'entité à laquelle ils appartiennent ; les emplacements des journaux sont clairement communiqués à l'entité propriétaire.			
A.1.4 Activer les processus d'investigation légale rapide en cas d'incident dans l'environnement d'un commerçant ou d'un prestataire de services.	**A.1.4** Vérifier que le prestataire de services d'hébergement partagé a des politiques écrites garantissant la mise en œuvre rapide d'investigations légales sur les serveurs en cas d'incident.			

Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux conditions 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 la condition initiale de la norme PCI DSS.
2. Fournir une protection similaire à celle de la condition initiale de la norme PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par la condition initiale (Pour plus d'informations sur chaque condition PCI DSS, voir *Navigation dans la norme PCI DSS*).
3. Aller au-delà des autres conditions PCI DSS (Les contrôles compensatoires ne consistent pas simplement en la conformité à d'autres conditions PCI DSS).

   Lors de l'évaluation de la portée des contrôles compensatoires, 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 de la norme PCI DSS doit déterminer et valider la suffisance de tous les contrôles compensatoires. L'efficacité d'un contrôle compensatoire dépend des caractéristiques spécifiques de l'environnement dans lequel il est mis en œuvre, des contrôles de sécurité associés et de la configuration du contrôle proprement dit. Les entreprises doivent avoir conscience qu'un contrôle compensatoire particulier ne sera pas dans tous les environnements.*

   a) Les conditions existantes de la norme PCI DSS NE PEUVENT PAS être considérées comme des contrôles compensatoires si elles sont déjà exigées pour l'élément examiné. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être transmis sous forme cryptée afin de limiter les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut pas utiliser d'autres conditions de mot de passe de la norme PCI DSS (blocage des intrus, mots de passe complexes, etc.) pour compenser l'absence de mots de passe cryptés, puisque celles-ci ne limitent pas les risques d'interception des mots de passe en texte clair. Par ailleurs, les autres contrôles de mots de passe sont déjà exigés par la norme PCI DSS pour l'élément examiné (à savoir les mots de passe).

   b) Les conditions existantes de la norme PCI DSS PEUVENT être considérées comme des contrôles compensatoires si elles sont exigées dans un autre domaine, mais pas pour l'élément examiné. Par exemple, l'authentification à deux facteurs est exigée par la norme PCI DSS pour l'accès à distance. L'authentification à deux facteurs *à partir du réseau interne* peut aussi être considérée comme un contrôle compensatoire de l'accès administrateur non-console lorsque la transmission des mots de passe cryptés ne peut pas être prise en charge. L'authentification à deux facteurs est un contrôle compensatoire acceptable si : (1) elle satisfait à l'intention de la condition 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 conditions existantes de la norme 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 titulaires de cartes illisibles conformément à la condition 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 proportionnels aux risques supplémentaires qu'implique le non-respect de la condition PCI DSS.

L'évaluateur doit évaluer soigneusement les contrôles compensatoires pendant chaque évaluation annuelle de la norme PCI DSS afin de confirmer que chaque contrôle compensatoire couvre de manière

appropriée le risque ciblé par la condition initiale de la norme 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 les contrôles compensatoires dans toute situation où ces contrôles sont utilisés pour satisfaire une condition PCI DSS. Noter que les contrôles compensatoires doivent être documentés dans le Rapport sur la conformité, dans la section de la condition PCI DSS correspondante.

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

Numéro et définition des conditions :

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

Fiche de contrôles compensatoires – Exemple complété

Utiliser cette fiche de travail pour définir les contrôles compensatoires pour toute condition reconnue « en place » par le biais de ces contrôles.

Numéro de condition : 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 titulaires de cartes ?

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité à la condition initiale.	*La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « root ». La société XYZ ne peut pas gérer le nom d'utilisateur « root » ni consigner toutes les activités de chaque utilisateur « root ».*
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	*L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des informations d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière.*
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	*L'absence d'ID d'utilisateur uniques et le fait de ne pas pouvoir tracer les informations d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.*
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.	*Une société XYZ va demander à tous les utilisateurs de se connecter aux serveurs à partir de leur bureau à l'aide de la commande SU. Cette commande autorise les utilisateurs à accéder au compte « root » et à exécuter des actions sous ce compte, tout en permettant de consigner leurs activités dans le répertoire du journal SU. Il est ainsi possible de suivre les actions de chaque utilisateur par le biais du compte SU.*
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	*La société XYZ démontre à l'évaluateur l'exécution de la commande SU et lui montre que celle-ci permet d'identifier les utilisateurs connectés qui exécutent des actions sous le compte « root ».*
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	*La société XYZ décrit les processus et les procédures mis en place pour éviter la modification, l'altération ou la suppression des configurations SU de sorte que des utilisateurs individuels puissent exécuter des commandes root sans que leurs activités soient consignées ou suivies.*

Annexe D : Segmentation et échantillonnage des installations de l'entreprise et des composants du système