Industrie des cartes de paiement (PCI)

# Norme de sécurité des données

## Conditions et procédures d'évaluation de sécurité

**Version 3.0**

Novembre 2013

# 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 Norme de sécurité des données – Récapitulatif des changements entre les versions 1.1 et 1.2. 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 2010* | 2.0 | *Mise à jour et application des changements depuis la v1.2.1. Voir PCI DSS – Récapitulatif des modifications entre les versions 1.2.1 et 2.0 de la norme PCI DSS* | |
| *Novembre 2013* | 3.0 | *Mise à jour de la v2.0. Voir PCI DSS – Récapitulatif des modifications entre les versions 2.0 et 3.0 de la norme PCI DSS* | |

# Table des matières

# Introduction et présentation de la norme de sécurité des données PCI

La Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) a été développée dans le but d'encourager et de renforcer la sécurité des données du titulaire ainsi que pour 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 du titulaire. 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 services, ainsi qu'à toutes les autres entités qui stockent, traitent ou transmettent des données du titulaire (CHD) et/ou des données d'identification sensibles (SAD). Les 12 clauses de la norme PCI DSS sont détaillées ci-dessous.

**Norme de sécurité des données PCI – Présentation détaillée**

| | |
|---|---|
| **Création et gestion d'un réseau et d'un système sécurisés** | **1.** Installer et gérer une configuration de pare-feu pour protéger les données du titulaire<br>**2.** Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur |
| **Protection des données du titulaire** | **3.** Protéger les données du titulaire<br>**4.** Crypter la transmission des données du titulaire sur les réseaux publics ouverts |
| **Gestion d'un programme de gestion des vulnérabilités** | **5.** Utiliser des logiciels ou des logiciels antivirus et les mettre à jour régulièrement<br>**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 du titulaire aux seuls individus qui doivent les connaître<br>**8.** Identifier et authentifier l'accès aux composants du système<br>**9.** Restreindre l'accès physique aux données du titulaire |
| **Surveillance et test réguliers des réseaux** | **10.** Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données du titulaire<br>**11.** Tester régulièrement les processus et les systèmes de sécurité |
| **Gestion d'une politique de sécurité des informations** | **12.** Maintenir une politique qui adresse les informations de sécurité 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 de la norme PCI DSS et les procédures de test commencent en page 15

La norme PCI DSS comprend un ensemble de conditions pour la protection des données du titulaire et peut être renforcée de contrôles et pratiques supplémentaires pour réduire encore les risques, ainsi que par des lois et réglementations locales, régionales ou sectorielles. En outre, la législation ou la réglementation peuvent exiger une protection spécifique des informations personnelles identifiables ou autres éléments de données (par exemple, le nom du titulaire). La norme PCI DSS ne supplante pas les lois locales ou régionales, les réglementations gouvernementales ou autres obligations légales.

### *Ressources de la norme PCI DSS*

Le site Web du Conseil des normes de sécurité PCI (PCI SSC) (www.pcisecuritystandards.org) contient plusieurs ressources supplémentaires, destinées à aider les organisations au cours des validations et évaluations de la norme PCI DSS, y compris :

- Une bibliothèque de documents comprenant :
  - *PCI DSS – Récapitulatif des modifications entre les versions 2.0 et 3.0 de la norme PCI DSS*
  - *Guide de référence rapide de la norme PCI DSS*
  - *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*
  - *Suppléments d'information et directives*
  - *Approche prioritaire pour la norme PCI DSS*
  - *Rapport sur la conformité (ROC) Modèle de rapport et instructions concernant le rapport*
  - *Questionnaires d'auto-évaluation (SAQ), instructions et directives relatives au SAQ*
  - *Attestations de conformité (AOC)*
- Questions fréquentes (FAQ)
- PCI pour les sites Web de commerçants de petite taille
- Cours de formation PCI et webinaires d'information
- Liste des évaluateurs de sécurité qualifiée (QSA) et des prestataires de services d'analyse (ASV)
- Liste des appareils approuvés par PTS et des applications de paiement validées selon la norme PA-DSS

***Remarque** : Les suppléments d'information complètent la norme PCI DSS et identifient des considérations et recommandations supplémentaires pour remplir les conditions de la norme PCI DSS. Elles ne supplantent pas, ne remplacent pas et ne développent pas la norme PCI DSS, ni aucune de ses conditions.*

Veuillez consulter *www.pcisecuritystandards.org* pour de plus amples informations concernant ces ressources et d'autres ressources.

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

La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, y compris les commerçants, les entreprises de traitement, institutions financières et prestataires de services, ainsi qu'à toutes les autres entités qui stockent, traitent ou transmettent des données du titulaire et/ou des données d'identification.

Les données du titulaire et les données d'identification sensibles sont définies comme suit :

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

***Le numéro de compte primaire est le facteur de définition des données du titulaire.*** Si le nom du titulaire, 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 titulaire, ils doivent être protégés conformément à toutes les conditions applicables de la norme PCI DSS.

Les conditions de la norme PCI DSS s'applique aux organisations et aux environnements où les données de compte (données du titulaire et/ou données d'identification sensibles) sont stockées, traitées ou transmises. Certaines conditions de la norme PCI DSS peuvent aussi s'appliquer aux organisations qui ont sous-traitées les opérations de paiement ou la gestion de leur CDE[1]. De plus, les organisations qui sous-traitent leur CDE ou leurs opérations de paiement à des tiers doivent s'assurer que les données de comptes sont protégées par le tiers, conformément aux conditions applicables de la norme PCI DSS.

Le tableau de la page suivante présente un certain nombre d'éléments courants des données du titulaire et des données d'identification 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.

[1] Selon les programmes de conformité des marques de paiement individuelles

| | | Élément de données | Stockage autorisé | Rendre illisibles les données stockées selon la condition 3.4 |
|---|---|---|---|---|
| Données de compte | Données du titulaire | 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'identification sensibles[2] | Données complètes de piste magnétique[3] | Non | Stockage interdit selon la condition 3.2 |
| | | CAV2/CVC2/CVV2/CID[4] | Non | Stockage interdit selon la condition 3.2 |
| | | Code/bloc PIN[5] | Non | Stockage interdit selon la 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 titulaire, seul le PAN doit être rendu illisible selon la condition 3.4 de la norme PCI DSS.

Les données d'identification sensibles ne doivent pas être stockées après autorisation, même si elles sont cryptées. Cela s'applique même lorsqu'il n'y a pas de PAN dans l'environnement. Les organisations doivent contacter directement leur acquéreur ou la marque de paiement individuelle afin de savoir s'il est permis de stocker un SAD avant autorisation, pendant combien de temps, ainsi que pour connaitre toute condition d'utilisation et de protection en rapport.

2 Une fois le processus d'autorisation terminé, les données d'identification sensibles ne peuvent plus être stockées (même si elles sont cryptées).

3 Données de piste complètes extraites de la bande magnétique, données équivalentes de la puce, ou autre support.

4 Le nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement

5 Le numéro d'identification personnel saisi par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction

# Relation entre les normes PCI DSS et PA-DSS

### *Conditions d'application de la norme PCI DSS aux applications PA-DSS*

L'utilisation seule d'une application conforme à la norme de sécurité des données de l'application de paiement (PA-DDS), n'en fait pas une entité conforme à la norme 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.

Toutes les applications qui stockent, traitent ou transmettent les données du titulaire peuvent faire l'objet d'une évaluation PCI DSS d'entité, y compris les applications qui ont été validées pour PA-DSS. L'évaluation PCI DSS doit vérifier que l'application de paiement validée PA-DSS est correctement configurée et implémentée de manière sécuritaire selon les exigences de la norme PCI DSS. Si l'application de paiement a donné lieu à une personnalisation, un examen plus approfondi sera requis pendant l'évaluation PCI DSS, dans la mesure où l'application est susceptible de ne plus être représentative de la version validée PA-DSS

Les conditions de la norme PA-DSS sont issues des *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS* (définies dans le présent document). La norme PA-DSS 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 à la norme PCI DSS, réduisent le risque que des failles de sécurité compromettant les données de PAN, les données complètes de piste, 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.

Pour déterminer si la norme PA-DSS s'applique à une application de paiement donnée, veuillez consulter le Guide du programme de la norme PA-DSS, disponible sur www.pcisecuritystandards.org.

### *Conditions d'application de la norme PCI DSS aux fournisseurs d'application de paiement.*

La norme PCI DSS est susceptible de s'appliquer aux fournisseurs d'application de paiement si le fournisseur stocke, traite ou transmet des données du titulaire, ou a accès aux données du titulaire de ses clients (par exemple, dans le rôle d'un fournisseur de services).

# Portée des conditions de la norme PCI DSS

Les conditions de sécurité de la norme PCI DSS, s'appliquent à tous les composants du système inclus ou connectés à l'environnement des données du titulaire. L'environnement des données du titulaire (CDE) est constitué d'individus, de processus et de technologies qui stockent, traitent, ou transmettent les données du titulaire ou les données d'identification sensibles. Les « composants du système » comprennent les dispositifs de réseau, les serveurs, les périphériques informatiques et les applications. Les exemples de composants du système comprennent notamment :

- Les systèmes qui fournissent des services de sécurité (par exemple, les serveurs d'authentification), facilitent la segmentation (par exemple, les pare-feu internes) ou qui pourraient avoir un impact sur le CDE (par exemple, des serveurs de résolution de nom ou de redirection Web).
- Les composants de virtualisation comme les machines virtuelles, commutateurs/routeurs virtuels, outils virtuels, applications/bureaux virtuels ainsi que les hyperviseurs.
- Les composants réseau comprennent notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans-fil, les équipements réseau et autres appareils de sécurité.
- Les types de serveur comprennent notamment les serveurs Web, d'application, de base de données, d'authentification, de messagerie, proxy, NTP (Network Time Protocol - Protocole d'Heure Réseau) et DNS (Domain Name System - Système de Noms de Domaine).
- Les applications comprennent toutes les applications achetées et personnalisées, y compris les applications internes et externes (par exemple Internet).
- Tout autre composant ou dispositif situé à l'intérieur du CDE ou connecté au CDE

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 du titulaire 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'entité évaluée identifie et documente l'existence de toutes les données du titulaire dans son environnement, afin de vérifier qu'aucune donnée n'existe en dehors du CDE actuellement défini.
- Une fois tous les emplacements de données du titulaire 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 du titulaire).
- L'entité considère que toutes données du titulaire trouvées s'inscrit dans le cadre de l'évaluation PCI DSS et fait partie du CDE. Si l'entité identifie des données qui ne sont pas actuellement incluses dans le CDE, ces données doivent être supprimées de manière sécuritaire, déplacées vers le CDE actuellement défini ou le CDE redéfini doit inclure ces données.
- L'entité conserve la documentation qui montre comment la portée de la norme PCI DSS a été déterminée. La documentation est conservée pour l'examen de l'évaluateur et/ou pour référence au cours de l'activité annuelle de confirmation du champ d'application de la norme PCI DSS.

Pour chaque évaluation PCI DSS, l'évaluateur doit valider que la portée de l'évaluation soit effectivement définie et documentée.

### *Segmentation réseau*

La segmentation réseau, ou l'isolation (segmentation), de l'environnement des données du titulaire par rapport au reste du réseau de l'entreprise n'est pas une condition de la norme PCI DSS. Toutefois, cette approche est 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 du titulaire 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 être considéré comme étant hors de la portée de la norme PCI DSS, un composant de système doit être isolé (segmenté) correctement du CDE, de telle sorte que, même si le composant hors de portée devait être compromis, la sécurité du CDE ne serait pas mise en péril.

Pour limiter le champ d'application de l'environnement des données du titulaire, 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 du titulaire. Le regroupement des données du titulaire 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 du titulaire par le biais d'un schéma de flux des données permet de comprendre parfaitement tous les flux de données du titulaire et de s'assurer que toute segmentation réseau isole correctement l'environnement des données du titulaire.

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 du titulaire 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.

*Annexe D : La segmentation et l'échantillonnage des installations de l'entreprise et des composants du système* fournissent de plus amples 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 une technologie sans-fil est utilisée pour stocker, traiter ou transmettre les données du titulaire (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 du titulaire ou en fait partie, 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.

### *Utilisation de prestataires de services 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 du titulaire.

Un prestataire de services ou un commerçant peuvent faire appel à un prestataire tiers pour le stockage, le traitement ou la transmission des données du titulaire 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 du titulaire peut s'en trouver affectée.

Les parties doivent clairement identifier les services et les composants du système qui sont inclus dans la portée de l'évaluation PCI DSS du prestataire de service, les conditions spécifiques de la norme PCI DSS couvertes par le prestataire de service, ainsi que toutes les conditions pour lesquelles les clients du prestataire de services doivent inclure leurs propres examens PCI DSS. Par exemple, un fournisseur d'hébergement géré doit clairement définir quelles sont ses adresses IP qui sont analysées dans le cadre de leur processus trimestriel d'analyse de vulnérabilité, ainsi que les adresses IP que le client doit inclure dans ses propres analyses trimestrielles.

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.

Si le tiers effectue sa propre évaluation PCI DSS, il doit fournir suffisamment de preuves à ses clients pour vérifier que la portée de l'évaluation PCI DSS du prestataire a recouvert les services applicables au client et que les conditions pertinentes de la norme PCI DSS ont été examinées et déterminées comme ayant été mises en place. Le type de preuve spécifique fourni par le prestataire de service à ses clients dépendra de l'accord/contrat passé entre ces parties. Par exemple, si l'AOC et/ou les sections pertinentes de l'AOC du prestataire de service (rédigées de manière à protéger toute information confidentielle) pourraient aider à trouver tout ou partie de l'information.

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 du titulaire auxquels ils sont associés. *Pour plus d'informations, se reporter à la condition 12.8 du présent document.*

# Meilleures pratiques d'implémentation de la norme PCI DSS dans les processus d'affaires courantes

Pour assurer que les contrôles de sécurité continuent d'être correctement mis en œuvre, la norme PCI DSS doit être implémentée dans les activités d'affaires courantes (BAU) dans le cadre de la stratégie de sécurité globale de l'entité. Cette pratique permet à une entité de surveiller l'efficacité de leurs contrôles de sécurité sur une base continuelle et de maintenir la conformité de leur environnement à la norme PCI DSS entre les évaluations PCI DSS. Les exemples de la manière avec laquelle la norme PCI DSS peut être incorporée aux activités BAU comprennent notamment :

1. La surveillance des contrôles de sécurité, tels que les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention des intrusions (IDS/IPS), la surveillance d'intégrité de fichier (FIM), les anti-virus, les contrôles d'accès, etc. ; pour garantir qu'ils fonctionnent de manière efficace comme prévu.
2. Assurer que les défaillances des contrôles de sécurité soient détectées et résolues rapidement. Les processus de résolution des défaillances des contrôles de sécurité doivent comprendre :
    - La restauration des contrôles de sécurité ;
    - L'identification des causes de la défaillance ;
    - L'identification et la résolution des problèmes de sécurité survenus pendant la défaillance du contrôle de sécurité ;
    - L'implémentation des mesures d'atténuation (telles que les processus et les contrôles techniques) pour empêcher que la cause de la défaillance ne se reproduise ;
    - La reprise de la surveillance des contrôles de sécurité, éventuellement avec une surveillance accrue pendant un certain temps, afin de vérifier que le contrôle fonctionne de manière efficace.
3. L'examen des modifications de l'environnement (par exemple, l'ajout de nouveaux systèmes, les changements de configurations de système ou de réseau) avec l'accomplissement de la modification et effectuer les procédures suivantes :
    - Déterminer l'impact potentiel sur la portée de la norme PCI DSS (par exemple, une nouvelle règle de pare-feu qui permet la connectivité entre un système du CDE et un autre système pourrait amener des systèmes ou des réseaux supplémentaires dans la portée de la norme PCI DSS).
    - Identifier les conditions de la norme PCI DSS applicables aux systèmes et aux réseaux affectés par les changements (par exemple, si un nouveau système se trouve dans le champ d'application de la norme PCI DSS, il doit être configuré selon les normes de configuration de système, en tenant compte de la FIM, AV, des correctifs, de la journalisation d'audit, etc. ; et il doit être ajouté au programme d'analyse de vulnérabilité trimestriel).
    - Mettre à jour la portée de la norme PCI DSS et implémenter les contrôles de sécurité de manière appropriée.
4. Les changements de la structure organisationnelle (par exemple l'intégration ou l'acquisition d'une société) doivent donner lieu à un examen formel de l'impact sur la portée et les conditions de la norme PCI DSS.

5. Des examens et des communications périodiques doivent être effectués pour confirmer que les conditions de la norme PCI DSS demeurent en place et que le personnel respecte les processus de sécurité. Ces examens périodiques doivent recouvrir toutes les installations et tous les emplacements, y compris les détaillants, les centres de données, etc., et inclure un examen de tous les composants du système (ou des échantillons de composants du système), pour vérifier que les conditions de la norme PCI DSS demeurent en place, par exemple, les standards de configuration ont été appliqués, les correctifs et AV sont à jour, les journaux d'audit sont analysés et ainsi de suite. La fréquence des examens périodiques doit être déterminée par l'entité en fonction de la taille et de la complexité de son environnement.

   Les examens peuvent également être utilisés pour vérifier que les preuves suffisantes sont maintenues, par exemple journaux d'audit, rapports d'analyse de vulnérabilité, examens de pare-feu, etc. afin d'aider l'entité à se préparer pour sa prochaine évaluation de conformité.

6. Examiner les technologies de matériel et de logiciel au moins une fois par an pour confirmer qu'elles continuent d'être prises en compte par le fournisseur et qu'elles respectent les conditions de sécurité de l'entité, y compris celles de la norme PCI DSS. S'il s'avère que les technologies ne sont plus prises en charge par le fournisseur ou qu'elles ne peuvent plus répondre aux besoins de sécurité de l'entité, celle-ci doit préparer un plan de réparation, qui peut comprendre le remplacement de la technologie si besoin.

En plus des pratiques ci-dessus, les organisations peuvent également envisager la séparation des tâches pour leurs fonctions de sécurité de sorte que les fonctions de sécurité et/ou d'audit soient séparées des fonctions opérationnelles. Dans les environnements où un même individu assume des fonctions multiples (par exemple, opérations de sécurité et d'administration), les tâches peuvent être assignées de telle sorte qu'un seul individu ne soit pas en mesure d'exercer un contrôle de bout en bout sur un processus sans un point de contrôle indépendant. Par exemple, la responsabilité de la configuration et la responsabilité de l'approbation des changements doivent être assignées à des individus séparés.

***Remarque :*** *Ces meilleures pratiques de mise en œuvre de la norme PCI DSS dans les processus d'affaires courantes sont données uniquement à titre de recommandation et de guide, elles ne remplacement pas et ne développent pas les conditions de la norme PCI DSS.*

# Pour les évaluateurs : Échantillonnage des installations de l'entreprise et des composants du système

L'échantillonnage est une option qui permet de faciliter le processus d'évaluation pour les évaluateurs lorsqu'il existe un grand nombre d'installations commerciales et/ou de composants du système.

Bien qu'il soit acceptable qu'un évaluateur échantillonne les composants de système/installation commerciale dans le cadre de son analyse de la conformité d'une entité à la norme PCI DSS, il n'est pas acceptable qu'une entité applique les conditions de la norme PCI DSS uniquement à un échantillon de son environnement (par exemple, les conditions d'analyse de vulnérabilité trimestrielle s'appliquent à tous les composants du système). De même, il n'est pas acceptable qu'un évaluateur examine uniquement un échantillon des conditions de la norme PCI DSS pour déterminer la conformité.

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 et de tous les emplacements 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.

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 sélectionnée, 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, les serveurs Windows exécutant Oracle, les systèmes d'unités centrales 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 de contrôles opérationnels et de sécurité PCI DSS standardisés et centralisés sont mis en place pour garantir 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 tous composants du système sont configurés conformément aux processus standards. L'évaluateur doit vérifier que les contrôles standardisés et centralisés sont mis en œuvre et fonctionnent correctement.
-

- 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.
- Les échantillons de composants du système doivent comprendre chaque type et chaque combinaison en utilisation. Par exemple, quand les applications sont échantillonnées, l'échantillon doit comprendre toutes les versions et plateformes pour chaque type d'application.

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 : Segmentation et 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 *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

Les instructions et le contenu du Rapport sur la conformité (ROC) sont désormais fournis dans le *Modèle de rapport ROC PCI DSS*.

Le *Modèle de rapport ROC PA-DSS* doit être utilisé comme modèle pour créer le *Rapport de 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 paiement ou l'acquéreur pour déterminer les instructions et ses conditions en matière de rapports.

# Processus d'évaluation de la norme PCI DSS

1. *Confirmer le champ d'application de l'évaluation de la norme PCI DSS.*
2. *Effectuer l'évaluation de l'environnement selon la norme PCI DSS en suivant les procédures de test de chaque condition.*
3. *Si besoin, effectuez les actions de réparation pour tout élément n'étant pas en place.*
4. *Terminer le rapport applicable pour l'évaluation (par ex. Questionnaire d'auto-évaluation* (SAQ) ou Rapport sur la conformité (ROC), y compris la documentation concernant tous les contrôles de compensation, selon les directives et instructions PCI applicables.
5. *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.*
6. *Envoyer le SAQ ou ROC et l'Attestation de conformité, ainsi que toute autre documentation requise, comme les rapports d'analyse ASV, 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 de colonnes pour les Conditions et procédures d'évaluation de sécurité de la norme PCI DSS :

- **Conditions de la norme PCI DSS** – Cette colonne définit les conditions de la Norme de sécurité des données, 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 ont été respectées et sont « en place ».
- **Directive** – Cette colonne décrit le but ou l'objectif de sécurité derrière chaque condition de la norme PCI DSS. Cette colonne contient uniquement des directives et elle est destinée à aider à comprendre le but de chaque condition. La directive indiquée dans cette colonne ne remplace et n'étend pas les conditions de la norme PCI DSS ou les procédures de test.

***Remarque :*** *Les conditions de la norme PCI DSS ne doivent pas être considérées comme étant en place si les contrôles n'ont pas encore été mis en œuvre ou doivent être terminés à une date future. Une fois que tous les éléments ouverts ou les éléments n'étant pas mis en place ont été adressés par l'entité, l'évaluateur doit procéder de nouveau à l'évaluation afin de valider que la résolution soit complétée et vérifier que toutes les conditions sont satisfaites.*

*Veuillez consulter les ressources suivantes (disponibles sur le site Web du PCI SSC) pour documenter l'évaluation PCI DSS :*

- *Pour découvrir les instructions sur la compilation de rapports de conformité (ROC), consulter le* Modèle de rapport ROC PCI DSS.
- *Pour découvrir les instructions pour remplir les questionnaires d'auto-évaluation (SAQ), consulter les* Directives et instructions SAQ PCI DSS.
- *Pour découvrir les instructions sur la soumission des rapports de validation de conformité PCI DSS, consulter* Attestations de conformité PCI DSS.

# Création et gestion d'un réseau et d'un système sécurisés

### *Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données du titulaire*

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 du titulaire 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 commerce électronique, accès des employés à Internet à partir de leurs navigateurs, accès des employés à la messagerie électronique, connexions dédiées telles que les connexions inter-entreprises) 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 que ces composants remplissent les conditions minimales des pare-feu définies par la condition 1. Lorsque d'autres composants du système sont utilisés dans l'environnement des données du titulaire 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 | DIRECTIVES |
|---|---|---|
| **1.1** Établissement et mise en œuvre des normes de configuration des pare-feu et des routeurs comprenant les éléments suivants : | **1.1** Inspecter les normes de configuration de pare-feu et de routeurs et autres documents spécifiés ci-dessous pour vérifier que les normes sont complètes et mises en œuvre comme suit : | Les pare-feu et les routeurs sont les composants essentiels de l'architecture contrôlant les entrées et les sorties d'un réseau. Il s'agit de dispositifs logiciels ou matériels qui bloquent les accès indésirables et gèrent l'accès autorisé vers et hors du réseau.<br>Les normes et procédures de configuration aideront à garantir que la première ligne de défense de l'organisation en matière de protection des données demeure robuste. |
| **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.a** Examiner les procédures documentées pour vérifier qu'un processus formel de test et d'approbation est présent pour :<br>• Toutes les connexions du réseau et<br>• Toutes les modifications de pare-feu et de routeur. | Un processus mis en œuvre et documenté pour l'approbation et le test de toutes les connexions et des modifications apportées aux configurations des pare-feu et des routeurs permettront d'éviter les problèmes de sécurité dus aux erreurs de configuration du réseau, du routeur ou du pare-feu.<br>Sans procédure formelle d'approbation et de test des modifications, les archives des modifications |
| | **1.1.1.b** Pour obtenir un échantillon des connexions du réseau, interroger le personnel responsable et examiner les archives afin de vérifier que les connexions de réseau ont été | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | approuvées et testées. | sont susceptibles de ne pas être mises à jour, ce qui risque de provoquer des incohérences entre la documentation du réseau et la configuration effective. |
| | **1.1.1.c** Identifier un échantillon d'une modification effectivement apportée aux configurations de pare-feu et de routeur, comparer à la modification des archives et interroger le personnel responsable pour vérifier que les changements ont été approuvés et testés | |
| **1.1.2** Diagramme du réseau actuel qui identifie toutes les connexions entre l'environnement de données du titulaire et les autres réseaux, y compris tout réseau sans fil | **1.1.2.a** Examiner le ou les diagrammes et observer les configurations de réseau pour vérifier qu'un diagramme du réseau actuel existe bien et qu'il documente toutes les connexions aux données du titulaire, y compris tout réseau sans-fil. | Les diagrammes de réseau décrivent comment les réseaux sont configurés et identifient les emplacements des tous les périphériques du réseau.<br>Sans les diagrammes du réseau actuel, des dispositifs pourraient être négligés et inconsciemment laissés en dehors des contrôles de sécurité implémentés pour la norme PCI DSS et, par conséquent, être vulnérables aux attaques. |
| | **1.1.2.b** Interroger le personnel responsable pour vérifier que le diagramme est tenu à jour. | |
| **1.1.3** Diagramme actuel montrant le flux des données du titulaire dans les systèmes et les réseaux | **1.1.3** Examiner le diagramme des flux de données et interroger le personnel pour vérifier que le diagramme :<br>• Montre le flux des données du titulaire dans les systèmes et les réseaux.<br>• Est conservé à jour et mis à jour si besoin suite aux changements de l'environnement. | Les diagrammes de flux de données du titulaire identifient l'emplacement de toutes les données du titulaire qui sont enregistrées, traitées ou transmises dans le réseau.<br>Les diagrammes de réseau et de flux de données aident une organisation à comprendre et à suivre la portée de leur environnement, en montrant comment les données du titulaire circulent dans les réseaux et entre les systèmes et les dispositifs individuels. |
| **1.1.4** Conditions relatives au pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne | **1.1.4.a** Examiner les Normes de configuration de pare-feu et vérifier qu'elles comprennent les conditions relatives au pare-feu au niveau de chaque connexion Internet et entre toute DMZ et la zone de réseau interne. | L'utilisation d'un pare-feu sur chaque connexion Internet entrante (et sortante) du réseau et entre toute DMZ et le réseau interne permet à l'organisation de surveiller et de contrôler les accès et de réduire les risques qu'un individu malveillant parvienne à accéder au réseau interne grâce à une connexion non protégée. |
| | **1.1.4.b** Vérifier que le diagramme de réseau actuel est conforme aux normes de configuration des pare-feu. | |
| | **1.1.4.c** Observer les configurations de réseau pour vérifier qu'un pare-feu est en place à chaque connexion Internet et | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | entre toute zone démilitarisée (DMZ) et la zone de réseau interne, conformément aux normes de configuration documentées et aux diagrammes de réseau. | |
| **1.1.5** Description des groupes, des rôles et des responsabilités pour la gestion des composants du réseau | **1.1.5.a** Vérifier que les normes de configuration des pare-feu et des routeurs comprennent une description des groupes, des rôles et des responsabilités pour la gestion des composants réseau. | Cette description des rôles et affectation des responsabilités garantit que le personnel sait qui est responsable de la sécurité de tous les composants du réseau et que ceux à qui la gestion des composants est affectée connaissent leurs responsabilités. Si les rôles et les responsabilités ne sont pas assignés de manière formelle, des dispositifs pourraient demeurer sans gestion. |
| | **1.1.5.b** Interroger le personnel auquel responsable de la gestion des composants du réseau pour confirmer que les rôles et les responsabilités sont affectés ainsi qu'il est documenté. | |
| **1.1.6** 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.<br><br>Les exemples de services non sécurisés comprennent notamment les protocoles FTP, Telnet, POP3, IMAP et SNMP v1 et v2. | **1.1.6.a** Vérifier que les normes de configuration des pare-feu et des routeurs comprennent la liste documentée de, tous les services, protocoles et ports comprenant la justification commerciale de chacun des services, par exemple les protocoles HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer), SSH (Secure Shell) et VPN (Virtual Private Network). | Les risques sont souvent dus à la présence de services et de ports non utilisés dans la mesure où ces derniers ont souvent des vulnérabilités connues et beaucoup d'organisations ne corrigent pas les vulnérabilités des services, protocoles et ports qu'elles n'utilisent pas (même si les vulnérabilités existent bien). En définissant et en documentant clairement les services, les protocoles et les ports nécessaires à la conduite de leurs activités, les organisations peuvent s'assurer que tous les autres services, protocoles et ports sont désactivés ou éliminés.<br><br>Si des services, protocoles ou ports non sécurisés sont nécessaires à l'entreprise, le risque inhérent à l'utilisation de ces protocoles doit être clairement compris et accepté par l'organisation. L'utilisation du protocole doit être justifiée et les fonctions de sécurité permettant l'utilisation sécurisée de ces protocoles doivent être documentées et appliquées. Si ces services, protocoles ou ports non sécurisés ne sont pas nécessaires à l'entreprise, ils doivent être désactivés ou supprimés. |
| | **1.1.6.b** Identifier les services, protocoles et ports non sécurisés autorisés, et vérifier que les fonctions de sécurité sont documentées pour chaque service. | |
| | **1.1.6.c** Examiner les configurations de pare-feu et de routeur pour vérifier que les fonctions de sécurité documentées sont mises en œuvre pour chaque service, protocole ou port non sécurisé. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.1.7** Exigence d'analyse des règles concernant les pare-feu et les routeurs au moins tous les six mois | **1.1.7.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. | Cet examen donne à l'organisation une occasion, au moins tous les six mois, d'éliminer les règles superflues, obsolètes ou incorrectes et de s'assurer que toutes les règles n'admettent que les services et les ports autorisés correspondants aux besoins documentés de l'activité.<br>Les organisations qui connaissent un volume important de changement de règles de pare-feu et de routeur peuvent souhaiter effectuer des analyses plus fréquemment, pour s'assurer que les règles continuent de répondre aux besoins de l'entreprise. |
| | **1.1.7.b** Examiner la documentation relative aux examens des règles interroger le personnel responsable pour vérifier que les règles sont passées en revue au moins tous les six mois. | |
| **1.2** Créer des configurations de pare-feu et de routeur qui limitent les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données du titulaire.<br>***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 et suivre la procédure suivante pour vérifier que les connexions sont restreintes entre les réseaux non approuvés et les composants du système dans l'environnement des données du titulaire : | Il est essentiel d'installer une protection réseau entre le réseau approuvé interne et tout autre réseau non approuvé externe et/ou échappant au contrôle ou à la gestion de l'entreprise. Si cette mesure n'est pas correctement mise en place, l'entité sera exposée au risque d'intrusion d'individus ou de logiciels malveillants.<br>Pour que la fonction de pare-feu soit efficace, elle doit être configurée correctement pour contrôler et/ou limiter le trafic entrant et sortant du réseau de l'entité. |
| **1.2.1** Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données du titulaire et, particulièrement, refuser tout autre trafic. | **1.2.1.a** Examiner les normes de configuration de routeur et de pare-feu pour vérifier qu'ils identifient le trafic entrant et sortant nécessaire pour l'environnement de données du titulaire. | Cette condition est destinée à empêcher les individus malveillants de pénétrer le réseau de l'entreprise par le biais d'adresses IP non autorisées, ou d'utiliser des services, protocoles ou ports de manière non autorisée (par exemple, pour transmettre des données obtenues sur votre réseau vers un serveur non approuvé).<br>Mettre en œuvre une règle qui refuse tout trafic entrant ou sortant qui n'est pas nécessaire aide à empêcher les brèches par négligence qui pourraient permettre un trafic entrant ou sortant indésirable et potentiellement dommageable. |
| | **1.2.1.b** Examiner les configurations de routeur et de pare-feu pour vérifier que le trafic entrant et sortant est limité au trafic nécessaire à l'environnement des données du titulaire. | |
| | **1.2.1.c** Examiner les configurations de pare-feu et de routeur pour vérifier que tous les autres trafics entrants et sortants sont explicitement refusés, par exemple à l'aide d'une instruction « refuser tout » explicite ou d'un refus implicite après une instruction d'autorisation. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.2.2** Sécuriser et synchroniser les fichiers de configuration des routeurs. | **1.2.2.a** Examiner les fichiers de configuration du routeur pour vérifier qu'ils sont sécurisés contre un accès non autorisé. | Lorsque les fichiers de configuration de routeur en cours de fonctionnement (ou actifs) comprennent les réglages actuels actifs, les fichiers de démarrage (qui sont utilisés lorsque les routeurs sont redémarrés ou démarrés) doivent être mis à jour avec les mêmes réglages sécurisés pour assurer que ces réglages sont appliqués lorsque la configuration de démarrage est exécutée.<br><br>Puisqu'ils ne fonctionnent que de temps en temps, les fichiers de configuration de démarrage sont souvent oubliés et ne sont pas mis à jour. Lorsqu'un routeur redémarre et charge une configuration de démarrage qui n'a pas été mise à jour avec les mêmes réglages sécurisés que ceux de la configuration en fonctionnement, les règles pourraient être moins strictes et permettre l'accès d'un individu malveillant au réseau. |
| | **1.2.2.b** Examiner les configurations de routeur pour vérifier qu'elles sont synchronisées, par exemple, la configuration de fonctionnement (ou active) correspond à la configuration de démarrage (utilisée lorsque les machines sont mises en route). | |
| **1.2.3** Installer des pare-feu de périmètre entre tous les réseaux sans fil et l'environnement des données du titulaire, et configurer ces pare-feu pour refuser ou, s'il est nécessaire à des fins professionnelles, autoriser uniquement le trafic entre l'environnement sans fil et l'environnement de données du titulaire. | **1.2.3.a** Examiner les configurations de pare-feu et de routeur pour vérifier que des pare-feu de périmètre sont installés entre tous les réseaux sans-fil et l'environnement des données du titulaire. | La mise en œuvre et l'exploitation connues (ou inconnues) de la technologie sans fil sur un réseau sont souvent la voie qu'utilisent les individus malveillants pour accéder au réseau et aux données du titulaire. Si un périphérique ou un réseau sans fil est installé à l'insu d'une entreprise, un individu malveillant peut pénétrer dans le réseau de manière « invisible ». Si les pare-feu ne restreignent pas l'accès des réseaux sans fil dans le CDE, les individus malveillants qui accèdent au réseau sans fil sans autorisation peuvent facilement se connecter au CDE et compromettre les informations de comptes.<br><br>Des pare-feu doivent être installés entre tous les réseaux sans fil et l'environnement des données du titulaire, indépendamment de l'objectif de l'environnement auquel le réseau sans fil est connecté. Ceci peut inclure notamment les réseaux d'entreprise, les magasins de détail, les réseaux d'hôte, les environnements d'entrepôt, etc. |
| | **1.2.3.b** Vérifier que les pare-feu refusent ou, si ce trafic est nécessaire à des fins commerciales, permettent uniquement au trafic autorisé de circuler entre l'environnement du réseau sans-fil et l'environnement des données du titulaire. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.3** Interdire l'accès public direct entre Internet et tout composant du système dans l'environnement des données du titulaire**.** | **1.3** Examiner les configurations des pare-feu et des routeurs – y compris notamment, le routeur interne au niveau d'Internet, le routeur et le pare-feu DMZ, le segment DMZ du titulaire, le routeur du périmètre et le segment du réseau interne du titulaire et suivez la procédure décrite ci-après afin de déterminer qu'il n'existe aucun accès direct entre Internet et les composants du système dans le segment du réseau interne du titulaire : | L'objectif d'un pare-feu est de gérer et de contrôler toutes les connexions entre les systèmes publics et les systèmes internes, en particulier ceux qui stockent, traitent et transmettent des données du titulaire. Si un accès direct est autorisé entre les systèmes publics et le CDE, les protections assurées par le pare-feu sont contournées et les composants du système stockant les données du titulaire peuvent être compromis. |
| **1.3.1** Déployer une DMZ pour limiter le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public. | **1.3.1** Examiner les configurations de pare-feu et de routeur pour vérifier qu'une DMZ est déployée pour limiter le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public. | La DMZ est la partie du réseau qui gère les connexions entre Internet (ou tout autre réseau non approuvé) et les services internes qu'une entreprise doit mettre à la disposition du public (comme un serveur Web).<br>Cette fonction est destinée à empêcher des individus malveillants d'accéder au réseau interne de l'entreprise à partir d'Internet ou d'utiliser des services, des protocoles ou des ports de manière non autorisée. |
| **1.3.2** Limiter le trafic Internet entrant aux adresses IP dans la DMZ. | **1.3.2** Examiner les configurations de pare-feu et de routeur pour vérifier que le trafic Internet entrant est limité aux adresses IP dans la DMZ. | |
| **1.3.3** Autoriser aucune connexion directe entrante ou sortante de trafic entre Internet et l'environnement des données du titulaire. | **1.3.3** Examiner les configurations de pare-feu et de routeur pour vérifier que les connexions directes entrantes ou sortantes ne sont pas autorisées pour le trafic entre Internet et l'environnement des données du titulaire. | L'examen de toutes les connexions entrantes ou sortantes permet d'inspecter et de restreindre le trafic selon l'adresse de source et/ou de destination, ainsi que l'inspection et le blocage des contenus indésirables, ce qui permet d'empêcher l'accès non filtré entre les environnements non approuvés et approuvés. Ceci permet, par exemple, d'empêcher des individus malveillants d'acquérir des données au sein du réseau de l'entreprise, et de les envoyer à un serveur externe non approuvé d'un réseau qui ne l'est pas non plus. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.3.4** Mise en œuvre des mesures anti-usurpation pour détecter et pour empêcher les adresses IP de source frauduleuses de pénétrer sur le réseau.<br><br>(Par exemple, bloquer le trafic originaire d'Internet avec une adresse de source interne). | **1.3.4** Examiner les configurations de pare-feu et de routeur pour vérifier que les mesures anti-usurpation sont mises en œuvre, par exemple, les adresses internes ne peuvent pas passer d'Internet vers la DMZ**.** | Normalement, un paquet contient l'adresse IP de l'ordinateur qui l'a envoyé aux autres ordinateurs à l'origine, de manière à ce que les autres ordinateurs du réseau sachent d'où vient le paquet. Les individus malveillants essayeront souvent d'usurper (ou d'imiter) l'adresse IP d'expédition pour que le système cible pense que le paquet provient d'une source autorisée.<br><br>Le filtrage des paquets entrant dans le réseau aide, entre autres, à garantir que les paquets ne sont pas « usurpés » pour ressembler aux paquets provenant du réseau interne de l'organisation. |
| **1.3.5** Ne pas autoriser le trafic sortant non autorisé de l'environnement des données du titulaire vers Internet. | **1.3.5** Examiner les configurations de pare-feu et de routeur pour vérifier que le trafic sortant de l'environnement des données du titulaire vers Internet est expressément autorisé. | Tout le trafic sortant, issu de l'environnement des données du titulaire, doit être évalué afin de s'assurer qu'il suit toutes les règles établies et autorisées. Les connexions doivent subir une inspection afin de restreindre le trafic aux seules communications autorisées (par exemple en limitant les adresses/ports sources ou de destination et/ou en bloquant le contenu). |
| **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** Examiner les configurations de pare-feu et de routeur pour vérifier que le pare-feu effectue un contrôle avec état (filtrage dynamique des paquets). (Seules les connexions établies doivent être autorisées, et seulement si elles sont associées à une session précédemment établie.) | Un pare-feu qui effectue un contrôle des paquets avec état maintient « l'état » (ou le statut) de chaque connexion au pare-feu. En maintenant « l'état », le pare-feu sait si une réponse apparente à une connexion précédente est réellement une réponse valide et autorisée (puisqu'il conserve le statut de chaque connexion) ou s'il s'agit d'un trafic malveillant qui essaye de tromper le pare-feu pour qu'il accepte la connexion. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.3.7** Placer les composants du système qui stockent les données du titulaire (tels qu'une base de données) dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés. | **1.3.7** Examiner les configurations de pare-feu et de routeur pour vérifier que les composants du système qui stockent les données du titulaire se trouvent dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés. | Si les données de titulaires de carte se trouvent dans la DMZ, il est plus facile pour les pirates externes d'accéder à ces informations, puisqu'il a moins de couches à pénétrer. Sécuriser les composants du système qui stockent les données du titulaire dans une zone de réseau externe qui est séparée de la DMZ et des autres réseaux non autorisés par un pare-feu peut empêcher le trafic non autorisé du réseau d'atteindre le composant du système.<br>***Remarque :*** *Cette condition n'est pas destinée à être appliquée au stockage temporaire des données du titulaire dans la mémoire volatile.* |
| **1.3.8** Ne pas divulguer les adresses IP et les informations d'acheminement confidentielles à des parties non autorisés.<br>***Remarque :*** *Quelques-unes des méthodes permettant de dissimuler les adresses IP sont présentées ci-après :*<br>• *Traduction d'adresse réseau (Network Address Translation – NAT) ;*<br>• *Protéger les serveurs contenant des données du titulaire derrière des serveurs proxy/pare-feu ;*<br>• *Retrait ou filtrage des annonces d'acheminement pour les réseaux privés employant des adresses enregistrées ;*<br>• *Utilisation interne de l'espace d'adresse RFC1918 au lieu d'adresses enregistrées.* | **1.3.8.a** Examen configurations de pare-feu et de routeur pour 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.<br>**1.3.8.b** Interroger le personnel et examiner la documentation pour vérifier que toute divulgation d'adresses IP et d'informations d'acheminement confidentielles à des entités externes est autorisée. | Restreindre la diffusion des adresses IP internes ou privées est essentiel pour empêcher un pirate « d'apprendre » les adresses IP du réseau interne et d'utiliser cette information pour accéder au réseau.<br>Les méthodes utilisées pour remplir cette condition varient en fonction de la technologie réseau spécifique utilisée. Par exemple, les contrôles utilisés pour satisfaire à cette condition peuvent différer entre des réseaux IPv4 et IPv6. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **1.4** Installer un logiciel pare-feu personnel sur tout appareil portable et/ou ordinateur appartenant à un employé équipé d'une connexion à Internet (par exemple, les ordinateurs portables utilisés par les employés), qui est utilisé pour accéder au réseau. Les configurations de pare-feu comprennent que :<br>• Les réglages de configuration spécifiques sont définis pour les logiciels de pare-feu personnel.<br>• Le logiciel de pare-feu personnel fonctionne effectivement.<br>• Le logiciel de pare-feu personnel ne peut pas être altéré par les utilisateurs d'appareils mobiles et/ou appartenant aux employés. | **1.4.a** Examiner les politiques et les normes de configuration pour vérifier :<br>• Un logiciel pare-feu personnel est requis pour tous les appareils portables et/ou détenus par les employés équipés d'une connexion à Internet (par exemple, ordinateurs portables dont se servent les employés), qui sont utilisés en dehors du réseau et pour accéder au réseau de l'organisation.<br>• Les réglages de configuration spécifiques sont définis pour les logiciels de pare-feu personnel.<br>• Le logiciel de pare-feu personnel est configuré pour fonctionner effectivement.<br>• Le logiciel pare-feu personnel est configuré de sorte qu'il ne puisse pas être modifiée par les utilisateurs d'appareils portables et/ou appartenant à des employés. | Les appareils informatiques portables qui peuvent se connecter à Internet depuis l'extérieur du pare-feu de l'entreprise sont plus vulnérables aux menaces basées sur Internet. L'utilisation de pare-feu personnel aide à protéger les appareils des attaques originaires d'Internet qui pourraient utiliser l'appareil pour accéder aux systèmes et aux données de l'organisation une fois que l'appareil et à nouveau connecté au réseau.<br>Les réglages spécifiques de configuration de pare-feu sont déterminés par l'organisation.<br>***Remarque :*** *Cette condition s'applique aux ordinateurs détenus par la société ou par l'entreprise. Les systèmes qui ne peuvent pas être gérés selon la politique de l'entreprise introduisent une faiblesse dans le périmètre et procurent aux individus malveillants des opportunités à exploiter. Permettre aux systèmes non autorisés de se connecter au réseau d'une organisation pourrait permettre l'accès des pirates et autres utilisateurs malveillants.* |
| | **1.4.b** Inspecter un échantillon des appareils mobiles et/ou détenus par les employés pour vérifier que :<br>• Un logiciel de pare-feu personnel est installé et configuré selon les paramètres de configuration spécifiques de l'organisation.<br>• Le logiciel de pare-feu personnel fonctionne effectivement.<br>• Le logiciel de pare-feu personnel ne peut pas être altéré par les utilisateurs d'appareils mobiles et/ou appartenant aux employés. | |
| **1.5** Assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des pare-feu sont documentées, utilisées et connues de toutes les parties concernées. | **1.5** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la gestion des pare-feu sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour assurer que les pare-feu et les routeurs sont continuellement gérés de sorte que les accès non-autorisés au réseau soient empêchés. |

### *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 | DIRECTIVES |
|---|---|---|
| **2.1** Changer systématiquement les paramètres par défaut définis par le fournisseur ou désactiver les comptes par défaut inutiles **avant** d'installer un système sur le réseau.<br><br>Cette pratique s'applique à TOUS les mots de passe par défaut, y compris, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, application ou comptes de système, *point de vente (*POS*)* terminaux, chaînes de communauté de protocoles de gestion de réseau simple [SNMP], etc.). | **2.1.a** Choisir un échantillon des composants du système et essayer d'ouvrir une session (avec l'aide de l'administrateur du système) sur les appareils et applications en utilisant les comptes et mots de passe par défaut fournis par le fournisseur, pour vérifier que TOUS les mots de passe par défaut (y compris ceux des systèmes d'exploitation, des logiciels qui assurent des services de sécurité, des comptes d'application et de système, des terminaux de POS et des chaînes de communauté de protocole de gestion simple de réseau [SNMP]) ont 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.) | Les individus malveillants (à l'intérieur ou à l'extérieur d'une organisation) utilisent souvent les paramètres par défaut définis par le fournisseur, noms de compte et mots de passe, pour compromettre le logiciel du système d'exploitation, les applications et les systèmes sur lesquels ils sont installés. Dans la mesure où ces paramètres par défaut sont souvent publiés et sont bien connus des communautés de pirates, changer ces paramètres laissera le système moins vulnérable aux attaques.<br><br>Même si un compte par défaut n'est pas censé être utilisé, changer le mot de passe par défaut pour un mot de passe unique et robuste, puis désactiver le compte, empêchera qu'un individu malveillant puisse réactiver le compte et obtenir un accès avec le mot de passe par défaut. |
| | **2.1.b** Pour l'échantillon de composants du système, vérifier que tous les comptes par défaut inutiles (y compris les comptes utilisés par les systèmes d'exploitation, les applications, les systèmes, les terminaux de POS, SNMP, etc.) sont éliminés ou désactivés. | |
| | **2.1.c** Interroger le personnel et examiner la documentation connexe pour vérifier que :<br>• Tous les paramètres de fournisseur par défaut (y compris les mots de passe par défaut des systèmes d'exploitation, les logiciels assurant des services de sécurité, les comptes d'application et de système, les terminaux de POS, les chaînes de communauté SNMP, etc.) sont changés avant qu'un système ne soit installé sur le réseau.<br>• Les comptes par défaut inutiles (y compris les comptes utilisés par les systèmes d'exploitation, les applications, les systèmes, les terminaux de POS, SNMP, etc.) sont éliminés ou désactivés avant qu'un système ne soit installé sur le réseau. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **2.1.1** Pour les environnements sans fil connectés à l'environnement des données du titulaire ou qui transmettent des données du titulaire, changer TOUS les paramètres par défaut définis par le fournisseur à l'installation, notamment les clés de cryptage sans fil, les mots de passe et les chaînes de communauté SNMP. | **2.1.1.a** Interroger le personnel responsable et examiner la documentation connexe pour vérifier que :<br>• Les clés de cryptage ont été modifiées du réglage par défaut lors de l'installation.<br>• Les clés de cryptage par défaut sont modifiées à chaque fois qu'une personne qui les connaît quitte la société ou change de poste. | Si les réseaux sans fil ne sont pas déployés avec une configuration de sécurité suffisante (y compris par la modification des paramètres par défaut), des renifleurs sans fil peuvent intercepter le trafic, capturer facilement des données et des mots de passe et pénétrer sans difficulté le réseau pour l'attaquer.<br>En outre, le protocole d'échange de clés de l'ancienne version de cryptage 802.11x (Wired Equivalent Privacy -confidentialité équivalente aux transmissions par fil WEP) a été décrypté et peut rendre le cryptage inutile. Le firmware des dispositifs doit être mis à jour pour prendre en charge des protocoles plus sécurisés. |
| | **2.1.1.b** Interroger le personnel et examiner les politiques et les procédures vérifier que :<br>• Les chaînes de communauté SNMP par défaut doivent être modifiées à l'installation.<br>• Les mots/phrases de passe des points d'accès doivent être modifiés à l'installation. | |
| | **2.1.1.c** Examiner la documentation du fournisseur et ouvrir une session sur les dispositifs sans-fil, avec l'aide de l'administrateur du système, pour vérifier que :<br>• Les chaînes de communauté SNMP par défaut ne sont pas utilisées.<br>• Les mots/phrases de passe par défaut des points d'accès ne sont pas utilisés. | |
| | **2.1.1.d** Examiner la documentation du fournisseur et observer les paramètres de la configuration sans-fil pour vérifier que le firmware des périphériques sans-fil est mis à jour de manière à prendre en charge un cryptage robuste pour :<br>• L'authentification des réseaux sans fil ;<br>• La transmission sur les réseaux sans fil. | |
| | **2.1.1.e** Examiner la documentation du fournisseur et observer les paramètres de configuration sans-fil pour vérifier que les autres paramètres par défaut liés à la sécurité ont été changés, le cas échéant. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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.<br><br>Les sources des normes renforçant les systèmes en vigueur dans le secteur, comprennent, sans s'y limiter, les organismes suivants :<br>• Center for Internet Security (CIS – Centre de sécurité Internet)<br>• International Organization for Standardization (ISO – Organisation des normes internationales)<br>• SysAdmin Audit Network Security (SANS) Institute (Institut SANS)<br>• 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.<br><br>**2.2.b** Examiner les politiques et interroger le personnel pour vérifier que les normes de configuration du système sont mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités, qui se trouve dans la condition 6.1.<br><br>**2.2.c** Examiner les politiques et interroger le personnel pour vérifier que les normes de configuration du système sont appliquées lorsque de nouveaux systèmes sont configurés et que leur mise en place est vérifiée lorsqu'un système est installé sur le réseau.<br><br>**2.2.d** Vérifier que les normes de configuration du système comprennent les procédures suivantes pour tous les types de composants de système :<br>• Changer tous les paramètres par défaut fournis par le fournisseur et éliminer tous les comptes par défaut inutiles<br>• Appliquer uniquement une fonction primaire par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents<br>• Activer uniquement les services, protocoles, démons, etc. nécessaires pour le fonctionnement du système.<br>• Mettre en place des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaires que l'on estime non sécurisés.<br>• Configurer les paramètres de sécurité du système pour empêcher les actes malveillants<br>• Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus. | De nombreux systèmes d'exploitation, bases de données et applications d'entreprise présentent des points faibles connus et il existe des moyens également connus de les configurer pour résoudre les vulnérabilités de sécurité. Pour aider ceux qui manquent d'expertise en sécurité, un grand nombre d'entreprises de sécurité ont défini des recommandations et des directives visant à renforcer les systèmes, qui expliquent comment corriger ces faiblesses.<br><br>Les exemples de sources de directives sur les normes de configuration comprennent notamment : www.nist.gov, www.sans.org, et www.cisecurity.org, www.iso.org ainsi que les fournisseurs de produit.<br><br>Les normes de configuration de système doivent également être conservées à jour afin de garantir que les faiblesses récemment identifiées sont corrigées avant l'installation du système sur le réseau. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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).<br><br>***Remarque :*** *Lorsque des technologies de virtualisation sont utilisées, n'appliquer qu'une fonction primaire par composant de système virtuel.* | **2.2.1.a** Sélectionner un échantillon de composants du système et inspecter les configurations du système pour vérifier qu'une seule fonction primaire par serveur est implémentée.<br><br>**2.2.1.b** Si des technologies de virtualisation sont utilisées, inspecter les configurations de système pour vérifier que seule une fonction primaire est déployée par composant de système ou dispositif virtuel. | Si des fonctions de serveur qui ont besoin de niveaux de sécurité différents sont situées sur le même serveur, le niveau de sécurité des fonctions ayant le besoin de sécurité le plus important devront être réduits pas la présence de fonctions à moindre sécurité. En outre, les fonctions de serveur ayant un niveau de sécurité moins important sont susceptibles d'introduire une faiblesse dans les autres fonctions du même serveur. En considérant les besoins de sécurité de différentes fonctions du serveur dans le cadre des normes de configuration du système et des processus connexes, les organisations peuvent assurer que les fonctions qui requièrent des niveaux de sécurité différents ne coexistent pas sur le même serveur. |
| **2.2.2** Activer uniquement les services, protocoles, démons, etc., nécessaires pour le fonctionnement du système. | **2.2.2.a** Sélectionner un échantillon de composants du système et examiner les démons, les protocoles et les services activés du système pour vérifier que seuls les services ou protocoles nécessaires sont activés.<br><br>**2.2.2.b** Identifier tout service, démon, ou protocole actif et non sécurisé et interroger le personnel pour vérifier qu'ils sont justifiés selon les normes de configuration documentées. | Comme indiqué à la condition 1.1.6, une entreprise peut avoir besoin de nombreux protocoles (ou les avoir activés par défaut) et ceux-ci sont fréquemment utilisés par les individus malveillants pour endommager un réseau. Inclure cette condition dans le cadre des normes de configuration d'une organisation et des processus connexes garantit que seuls les services et protocoles nécessaires sont activés. |
| **2.2.3** Mettre en œuvre les fonctions de sécurité pour tout service, protocole ou démon nécessaires qui sont 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 tels que NetBIOS, le partage de fichiers, Telnet, FTP, etc. | **2.2.3** Inspecter les réglages de configuration pour vérifier que les fonctions de sécurité sont documentées et mises en œuvre pour tous les services, démons ou protocoles non sécurisés. | Activer les fonctions de sécurité avant que les nouveaux serveurs ne soient déployés empêchera que des serveurs soient installés dans l'environnement ayant des configurations non sécurisées.<br><br>Assurer que tous les services, protocoles et démons non sécurisés soient sécurisés à l'aide de fonctions de sécurité appropriées rend la tâche difficile pour les individus malveillants qui cherchent à tirer avantage des points compromis généralement utilisés dans un réseau. |
| **2.2.4** Configurer les paramètres de sécurité du système pour empêcher les | **2.2.4.a** Interroger les administrateurs système et/ou les responsables de la sécurité pour vérifier qu'ils connaissent les | Les normes de configuration et les processus connexes doivent répondre de manière spécifique |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| actes malveillants. | paramètres de sécurité courants des composants du système. | aux réglages et aux paramètres qui ont des implications de sécurité connues pour chaque type de système utilisé.<br><br>*(suite à la page suivante)* |
| | **2.2.4.b** Examiner les normes de sécurité du système pour vérifier que les paramètres de sécurité courants sont inclus. | |
| | **2.2.4.c** Sélectionner un échantillon de composants du système et inspecter les paramètres de sécurités communs pour vérifier qu'ils sont configurés de manière appropriée et selon les normes de configuration. | Pour que les systèmes soient configurés de manière sécurisée, le personnel responsable de la configuration et/ou de l'administration des systèmes doivent être bien informés des paramètres et des réglages de sécurité spécifiques qui s'appliquent au système. |
| **2.2.5** Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus. | **2.2.5.a** Sélectionner un échantillon de composants du système et inspecter la configuration pour vérifier que toutes les fonctionnalités qui ne sont pas nécessaires (par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers, etc.) sont supprimées. | Les fonctions superflues peuvent apporter une opportunité supplémentaire d'accéder au système pour des individus malveillants. En éliminant les fonctions superflues, les organisations peuvent se concentrer sur la sécurisation des fonctions qui sont requises et sur la réduction du risque que des fonctions inconnues soient exploitées.<br><br>Inclure ces normes et ces processus renforçant les serveurs répond aux implications de sécurité spécifiques associées avec les fonctions superflues (par exemple, avec la suppression/désactivation de la fonction FTP ou du serveur Web si celui-ci n'exécute pas ces fonctions). |
| | **2.2.5.b**. Examiner la documentation et les paramètres de sécurité pour vérifier que les fonctions activées sont documentées et prennent en charge une configuration sécurisée. | |
| | **2.2.5.c**. Examiner la documentation et les paramètres de sécurité pour vérifier que seules les foncions documentés sont présentes sur les composants de système échantillonnés. | |
| **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 via le Web et autres accès administratifs non-console. | **2.3** Sélectionner un échantillon de composants du système et vérifier l'accès administratif non-console est crypté en suivant la procédure ci-après : | Si l'administration non console (y compris l'administration à distance) ne s'effectue pas par le biais d'une authentification sécurisée et de communications cryptées, les informations administratives ou de niveau opérationnel sensible (comme les mots de passe de l'administrateur) peuvent être interceptées. Un individu malveillant pourrait utiliser ces informations pour accéder au réseau, se substituer à l'administrateur et subtiliser des données. |
| | **2.3.a** Observer un administrateur se connecter à chaque système et examiner les configurations de 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** Examiner les services et les fichiers de paramètre sur le système pour déterminer que Telnet et d'autres commandes de connexion à distance non sécurisées ne sont pas | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | disponibles pour l'accès non console. | Les protocoles en texte clair (tels que HTTP, Telnet, etc.) ne cryptent pas les détails de trafic ou de connexion, il est donc plus facile pour une personne malveillante d'intercepter cette information.<br><br>Pour être considérés comme une « cryptographie robuste », des protocoles reconnus par le secteur avec des clés robustes et une gestion de clé appropriée doivent être mis en place et être applicables pour le type de technologie utilisée. (Consulter « cryptographie robuste » dans le *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*.) |
| | **2.3.c** Observer un administrateur se connecter à chaque système pour vérifier que l'accès administrateur aux interfaces de gestion Web est crypté au moyen d'une méthode de cryptage robuste. | |
| | **2.3.d** Examiner la documentation du fournisseur et interroger le personnel pour vérifier qu'une cryptographie robuste est implémentée pour la technologie utilisée, conformément aux meilleures pratiques du secteur et/ou aux recommandations du fournisseur. | |
| **2.4** Maintenir un inventaire des composants du système qui se trouvent dans le champ d'application de la norme PCI DSS. | **2.4.a** Examiner l'inventaire de système pour vérifier qu'une liste de composants de logiciel et de matériel est maintenue et comprend une description de la fonction/utilisation de chacun de ces composants. | Maintenir une liste actualisée de tous les composants du système permettra à une organisation de définir précisément et efficacement la portée de son environnement pour l'implémentation des contrôles PCI DSS. Sans inventaire, certains composants du système pourraient être oubliés et être exclus par inadvertance des normes de configuration de l'organisation. |
| | **2.4.b** Interroger le personnel pour vérifier que l'inventaire documenté est tenu à jour. | |
| **2.5** Assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres par défaut du fournisseur et des autres paramètres de sécurité sont documentées, utilisées et connues de toutes les parties concernées. | **2.5** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres par défaut du fournisseur et des autres paramètres de sécurité sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles quotidiennes pour assurer que les paramètres par défaut du fournisseur et les autres paramètres de sécurité sont continuellement gérés pour empêcher les configurations non sécurisées. |
| **2.6** Les fournisseurs d'hébergement partagé doivent protéger l'environnement hébergé et les données du titulaire de chaque entité. Ces fournisseurs doivent satisfaire aux exigences spécifiques décrites dans *l'annexe A : Autres clauses de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.* | **2.6** 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). | Ceci est destiné aux fournisseurs d'hébergement qui proposent des environnements d'hébergement partagé à des clients multiples sur le même serveur. Lorsque les données sont sur le même serveur et sous contrôle d'un seul environnement, souvent les réglages de ces serveurs partagés ne sont pas gérables par les clients individuels. Cela permet aux clients d'ajouter des fonctions et des scripts non sécurisés susceptibles d'affecter la |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | | sécurité des environnements de tous les autres clients et, par conséquent, permettent à un individu malveillant de compromettre les données d'un client, et par là, d'accéder à toutes les données des autres clients. Voir *l'annexe A* pour les détails des conditions. |

# Protection des données du titulaire

### *Condition 3 : Protéger les données du titulaire 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 du titulaire. 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 aussi être envisagées pour potentiellement limiter les risques. Par exemple, pour minimiser les risques, éviter de stocker les données du titulaire à moins que cela ne soit absolument nécessaire, tronquer les données du titulaire 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 | DIRECTIVE |
|---|---|---|
| **3.1** Garder le stockage de données du titulaire à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données, qui comprennent au moins les mesures suivantes pour le stockage des données du titulaire (CHD) :<br>• La limitation de la quantité de données stockées et du délai de conservation restreints aux obligations professionnelles, légales et réglementaires ;<br>• Des processus pour la suppression sécurisée des données devenues inutiles ;<br>• Des conditions de conservation | **3.1.a** Examiner les politiques, procédures et processus de conservation et d'élimination des données pour vérifier qu'elles comprennent les points suivants :<br>• Les conditions légales, réglementaires et commerciales pour la conservation des données, y compris<br>• Les conditions spécifiques de conservation des données du titulaire (par exemple, ces données doivent être conservées pendant une période X pour des raisons professionnelles Y) ;<br>• La suppression sécurisée des données du titulaire lorsqu'elles ne sont plus requises pour les besoins légaux, réglementaires ou commerciaux.<br>• La couverture de la totalité du stockage des données du titulaire<br>• Un processus trimestriel pour l'identification et la suppression sécurisées des données du titulaire stockées excédant les conditions de conservation définies. | Une politique officielle de conservation des données identifie les données qui doivent être conservées, leur lieu de conservation afin de pouvoir les détruire en toute sécurité dès qu'elles ne sont plus nécessaires.<br>Les seules données du titulaire à stocker après autorisation sont le numéro de compte primaire ou PAN (rendu illisible), la date d'expiration, le nom du titulaire de la carte et le code de service.<br>Comprendre où les données du titulaire sont situées est nécessaire pour que ces données puissent être conservées ou éliminées lorsqu'elles ne sont plus nécessaires. Afin de définir les conditions appropriées de conservation, une entreprise doit d'abord comprendre les besoins de son activité ainsi que les obligations légales et réglementaires qui |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| spécifiques pour les données du titulaire ;<br>• Un processus trimestriel pour l'identification et la suppression sécurisées des données du titulaire stockées excédant les conditions de conservation définies. | **3.1.c** Interroger le personnel pour vérifier que :<br>• Tous les emplacements où des données du titulaire sont stockées sont inclus dans les processus de rétention et d'élimination.<br>• Un processus trimestriel automatique ou manuel est en place pour l'identification et la suppression sécurisée des données du titulaire stockées.<br>• Le processus trimestriel automatique ou manuel est effectué sur tous les emplacements de données du titulaire. | s'appliquent à son secteur et/ou au type de données conservées.<br><br>*(suite à la page suivante)* |
| | **3.1.c** Pour un échantillon des composants du système qui stockent les données du titulaire :<br>• Examiner les archives de fichiers et de système pour vérifier que les données stockées n'excèdent pas les conditions définies dans la politique de conservation des données.<br>• Observer le mécanisme d'élimination pour vérifier que les données sont éliminées de manière sécurisée. | L'identification et la suppression des données stockées qui ont dépassé la période de rétention spécifiée empêchent la rétention de données qui ne sont plus utiles. Ce processus peut être automatique ou manuel, ou une combinaison des deux. Par exemple, une procédure de programmation (automatique ou manuelle) pour localiser et supprimer les données et/ou un examen manuel des zones de stockage de données pourraient être effectués.<br>La mise en œuvre de méthodes de destruction sécurisées garantit que les données ne pourront pas être récupérées une fois qu'elles ne seront plus nécessaires.<br>***Il ne faut pas oublier qu'il est inutile de stocker ce dont on n'a pas besoin !*** |
| **3.2** Ne stocker aucune donnée d'identification sensible après autorisation (même cryptée). Si des données d'identification sensibles sont reçues, rendre toutes les données irrécupérables à la fin du processus d'autorisation.<br>*Il est permis aux émetteurs et aux* | **3.2.a** Pour les émetteurs et/ou sociétés qui prennent en charge les services d'émission et stockent des données d'identification sensibles, examiner les politiques et interroger le personnel pour vérifier qu'il y a une justification commerciale documentée pour le stockage des données d'identification sensibles. | Les données d'identification sensibles sont constituées par les données complètes de piste, le code ou la valeur de validation de carte et les données PIN. Le stockage des données d'identification sensibles n'est pas autorisé ! Ces données sont précieuses pour les individus malveillants, car elles leur permettent de créer de fausses cartes de paiement et de procéder à des transactions frauduleuses. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| *sociétés qui prennent en charge les services d'émissions de stocker des données d'identification sensibles si :*<br>• Une justification commerciale existe et les données sont stockées de manière sécurisée<br><br>Les données concernées sont mentionnées dans les conditions 3.2.1 à 3.2.3 suivantes : | **3.2.b** Pour les émetteurs et/ou les sociétés qui prennent en charge les services d'émission et stockent des données d'identification sensibles, examiner les stockages de données et les configurations de système pour vérifier que les données d'identification sensibles sont sécurisées. | Les entités qui émettent des cartes de paiement ou qui fournissent ou soutiennent des services d'émission créeront et contrôleront souvent des données d'identification dans le cadre de la fonction d'émission. Les entreprises peuvent exécuter, permettre ou prendre en charge des services de stockage des données d'identification sensibles UNIQUEMENT SI elles en ont un besoin professionnel légitime.<br><br>Il faut remarquer que l'ensemble des conditions de la norme PCI DSS s'applique aux émetteurs et que la seule exception les concernant, ainsi que leurs processeurs, est que les données d'identification sensibles peuvent être conservées s'il existe une raison légitime pour ce faire. Une raison légitime est une raison nécessaire pour l'accomplissement de la fonction fournie pour l'émetteur, et non une raison de pure convenance. Ces données doivent être stockées en sécurité, conformément à toutes les conditions de la norme PCI DSS et à aux conditions spécifiques de la marque de carte de paiement. |
| | **3.2.c** Pour toutes les autres entités, si des données d'identification sensibles sont reçues, examiner les politiques et procédures et examiner les configurations de système pour vérifier que les données ne sont pas conservées après autorisation. | |
| | **3.2.b** Pour toutes les autres entités, si des données d'identification sensibles sont reçues, examiner les procédures et les processus d'élimination sécurisée des données pour vérifier que les données ne son pas récupérables. | Pour les entités non-émettrices qui conservent des données d'identification sensibles, la post-autorisation n'est pas permise. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **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 désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique.<br><br>***Remarque :*** *dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique suivants :*<br>• *Le nom du titulaire de la carte*<br>• *Le numéro de compte primaire (PAN) ;*<br>• *La date d'expiration ;*<br>• *Le code de service*<br>*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, ou donnée équivalente sur une puce, n'est en aucun cas stockée après autorisation :<br>• Les données de transaction entrantes ;<br>• Tous les journaux (par exemple, transactions, historique, débogage, erreur) ;<br>• Les fichiers d'historique ;<br>• Les fichiers trace ;<br>• Plusieurs schémas de bases de données ;<br>• Contenu des bases de données. | Si les données complètes de piste étaient stockées, les individus malveillants qui obtiennent ces données pourraient les utiliser pour reproduire et vendre des cartes de paiement pour effectuer des transactions frauduleuses. |
| **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 absentes. | **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 après autorisation :<br>• Les données de transaction entrantes ;<br>• Tous les journaux (par exemple, transactions, historique, débogage, erreur) ;<br>• Les fichiers d'historique ;<br>• Les fichiers trace ;<br>• Plusieurs schémas de bases de données ;<br>• Contenu des bases de données. | Le code de validation des cartes est destiné à protéger les transactions « carte absente », transactions effectuées via Internet ou ordre de paiement par e-mail/téléphone (MOTO), en l'absence du consommateur et de la carte.<br><br>Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions frauduleuses par MO/TO et Internet. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **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 pas stockés après autorisation :<br>• Les données de transaction entrantes ;<br>• Tous les journaux (par exemple, transactions, historique, débogage, erreur) ;<br>• Les fichiers d'historique ;<br>• Les fichiers trace ;<br>• Plusieurs schémas de bases de données ;<br>• Contenu des bases de données. | Ces valeurs ne doivent être connues que du titulaire de la carte ou de la banque émettrice de la carte. Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions de débit frauduleuses à l'aide du code PIN (par exemple, retraits à un GAB). |
| **3.3** Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel dont le besoin commercial est légitime puisse voir le PAN dans sa totalité.<br>***Remarque :*** *Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données du titulaire, par exemple, pour les reçus des points de vente (POS).* | **3.3.a** Examiner les politiques et les procédures écrites de masquage de l'affichage de PAN pour vérifier que :<br>• Une liste des rôles qui ont besoin d'accéder au PAN entier est documentée, ainsi que le besoin commercial légitime qu'à chaque rôle à avoir cet accès.<br>• Le PAN doit être masqué de sorte que seul le personnel qui a un besoin professionnel légitime puisse voir la totalité du PAN.<br>• Tous les autres rôles qui ne sont pas spécifiquement autorisés à voir le PAN entier doivent uniquement voir des PAN masqués. | Grâce à l'affichage du PAN intégral sur un écran d'ordinateur, un reçu de carte de paiement, un fax où un rapport sur papier, des individus non autorisés pourraient y avoir accès et l'utiliser de manière frauduleuse. Assurer que le PAN est uniquement affiché pour les personnes ayant un besoin commercial légitime de le voir minimise les risques de personnes non autorisées obtenant accès aux données de PAN.<br>Cette condition porte sur la protection du PAN *visible* sur les écrans, reçus papier, impressions, etc. et elle ne doit pas être confondue avec la condition 3.4 de protection du PAN lorsqu'il est *stocké* dans des fichiers, des bases de données, etc. |
| | **3.3.b** Examiner les configurations de système pour vérifier que le PAN entier est uniquement affiché pour les utilisateurs/rôles ayant un besoin commercial documenté et que le PAN est masqué pour toutes les autres demandes. | |
| | **3.3.c** Examiner l'affichage des PAN (par exemple, à l'écran, sur les reçus papier) afin de vérifier que les PAN sont masqués lors de l'affichage des données du titulaire, sauf pour les utilisateurs qui ont un besoin professionnel légitime de voir l'intégralité du PAN. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **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 :<br>• Hachage unilatéral s'appuyant sur une méthode cryptographique robuste (la totalité du PAN doit être hachée) ;<br>• Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ;<br>• Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ;<br>• Cryptographie robuste associée aux processus et procédures de gestion des clés.<br>***Remarque :*** *Il s'agit d'un effort* | **3.4.a** Examiner 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) pour vérifier que le PAN est rendu illisible en utilisant l'une des méthodes suivantes :<br>• Hachage unilatéral s'appuyant sur une méthode cryptographique robuste,<br>• Troncature<br>• Jetons et pads d'index, les pads devant être stockés de manière sécurisée ;<br>• Cryptographie robuste associée aux processus et procédures de gestion des clés.<br>**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).<br>**3.4.c** Examiner un échantillon de support amovible (par exemple, bandes de sauvegarde) pour s'assurer que le PAN est rendu illisible. | Les PAN stockés sur les supports de stockage principal (bases de données ou fichiers plats comme les feuilles de calcul) et autres supports secondaires (sauvegardes ou journaux d'audit, d'anomalies ou de dépannage) doivent tous être protégés.<br>Les fonctions de hachage unilatéral reposant sur une cryptographie robuste peuvent être utilisées pour rendre les données du titulaire illisibles. Ces fonctions de hachage sont appropriées lorsqu'il n'est pas nécessaire de récupérer le numéro d'origine (le hachage unilatéral est irréversible). Il est recommandé, bien que ce ne soit pas une condition, qu'une valeur supplémentaire aléatoire soit ajoutée aux données du titulaire avant le hachage pour réduire la possibilité qu'un pirate puisse comparer les données (et découvrir le PAN) à des tableaux de valeurs de hachage pré-calculées. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| *relativement peu important pour un individu malveillant de reconstruire les données du PAN d'origine, s'il a à la fois accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachées et tronquées du même PAN sont présentes dans l'environnement de l'entité, des contrôles supplémentaires doivent être en place pour garantir que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.* | **3.4.d** Examiner un échantillon des journaux d'audit pour confirmer que le PAN est bien illisible ou supprimé des journaux. | La troncature vise à ne stocker qu'une partie seulement du PAN (sans dépasser les six premiers et les quatre derniers chiffres).<br><br>Un « jeton d'index » est un élément cryptographique qui remplace le PAN en fonction d'un indice donné, par une valeur imprévisible. Un pad ponctuel est un système dans lequel une clé privée, générée de façon aléatoire, est utilisée une seule fois pour crypter un message, qui est ensuite décrypté à l'aide de la clé et du pad ponctuel correspondant.<br><br>L'objectif de la cryptographie robuste (selon la définition du *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*) est de fonder le cryptage sur un algorithme testé et accepté par le secteur (non pas un algorithme exclusif ou « développé en interne »), avec de robustes clés cryptographiques.<br><br>En corrélant les versions hachées et tronquées d'un PAN donné, un individu malveillant peut facilement reconstituer le PAN d'origine. Des contrôles empêchant la corrélation de ces données permettront de garantir que le PAN d'origine reste illisible. |
| **3.4.1** Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès logique doit être géré séparément et indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales ou des justificatifs génériques de connexion au réseau). Les clés de décryptage ne doivent pas être | **3.4.1.a** Si un cryptage par disque est utilisé, inspecter la configuration et le processus d'authentification pour 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 ou des justificatifs génériques de connexion au réseau).<br><br>**3.4.1.b** Examiner les processus et interroger le personnel pour vérifier que les clés cryptographiques sont stockées de manière sécurisée (par exemple, sur des supports amovibles correctement protégés avec des contrôles d'accès stricts). | Le but de cette condition est d'adresser l'acceptabilité du cryptage par disque pour rendre les données du titulaire illisibles. Le cryptage par disque crypte la totalité du disque/de la partition sur un ordinateur et décrypte automatiquement les informations à la demande d'un utilisateur autorisé. De nombreuses solutions de cryptage par disque interceptent les opérations de lecture et d'écriture du système d'exploitation et exécutent les transformations cryptographiques appropriées sans autre action particulière de l'utilisateur que la saisie d'un mot de passe ou phrase au démarrage du système ou au début |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| associées à des comptes d'utilisateur. | **3.4.1.c** Examiner les configurations et observer les processus pour vérifier que les données du titulaire sur les supports amovibles sont cryptées où qu'elles soient stockées.<br><br>***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.* | d'une session. Compte tenu de ces caractéristiques du cryptage par disque, pour être conforme à cette condition, la méthode ne peut pas :<br>1) Utiliser le même authentifiant de compte utilisateur que le système d'exploitation, ou<br>2) Utiliser une clé de décryptage qui est associée ou dérivée de la base de données du compte d'utilisateur local de système ou des justificatifs génériques de connexion au réseau.<br><br>Le cryptage total par disque aide à protéger les données en cas de perte physique d'un disque et il peut donc convenir aux périphériques portables qui stockent les données du titulaire. |
| **3.5** Documenter et mettre en œuvre des procédures pour protéger les clés utilisées pour sécuriser le données du titulaire stockées contre la divulgation et l'utilisation illicites :<br><br>***Remarque :*** *Cette condition s'applique également aux clés utilisées pour crypter les données du titulaire stockées et elle s'applique aux clés de cryptage de clé utilisées pour protéger les clés de cryptage de données – ces clés de cryptage de clés doivent être au moins aussi robustes que la clé de cryptage de données.* | **3.5** Vérifier les politiques et procédures de gestion des clés pour vérifier que des processus sont spécifiés pour protéger les clés utilisées pour le cryptage des données du titulaire contre la divulgation et l'utilisation illicite en procédant comme suit :<br>• L'accès aux clés cryptographiques est restreint au plus petit nombre d'opérateurs possible.<br>• Les clés de cryptage de clés sont au moins aussi robustes que les clés de cryptage de données qu'elles protègent.<br>• Les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données.<br>• Les clés sont stockées de manière sécurisée dans aussi peu d'emplacements et sous aussi peu de formes que possible | Les clés cryptographiques doivent être parfaitement bien protégées, car tout individu qui parviendrait à y accéder pourrait décrypter les données. Les clés de cryptage de clés, si elles sont utilisées, doivent au moins être aussi robustes que les clés de cryptage de données afin de garantir une protection adéquate de la clé qui crypte les données aussi bien que des données cryptées à l'aide de la clé.<br><br>L'obligation de protéger les clés d'une divulgation et d'une utilisation illicites s'applique aux clés de cryptage des données comme à celles assurant le cryptage des clés. Une seule clé de cryptage de clé pouvant permettre d'accéder à de nombreuses clés de cryptage de données, il est nécessaire d'appliquer des mesures robustes pour protéger les clés de cryptage de clés. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **3.5.1** Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible. | **3.5.1** Examiner les listes d'accès utilisateur afin de vérifier que l'accès aux clés est restreint aux opérateurs strictement nécessaires. | Seul un petit nombre de personnes doit avoir accès aux clés cryptographiques (pour réduire le potentiel de rendre les données du titulaire visibles pour des parties non autorisées), en général ceux qui sont chargés de la gestion de ces clés. |
| **3.5.2** Stocker toujours les clés secrètes et privées utilisées pour crypter/décrypter les données sous l'une (ou sous plusieurs) des formes suivantes :<br>• Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stocké séparément de la clé de cryptage de données.<br>• Avec un dispositif cryptographique robuste (tel qu'un module de sécurité hôte (HSM) ou un dispositif de point d'interaction approuvé PTS)<br>• En tant que deux composants de clé ou partages de clé de pleine longueur au moins conformément à la méthode acceptée par l'industrie<br>***Remarque :*** *Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes.* | **3.5.2.a** Examiner les procédures documentées pour vérifier que les clés cryptographiques utilisées pour crypter/décrypter les données du titulaire doivent exister au moins sous l'une (ou sous plusieurs) des formes suivantes :<br>• Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stocké séparément de la clé de cryptage de données.<br>• Avec un dispositif cryptographique robuste (tel qu'un module de sécurité hôte (HSM) ou un dispositif de point d'interaction approuvé PTS)<br>• En tant que deux composants de clé ou partages de clé conformément à la méthode acceptée par l'industrie<br>**3.5.2.b** Examiner les configurations du système et les emplacements de stockage de clés pour vérifier que les clés cryptographiques utilisées pour crypter/décrypter les données du titulaire existent toujours au moins sous l'une (ou sous plusieurs) des formes suivantes :<br>• Cryptées avec une clé de cryptage de clé<br>• Avec un dispositif cryptographique robuste (tel qu'un module de sécurité hôte (HSM) ou un dispositif de point d'interaction approuvé PTS)<br>• En tant que deux composants de clé ou partages de clé conformément à la méthode acceptée par l'industrie | Les clés cryptographiques doivent être stockées de manière sécurisée pour prévenir des accès non autorisés ou inutiles qui pourraient provoquer l'exposition des données du titulaire.<br>Il n'est pas prévu de crypter les clés de cryptage de clés, mais celles-ci doivent cependant être protégées de la divulgation et de l'utilisation illicites comme le définit la condition 3.5 Si des clés de cryptage de clé sont utilisées, le stockage des clés de cryptage des clés dans des endroits matériels et/ou logiciels distincts de ceux des clés de cryptage de données réduit le risque d'accès non autorisé à ces deux types de clés. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| | **3.5.2.c** Lorsque des clés de cryptage de clé sont utilisées, examiner les configurations du système et les emplacements de stockage de clé pour vérifier que :<br>• Les clés de cryptage de clés sont au moins aussi robustes que les clés de cryptage de données qu'elles protègent.<br>• Les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données. | |
| **3.5.3** Stocker les clés cryptographiques dans aussi peu d'emplacements que possible. | **3.5.3** Examiner les emplacements de stockage de clé et observer les processus pour vérifier que les clés sont stockées dans aussi peu d'endroits que possible. | Le stockage des clés cryptographiques dans le moins d'endroits possible aide une organisation à suivre et à surveiller tous les emplacements de clés et à minimiser le potentiel que les clés soient exposées à des parties non autorisées. |
| **3.6** Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données du titulaire, notamment ce qui suit :<br>***Remarque :*** *De nombreuses normes du secteur pour la gestion des clés sont disponibles auprès de diverses ressources, notamment NIST, que vous trouverez à l'adresse suivante : http://csrc.nist.gov.* | **3.6.a** ***Procédures de test supplémentaires pour les prestataires de services :*** Si le prestataire de services partage des clés avec ses clients pour la transmission ou le stockage de données du titulaire, examiner la documentation apportée par le prestataire de service à ses clients pour vérifier qu'elle comprend 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.<br>**3.6.b** Examiner les procédures et les processus de gestion de clé utilisée pour le cryptage des données du titulaire et effectuer ce qui suit : | La manière dont les clés cryptographiques sont gérées est un aspect essentiel de la sécurité permanente de la solution de cryptage. Un bon processus de gestion des clés, qu'il soit manuel ou automatique, dans le cadre du produit de cryptage, se base sur les normes du secteur et prend en charge tous les éléments essentiels décrits aux points 3.6.1 à 3.6.8.<br>Donner des directives aux clients sur la manière de transmettre, stocker et mettre à jour les clés cryptographiques de manière sécurisée peut aider à empêcher que les clés soient mal gérées ou communiquées à des entités non autorisées.<br>Cette condition s'applique aux clés utilisées pour crypter les données du titulaire stockées ainsi qu'à toute clé de cryptage de clé associée. |
| **3.6.1** Génération de clés cryptographiques robustes | **3.6.1.a** Vérifier que des procédures de gestion des clés spécifient comment générer des clés robustes.<br>**3.6.1.b** Observer la méthode de génération des clés pour vérifier que des clés robustes sont générées. | La solution de cryptage doit générer des clés robustes, aux termes du Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS, dans le chapitre « cryptographie robuste ». L'utilisation de clés cryptographiques robustes augmente de manière significative le niveau de sécurité des données du titulaire. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **3.6.2** Sécuriser la distribution des clés cryptographiques | **3.6.2.a** Vérifier que des procédures de gestion des clés spécifient comment distribuer les clés de manière sécurisée.<br><br>**3.6.2.b** Observer la méthode de distribution des clés pour vérifier que les clés sont distribuées de manière sécurisée. | La solution de cryptage doit distribuer les clés de manière sécurisée, c'est-à-dire que les clés sont uniquement distribuées aux individus chargés de leur gestion identifiés au point 3.5.1 et qu'elles ne sont jamais distribuées en texte clair. |
| **3.6.3** Sécuriser le stockage des clés cryptographiques | **3.6.3.a** Vérifier que des procédures de gestion des clés spécifient comment stocker les clés de manière sécurisée.<br><br>**3.6.3.b** Observer la méthode de stockage de clé pour vérifier que les clés sont stockées de manière sécurisée. | La solution de cryptage doit stocker les clés de manière sécurisée, par exemple, en les cryptant à l'aide d'une clé de cryptage de clé. Le stockage des clés sans protection adéquate pourrait donner un accès aux pirates et provoquer le décryptage et l'exposition des données du titulaire. |
| **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.a** Vérifier que les procédures de gestion des clés comprennent une cryptopériode définie pour chaque type de clé en utilisation et définissent un processus de changement de clé à la fin de la ou les cryptopériodes définies.<br><br>**3.6.4.b** Interroger le personnel pour vérifier que les clés sont changées la fin de la ou des cryptopériodes définies. | La cryptopériode est la période durant laquelle une clé cryptographique donnée peut être utilisée dans le but pour lequel elle est prévue. Les facteurs à prendre en compte pour définir la cryptopériode sont, sans s'y limiter, la complexité de l'algorithme sous-jacent, la taille ou la longueur de la clé, le risque de compromission de la clé, et la sensibilité des données cryptées.<br><br>Il est impératif de changer les clés de cryptage une fois leur cryptopériode écoulée, afin de réduire le risque qu'un tiers se les procure et les utilise pour décrypter des données. |
| **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.<br><br>***Remarque :*** *Si les clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par* | **3.6.5.a** Vérifier que des procédures de gestion des clés spécifient les processus pour les points suivants :<br>• Le retrait ou le remplacement des clés lorsque l'intégrité de la clé a été affaiblie ;<br>• Le remplacement des clés compromises ou suspectées de l'être.<br>• Toute clé retirée ou remplacée n'est pas utilisée pour les opérations de cryptages.<br><br>**3.6.5.b** Interroger le personnel pour vérifier que des procédures sont mises en œuvre :<br>• Les clés sont retirées ou remplacées si nécessaire lorsque leur intégrité a été affaiblie, y compris lorsque | Les clés qui ne sont plus utilisées ou nécessaires, ou les clés dont on sait ou on soupçonne qu'elles sont compromises, doivent être révoquées et/ou détruites pour assurer qu'elles ne puissent plus être utilisées. Ces clés doivent être conservées (par exemple, pour prendre en charge des données cryptées archivées), elles doivent être parfaitement protégées.<br><br>La solution de cryptage doit également permettre et faciliter un processus de remplacement des clés qui doivent être remplacées ou dont on sait, ou dont on soupçonne qu'elles sont compromises. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| *exemple, en utilisant une clé de cryptage de clé). Les clés cryptographiques archivées doivent être utilisées uniquement pour un décryptage ou une vérification.* | quelqu'un connaissant la clé quitte la société.<br>• Les clés sont remplacées si on sait ou on soupçonne qu'elles sont compromises.<br>• Toute clé conservée après son retrait ou son remplacement n'est pas utilisée pour les opérations de cryptages. | |
| **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.<br><br>***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.a** Vérifier que des procédures de gestion manuel des clés en texte clair spécifient les processus d'utilisation de ce qui suit :<br>• Fractionnement des connaissances de clés, de sorte que les composants de clé sont sous le contrôle d'au moins deux personnes qui ne connaissent que leur propre composant de clé ET<br>• Le double contrôle des clés, de sorte qu'au moins deux personnes doivent effectuer toutes les opérations de gestion de clé et qu'une seule personne ait accès au matériel d'authentification (par exemple les mots de passe ou les clés) d'une autre. | Le fractionnement des connaissances et le double contrôle des clés sont utilisés pour éliminer la possibilité qu'une seule personne puisse accéder à l'intégralité d'une clé. Ce contrôle s'applique aux opérations manuelles de cryptage des clés ou si la gestion des clés n'est pas prise en charge par la solution de cryptage.<br><br>Le fractionnement des connaissances est une méthode par laquelle deux personnes ou plus détiennent séparément des composants clés ; chaque personne connaît uniquement son propre composant de clé et les composants de clé individuels ne contiennent aucune connaissance de la clé cryptographique d'origine.<br><br>Le double contrôle demande que deux personnes ou plus effectuent une fonction et qu'une seule personne ne puisse pas accéder ou utiliser le matériel d'authentification d'une autre. |
| | **3.6.6.b** Interroger le personnel et/ou observer les processus pour vérifier que les clés manuelles en texte clair sont gérées avec :<br>• Le fractionnement des connaissances ET<br>• Le double contrôle | |
| **3.6.7** Prévention de la substitution non autorisée des clés cryptographiques. | **3.6.7.a** Vérifier que les procédures de gestion des clés spécifient les processus empêchant la substitution non autorisée des clés. | La solution de cryptage ne doit pas autoriser ni accepter la substitution de clés de la part de sources non autorisées ou de processus inattendus. |
| | **3.6.7.b** Interroger le personnel et/ou observer les processus pour vérifier que la substitution non autorisée des clés est empêchée. | |
| **3.6.8** Condition selon laquelle les opérateurs chargés de la gestion de clés cryptographiques reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités en tant | **3.6.8.a** Vérifier que les procédures de gestion des clés spécifient les processus selon lesquels les opérateurs chargés de la gestion de clés cryptographiques reconnaissent (par écrit ou électroniquement) qu'ils comprennent et acceptent leurs responsabilités en tant que telles. | Ce processus aidera à garantir que les individus chargés de la gestion des clés s'engagent vis-à-vis de leur rôle de détenteur de clé et qu'ils comprennent et acceptent leurs responsabilités. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| que telles. | **3.6.8.b** Observer la documentation et les autres preuves montrant que les opérateurs chargés de la gestion de clés cryptographiques reconnaissent (par écrit ou électroniquement) qu'ils comprennent et acceptent leurs responsabilités en tant que telles. | |
| **3.7** Assurer que les politiques de sécurité et les procédures opérationnelles pour la protection des données du titulaire sont documentées, utilisées et connues de toutes les parties concernées. | **3.7** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection des données du titulaire stockées sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles documentées pour la gestion du stockage sécurisé des données du titulaire sur une base continuelle. |

## *Condition 4 : Crypter la transmission des données du titulaire 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 du titulaire.

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **4.1** Utiliser des protocoles de sécurité et de cryptographie robustes (par exemple, SSL/TLS, IPSEC, SSH, etc.) afin de protéger les données sensibles du titulaire durant la transmission sur des réseaux publics ouverts, y compris :<br>• Seuls des clés et certificats approuvés sont acceptés.<br>• Le protocole utilisé prend uniquement en charge les versions ou configurations sécurisées.<br>• La force du cryptage est appropriée pour la méthodologie de cryptage employée.<br>*Voici quelques exemples, parmi d'autres, de réseaux publics ouverts :*<br>• *Internet,* | **4.1.a** Identifier tous les emplacements où les données du titulaire sont transmises ou reçues sur des réseaux publics ouverts. Examiner les normes documentées et comparer aux configurations de système pour vérifier l'utilisation de protocoles de sécurité et l'utilisation d'une cryptographie robuste pour tous les emplacements.<br>**4.1.b** Examiner les politiques et procédures documentées pour vérifier que des processus sont documentés pour les points suivants :<br>• Pour l'acceptation exclusive des clés/certificats approuvés<br>• Pour que le protocole utilisé prenne uniquement en charge les versions ou configurations sécurisées (pour que les versions ou configurations non sécurisées ne soient pas prises en charge)<br>• Pour l'implémentation d'un niveau de cryptage approprié pour la méthodologie de cryptage employée | Les informations sensibles doivent être cryptées durant leur transmission sur des réseaux publics, car il est facile et courant qu'un individu malveillant les intercepte et/ou les détourne pendant cette opération.<br>La transmission sécurisée des données du titulaire nécessite des clés/certificats fiables, un protocole sécurisé pour le transport et un cryptage d'une force suffisante pour le codage des données du titulaire. Les demandes de connexion de systèmes qui ne prennent pas en charge le cryptage de la robustesse requise, et qui provoquerait une connexion non sécurisée, ne doit pas être accepté.<br>Noter que l'implémentation de certains protocoles (tels que SSL version 2.0, SSH version 1.0 et TLS 1.0) a des vulnérabilités connues qu'un pirate |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| • *Technologies sans fil, y compris 802.11 et Bluetooth*<br>• *Les technologies cellulaires, par exemple, Système global pour les communications mobiles (GSM), Accès multiple de division de code (CDMA)*<br>• *GPRS (General Packet Radio Service).*<br>• *Communications par satellite.* | **4.1.c** Sélectionner et examiner un échantillon de transmissions entrantes et sortantes pendant qu'elles s'exécutent afin de vérifier que les données du titulaire sont cryptées à l'aide d'une cryptographie robuste pendant le transfert. | peut utiliser pour obtenir le contrôle du système affecté. Quel que soit le protocole de sécurité utilisé, s'assurer qu'il est configuré de manière à n'utiliser que des configurations et versions sécurisées pour empêcher l'utilisation d'une connexion non sécurisée. Par exemple, les certificats TLS v1.1 ou ultérieurs, obtenus auprès d'une autorité de certification publique reconnue et qui prennent uniquement en charge un cryptage robuste, peuvent être considérés.<br>Vérifier que les certificats sont des certificats de confiance (par exemple, qu'ils ne sont pas arrivés à expiration et qu'ils proviennent d'une source autorisée) aide à assurer l'intégrité de la connexion sécurisée. |
| | **4.1.d** Examiner les clés et les certificats pour vérifier que seuls des clés/certificats approuvés sont acceptés. | |
| | **4.1.e** Examiner les configurations de système pour vérifier que le protocole est déployé de manière à n'utiliser que des configurations sécurisées et qu'il ne prend en charge aucune version ou configuration non sécurisée. | |
| | **4.1.f** Examiner les configurations du système pour 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.g** Pour les implémentations SSL/TLS, examiner les configurations de système pour vérifier que SSL/TLS est activé lorsque les données du titulaire sont transmises ou reçues.<br>Par exemple, pour les implémentations basées sur le navigateur :<br>• La mention « HTTPS » apparaît comme protocole de l'adresse URL (Universal Record Locator, localisateur uniforme de ressource) du navigateur et<br>• Les données du titulaire sont uniquement requises lorsque la mention « HTTPS » apparaît dans l'adresse URL. | Généralement, l'URL de la page Web doit commencer par « HTTPS » et/ou une icône de cadenas apparaît dans la fenêtre du navigateur. De nombreux fournisseurs de certificats SSL apportent également un sceau de vérification haute visibilité, parfois dénommé « sceau de sécurité », « sceau de site sécurisé », ou « sceau de sécurisation de confiance », qui est susceptible de donner la possibilité de cliquer sur le sceau pour afficher des informations concernant le site Web. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVE |
|---|---|---|
| **4.1.1** S'assurer que les réseaux sans-fil sur lesquels sont transmises les données du titulaire ou qui sont connectés à l'environnement des données du titulaire mettent en œuvre les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste pour l'authentification et la transmission.<br><br>***Remarque :*** *L'utilisation du protocole WEP comme contrôle de sécurité est interdite.* | **4.1.1** Identifier tous les réseaux sans fil qui transmettent des données du titulaire ou qui sont connectés à l'environnement de données du titulaire. Examiner les normes documentées et comparer aux réglages de configurations de système pour vérifier les points suivants pour tous les réseaux sans fil identifiés :<br>• Les meilleures pratiques du secteur (par exemple, IEEE 802.11i) sont utilisées pour l'implémentation d'un cryptage robuste à l'authentification et la transmission.<br>• Aucun cryptage faible (par exemple WEP, SSL version 2.0 ou antérieure) n'est utilisé comme contrôle de sécurité pour l'authentification ou la transmission. | Les utilisateurs malveillants emploient des outils gratuits et largement répandus pour écouter les communications sans fil. L'utilisation d'une cryptographie robuste peut aider à limiter la divulgation d'informations sensibles sur les réseaux sans fil.<br><br>Une cryptographie robuste pour l'authentification et la transmission des données du titulaire est obligatoire pour empêcher les utilisateurs malveillants d'accéder au réseau sans fil ou d'utiliser les réseaux sans fil pour accéder à d'autres données ou réseaux internes. |
| **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, etc.). | **4.2.a** Si des technologies de messagerie d'un utilisateur final sont utilisées, observer les processus d'envoi de PAN et examiner un échantillon de transmissions sortantes lorsqu'elles ont lieu pour vérifier que le PAN est rendu illisible ou sécurisé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie d'utilisateurs finaux.<br><br>**4.2.b** Examiner les politiques écrites pour vérifier l'existence d'une politique interdisant la transmission de PAN non protégé à l'aide de technologies de messagerie d'utilisateurs finaux. | La messagerie électronique, la messagerie instantanée et le chat peuvent être facilement interceptés par reniflage de paquets durant le l'envoi aux réseaux internes et publics. N'utiliser ces outils de messagerie pour envoyer de PAN à moins qu'ils ne soient configurés pour intégrer des fonctions de cryptage robustes. |
| **4.3** Assurer que les politiques de sécurité et les procédures opérationnelles pour le cryptage des données du titulaire sont documentées, utilisées et connues de toutes les parties concernées. | **4.3** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection des données du titulaire stockées sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la gestion de la transmission sécurisée des données du titulaire sur une base continuelle. |

# Gestion d'un programme de gestion des vulnérabilités

### *Condition 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes*

Des logiciels malicieux, généralement appelés « logiciels 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 logiciels malveillants afin de les protéger contre les menaces logicielles actuelles et futures. Des solutions contre les logiciels malveillants supplémentaires peuvent être envisagées en complément du logiciel anti-virus ; toutefois, ces solutions supplémentaires ne supplantent pas le besoin de mise en place d'un logiciel anti-virus.

| Conditions PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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. | Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). En l'absence de solution antivirus régulièrement mise à jour, ces nouvelles formes de logiciel malveillant peuvent attaquer les systèmes et désactiver un réseau ou compromettre les données. |
| **5.1.1** S'assurer que tous les programmes anti-virus sont capables de détecter et d'éliminer tous les types de logiciel malveillant connus, et d'assurer une protection efficace. | **5.1.1** Examiner la documentation du fournisseur et examiner les configurations d'anti-virus pour vérifier que les programmes d'anti-virus :<br>• Détectent tous les types de logiciel malveillant connus,<br>• Éliminent tous les types de logiciel malveillant connus et<br>• Protègent contre tous les types de logiciel malveillant connus.<br>*Les exemples de types de logiciel malveillant connus comprennent les virus, les chevaux de Troie, les vers, les logiciels espions et publicitaires et les logiciels malveillants furtifs.* | Il est important de se protéger contre **TOUS** les types et formes de logiciel malveillant. |

| Conditions PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **5.1.2** Pour les systèmes considérés comme n'étant pas affectés par les logiciels malveillants, effectuer des évaluations régulières pour identifier et évaluer l'évolution de la menace posée par les logiciels malveillants afin de confirmer que ces systèmes continuent d'opérer sans logiciel anti-virus. | **5.1.2** Interroger le personnel pour vérifier que l'évolution de la menace posée par les logiciels malveillants est surveillée et évaluée pour les systèmes n'étant pas actuellement considérés comme n'étant pas communément affectés par les logiciels malveillants, afin de confirmer que ces systèmes continuent d'opérer sans logiciel anti-virus. | Habituellement, les systèmes d'unités centrales, les ordinateurs de moyenne gamme (tels que AS/400) et les systèmes similaires ne sont pas communément ciblés ou attaqués par les logiciels malveillants. Toutefois, les tendances du secteur en matière de logiciels malveillants peuvent changer rapidement, il est donc important que les organisations soient conscientes des nouveaux logiciels malveillants qui pourraient affecter leur système, par exemple en surveillant les avis de sécurité des fournisseurs et les groupes d'information consacrés aux anti-virus pour déterminer si leur système pourrait être menacé par de nouveaux logiciels malveillants.<br><br>Les tendances liées aux logiciels malveillants doivent être incluses dans l'identification des nouvelles vulnérabilités en matière de sécurité et les méthodes de résolution correspondantes doivent être intégrées aux normes de configuration et aux mécanismes de protection de l'entreprise, comme requis. |
| **5.2** Assurer que tous les mécanismes antivirus sont maintenus comme suit :<br>• Maintenus à jour<br>• Effectuent régulièrement des scans<br>• Génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS. | **5.2.a** Examiner les politiques et les procédures pour vérifier que les logiciels et les définitions d'anti-virus sont conservées à jour.<br><br>**5.2.b** Examiner les configurations anti-virus, y compris l'installation du logiciel maître, pour vérifier que les mécanismes anti-virus sont :<br>• Configurés pour effectuer automatiquement les mises à jour et<br>• Configurées pour effectuer régulièrement des scans<br><br>**5.2.c** Examiner un échantillon de composants du système, y compris tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, pour vérifier que :<br>• Le logiciel anti-virus et les définitions sont à jour.<br>• Des scans sont effectués régulièrement. | Même les meilleures solutions anti-virus sont limitées du point de vue de l'efficacité si elles ne sont pas maintenues et mises à jour avec les dernières mises à jour de sécurité, fichiers de signature ou protection contre les logiciels malveillants.<br><br>Les journaux d'audit permettent de surveiller l'activité des virus et des logiciels malveillants, ainsi que les réactions contre les logiciels malveillants. Par conséquent, il est impératif que la solution antivirus soit configurée pour générer des journaux d'audit et de gérer ces derniers conformément à la condition 10. |

| Conditions PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | **5.2.b** Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que :<br>• La production de journaux de logiciel anti-virus est activée et<br>• Les journaux sont conservés conformément à la condition 10.7 de la norme PCI DSS. | |

| Conditions PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **5.3** Assurer que les mécanismes anti-virus fonctionnement de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.<br><br>***Remarque :*** *Les solutions anti-virus peuvent être désactivées temporairement uniquement s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la protection anti-virus doit être désactivée dans un but spécifique, cette désactivation doit donner lieu à une autorisation formelle. Des mesures de sécurité supplémentaires doivent également être mises en œuvre pour la période de temps pendant laquelle la protection anti-virus n'est pas active.* | **5.3.a** Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel anti-virus fonctionne activement.<br><br>**5.3.b** Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel anti-virus ne peut pas être désactivé ou altéré par les utilisateurs.<br><br>**5.3.c** Interroger le personnel responsable et observer les processus pour vérifier que les logiciels anti-virus ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps. | Un anti-virus qui fonctionne continuellement et qui ne peut pas être altéré offrira une sécurité persistante contre les logiciels malveillants.<br><br>L'utilisation de contrôles basés sur une politique sur tous les systèmes pour assurer que les protections contre les logiciels malveillants ne puissent pas être altérées ou désactivées aidera à empêcher que les faiblesses du système ne soient exploitées par les logiciels malveillants.<br><br>Des mesures de sécurité supplémentaires peuvent également être mises en œuvre pour la période pendant laquelle la protection anti-virus n'est pas active, par exemple déconnecter le système sans protection d'Internet lorsque la protection anti-virus est désactivée, et effectuer un scan complet une fois qu'elle est réactivée. |
| **5.4** Assurer que les politiques de sécurité et les procédures opérationnelles pour la protection contre les logiciels malveillants sont documentées, utilisées et connues de toutes les parties concernées. | **5.4** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection contre les logiciels malveillants sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que les systèmes sont protégés contre les logiciels malveillants sur une base continuelle. |

## *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 doivent être dotés des correctifs logiciels appropriés afin d'empêcher l'exploitation et l'altération des données du titulaire 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 | DIRECTIVES |
|---|---|---|
| **6.1** Établir un processus pour identifier les vulnérabilités de la sécurité, en utilisant des sources externes de bonne réputation pour la sécurité des informations concernant la vulnérabilité et affecter un classement du risque (par exemple « élevé », « moyen » ou « faible ») aux vulnérabilités de sécurité nouvellement découvertes.<br><br>***Remarque :*** *Le classement des risques doit se baser sur les meilleures pratiques du secteur, ainsi que sur la prise en compte de l'impact potentiel. Par exemple, les critères de classement des vulnérabilités peuvent inclure la prise en compte du score de base CVSS et/ou la classification par le fournisseur et/ou le type de système affecté.*<br><br>*Les méthodes d'évaluation de vulnérabilité et d'affectation des classements de risque varieront selon l'environnement de l'organisation et la stratégie d'évaluation des risques. Le classement de risque doit, au minimum, identifier toutes les vulnérabilités considérées comme posant un « risque élevé » pour l'environnement. En plus du classement de risque, les vulnérabilités peuvent être considérées comme « critiques » si elles constituent une menace imminente pour l'environnement, ont un impact critique sur les systèmes et/ou si elles* | **6.1.a** Examiner les politiques et procédures pour vérifier que les processus sont définis pour les points suivants :<br>• Pour identifier les nouvelles vulnérabilités de la sécurité<br>• Pour assigner un classement du risque des vulnérabilités qui comprend une identification des vulnérabilités à « haut risque » et des vulnérabilités « critiques ».<br>• Pour utiliser des sources externes fiables pour les informations sur les vulnérabilités en matière de sécurité<br><br>**6.1.b** Interroger le personnel responsable et examiner le processus pour vérifier que :<br>• Les nouvelles vulnérabilités de la sécurité sont identifiées.<br>• Un classement du risque des vulnérabilités est établi qui comprend une identification des vulnérabilités à « haut risque » et des vulnérabilités « critiques »<br>• Des processus pour identifier les nouvelles vulnérabilités de sécurité comprennent l'utilisation des sources externes d'information sur la vulnérabilité de sécurité. | L'objectif de cette condition est de faire en sorte que les organisations restent à jour et informées des nouvelles vulnérabilités pouvant affecter leur environnement.<br><br>Les sources d'informations concernant la vulnérabilité doivent être fiables et elles comprennent souvent les sites Web des fournisseurs, les groupes d'information du secteur, les listes de diffusion ou flux RSS.<br><br>Une fois qu'une organisation identifie une vulnérabilité qui pourrait affecter son environnement, le risque posé par cette vulnérabilité doit être évalué et classé. L'organisation doit donc avoir mis en place une méthode pour évaluer les vulnérabilités sur une base continuelle et affecter un classement du risque posé par ces vulnérabilités. Cet objectif n'est pas atteint avec un scan ASV ou un scan de vulnérabilité interne, un processus est nécessaire pour surveiller de manière active les sources de l'industrie pour connaître les informations portant sur les vulnérabilités.<br><br>Établir un classement des risques (par exemple, « élevé », « moyen » et « faible ») permet aux organisations d'identifier et de répondre plus rapidement aux éléments de risque de priorité élevée, et de réduire la probabilité que les vulnérabilités impliquant les risques les plus élevés soient exploitées. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| *sont susceptibles de compromettre l'application si elles ne sont pas résolues. Les exemples de systèmes critiques peuvent inclure les systèmes de sécurité, les dispositifs et systèmes ouverts au public, les bases de données et autres systèmes qui stockent, traitent ou transmettent des données du titulaire.* | | |
| **6.2** S'assurer que tous les logiciels et les composants du système sont protégés de vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.<br><br>***Remarque :*** *Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.* | **6.2.a** Examiner les politiques et procédures les politiques relatives à l'installation des correctifs de sécurité pour vérifier que les processus sont définis pour :<br>• Installer les correctifs de sécurité critiques pertinents fournis par le fournisseur dans le mois qui suit leur commercialisation.<br>• Installer tous les correctifs de sécurité critiques pertinents fournis par le fournisseur dans un délai acceptable (par exemple, dans les trois mois).<br><br>**6.2.b** Pour 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, pour vérifier les points suivants :<br>• Les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans le mois qui suit leur commercialisation.<br>• Tous les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans un délai acceptable (par exemple, dans les trois mois). | Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). Si les correctifs les plus récents ne sont pas mis en œuvre dès que possible sur les systèmes critiques, un individu malveillant pourrait exploiter cette faiblesse pour attaquer ou désactiver un système ou pour accéder à des données sensibles.<br><br>Établir une priorité des correctifs pour l'infrastructure critique garantit que les systèmes et les dispositifs de haute priorité sont protégés des vulnérabilités aussi tôt que possible après la commercialisation d'un correctif. Envisager donner la priorité à l'installation de correctif, de sorte que les correctifs de sécurité pour les systèmes critiques ou à risque soient installés dans les 30 jours et les correctifs de sécurité moins critique dans les 2-3 mois.<br><br>Cette condition s'applique à tous les correctifs applicables pour tous les logiciels installés. |
| **6.3** Développer des applications logicielles internes et externes (y compris l'accès administratif aux applications par le Web) conformément aux points suivants :<br>• Conformément à la norme PCI DSS (par exemple, authentification et connexion | **6.3.a** Examiner les processus écrits de développement de logiciel pour vérifier qu'ils se basent sur les normes du secteur et/ou les meilleures pratiques.<br><br>**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. | Faute d'intégrer la sécurité aux phases de définition des conditions, de conception, d'analyse et de test du développement d'un logiciel, des vulnérabilités de sécurité peuvent être introduites, accidentellement ou par malveillance, dans l'environnement de production. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| sécurisées)<br>• Basés sur les normes/meilleures pratiques du secteur.<br>• Incorporer la sécurité des informations de sécurité au cours du cycle de vie de la conception d'un logiciel.<br>***Note** : ce point s'applique à tous les logiciels développés à l'interne, ainsi qu'aux logiciels sur mesure ou personnalisés qui sont développés par un tiers.* | **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.<br><br>**6.3.d** Interroger les développeurs de logiciel pour vérifier que les processus écrits de développement de logiciel sont mis en œuvre. | Comprendre comment les données sensibles sont traitées par l'application, y compris lorsqu'elles sont stockées, transmises et lorsqu'elles sont en mémoire peut aider à identifier l'emplacement où les données ont besoin d'être protégées. |
| **6.3.1** Supprimer les comptes de développement, de test et/ou les comptes d'application personnalisés, les ID d'utilisateur et des mots de passe avant l'activation des applications ou leur mise à la disposition des clients. | **6.3.1** Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour vérifier que les comptes de pré-production et/ou les comptes d'application personnalisée, les ID d'utilisateur et/ou les mots de passe sont éliminés avant qu'une application entre en production ou sont mise à disposition des clients. | Les comptes d'application personnalisés et/ou de test, les ID utilisateur et les mots de passe doivent être supprimés du code de production avant l'activation de l'application ou sa mise à la disposition des clients puisque ces éléments peuvent révéler des informations sur le fonctionnement de l'application. Grâce à la possession de ces informations, il est plus facile de compromettre l'application et les données du titulaire associées. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.3.2** Examiner le code d'application personnalisé avant la mise en production ou la mise à la disposition des clients afin d'identifier toute vulnérabilité de codage éventuelle (à l'aide de processus manuels ou automatiques) pour inclure au moins les points suivants :<br>• Les modifications de code sont examinées par des individus autres que l'auteur initial du code et par des individus compétents en la matière de techniques d'analyse de code et de pratiques de codage sécurisées.<br>• Les examens de code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé<br>• Les corrections appropriées sont implémentées avant la publication.<br>• Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement.<br>*(suite à la page suivante)* | **6.3.2.a** Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour tous les changements d'applications personnalisées doivent être analysés (à l'aide de processus manuels ou automatiques) comme suit :<br>• 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.<br>• 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).<br>• Les corrections appropriées sont implémentées avant la publication.<br>• Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. | Les vulnérabilités de sécurité du code personnalisé sont généralement exploitées par les individus malveillants pour accéder à un réseau et compromettre les données du titulaire.<br>Une personne compétente et expérimentée en matière de techniques d'analyse de code doit prendre part au processus d'analyse. Les analyses de code doivent être effectuées par une personne autre que le développeur du code, afin que le contrôle puisse être indépendant et objectif. Des outils ou processus automatiques peuvent également être utilisés alternativement aux analyses manuelles, mais soyez conscient du fait qu'il pourrait être difficile ou même impossible pour un outil automatique d'identifier certains problèmes de codage.<br>La correction des erreurs de codage avant que le code ne soit déployé dans un environnement de production ou mis à la disposition des clients empêche que le code n'expose l'environnement aux exploitations indésirables. Un code défaillant est bien plus difficile et cher à résoudre après qu'il ait été déployé ou lancé dans l'environnement de production.<br>Inclure un examen formel et une signature des responsables avant le lancement aide à garantir que ce code est approuvé et a été développé selon les politiques et procédures. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| ***Remarque :*** *Cette condition s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de conception du système.*<br>*Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers. Les applications Web disponibles au public font également l'objet de contrôles supplémentaires afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par la condition 6.6 de la norme PCI DSS.* | **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.a 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 les points suivants : | **6.4** Examiner les politiques et procédures pour vérifier que les points suivants sont définis :<br>• Les environnements de test/développement sont distincts de l'environnement de production et il existe un contrôle d'accès pour garantir la séparation.<br>• Il existe une séparation des tâches entre le personnel affecté aux environnements de développement/test et le personnel affecté à l'environnement de production.<br>• Les données de production (PAN actifs) ne sont pas utilisées à fins de test ou de développement.<br>• Les comptes et les données de test sont supprimés avant que le système de production ne devienne actif.<br>• Les changements de procédure de contrôle relatifs à la mise en œuvre de correctifs de sécurité et aux modifications de logiciel sont documentés. | Sans un contrôle correctement documenté et implémenté des modifications, les fonctions de sécurité peuvent être accidentellement ou délibérément omises ou rendues inopérantes, des irrégularités de traitement peuvent se produire ou un code malveillant peut être introduit. |
| **6.4.1** Séparer les environnements de test/développement des environnements de production et appliquer la séparation à l'aide de contrôles d'accès | **6.4.1.a** Examiner la documentation de réseau et les configurations de dispositif de réseau pour vérifier que les environnements de test/développement sont distincts de l'environnement de production.<br>**6.4.1.b** Examiner les réglages de contrôle d'accès pour vérifier que les contrôles d'accès sont en place pour appliquer la séparation entre les environnements de test/développement et l'environnement de production. | En raison de leur évolution constante, les environnements de développement et de test tendent à être moins sécurisés que les environnements de production. Sans une séparation appropriée des environnements, l'environnement de production et les données du titulaire pourraient être compromis en raison de configurations de sécurité moins strictes et de possibles vulnérabilités dans un environnement de test ou de développement. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.4.2** Séparation des obligations entre les environnements de développement/test et de production. | **6.4.2** Examiner les processus et interroger le personnel affecté aux environnements de développement/test et le personnel affecté aux environnements de production pour vérifier que la séparation des tâches est en place entre les environnements de test/développement et l'environnement de production. | Réduire le nombre de personnes ayant accès à l'environnement de production et aux données du titulaire minimise le risque et permet de garantir que l'accès est limité aux seuls individus ayant un besoin professionnel d'en connaître.<br><br>Cette condition est destinée à garantir la séparation entre les fonctions de test et de développement et les fonctions de production. Par exemple, un développeur peut utiliser un compte de niveau administrateur avec des privilèges de haut rang dans l'environnement de développement et posséder un compte distinct avec un accès de niveau utilisateur à l'environnement de production. |
| **6.4.3** Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement. | **6.4.3.a** Examiner les processus de test et interroger le personnel pour vérifier que des procédures sont en place pour garantir que les données de production (PAN actifs) ne sont plus utilisées pour le test ou le développement. | Les contrôles de sécurité ne sont généralement pas aussi stricts dans les environnements de test ou de développement. L'utilisation des données de production donne aux individus malveillants la possibilité d'y accéder (données du titulaire) sans y être autorisés. |
| | **6.4.3.b** Examiner un échantillon de données de test pour vérifier que les données de production (PAN actifs) ne sont pas utilisées à fin 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.a** Examiner les processus de test et interroger le personnel pour vérifier que les données et les comptes de test sont éliminés avant qu'un système de production ne devienne actif. | Les comptes et les données de test doivent être supprimés du code de production avant l'activation de l'application, puisque ces éléments peuvent divulguer des informations sur le fonctionnement de l'application ou du système. Avec ces informations, il est plus facile de compromettre le système et les données du titulaire associées. |
| | **6.4.4.b** Examiner un échantillon des données et de comptes des systèmes de production récemment installés ou mis à jour pour vérifier que les données et les comptes de test sont éliminés avant que le système de devienne actif. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.4.5** Les changements des procédures de contrôle pour l'implémentation des correctifs de sécurité et de modifications de logiciel doivent inclure les points suivants : | **6.4.5.a** Examiner les changements documentés de procédures de contrôle relatifs à la mise en œuvre de correctifs de sécurité et aux modifications de logiciel et vérifier que les procédures sont définies pour :<br>• Documentation de l'impact<br>• Approbation de changement documentée par les parties autorisées<br>• Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système.<br>• Procédures de suppression | En cas de gestion inadéquate, l'impact des mises à jour du logiciel et des correctifs de sécurité ne sera pas pleinement effectif et risquerait d'avoir des conséquences non intentionnelles. |
| | **6.4.5.b** Pour un échantillon de composants du système, interroger le personnel responsable pour déterminer les correctifs de sécurité/changements récents. Retracer ces changements sur la documentation de contrôle des changements associés. 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. | L'impact de la modification doit être documenté de sorte que toutes les parties concernées soient en mesure de planifier en conséquence pour tout changement du traitement. |
| **6.4.5.2** Documentation du changement approuvée par les parties autorisées. | **6.4.5.2** Vérifier qu'une approbation documentée par les responsables existe pour chaque modification échantillonnée. | L'approbation par les responsables autorisés indique que la modification est légitime et que son approbation est ratifiée par l'organisation. |
| **6.4.5.3** 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. | Un test approfondi doit être effectué afin de vérifier que la sécurité de l'environnement n'est pas diminuée par la mise en œuvre d'une modification. Le test doit valider que tous les contrôles de sécurité existants restent en place, soient remplacés par des contrôles de force équivalente, ou soient renforcés après toute modification de l'environnement. |
| | **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. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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. | Pour chaque modification, il doit exister des procédures de retrait documentées au cas où la modification échouerait ou aurait des effets néfastes sur la sécurité de l'application ou du système, afin de pouvoir restaurer le système à son état antérieur. |
| **6.5** Adresser les vulnérabilités de code les plus fréquentes dans les processus de développement de logiciel, afin d'inclure les éléments suivants :<br>• Former les développeurs aux techniques de codage sécurisées, y compris comment éviter les vulnérabilités de codage usuelles et comprendre comment les données sensibles sont traitées dans la mémoire.<br>• Développer des applications basées sur les directives de codage sécurisé.<br>***Remarque :*** *les vulnérabilités décrites aux points 6.5.1 à 6.5.10 faisaient partie des meilleures pratiques du secteur au moment de la publication de cette version de la norme PCI DSS. Cependant, comme les meilleures pratiques de gestion de la vulnérabilité du secteur sont actualisées (par exemple, le guide OWASP, le Top 25 SANS CWE, le codage sécurisé CERT, etc.), se reporter aux meilleures pratiques actuelles pour ces conditions.* | **6.5.a** Examiner les politiques et les procédures de développement de logiciel pour vérifier que la formation aux techniques de codage sécurisées est requise pour les développeurs, basée sur les meilleures pratiques et les directives de l'industrie.<br>**6.5.b** Interroger un panel de développeurs pour vérifier qu'ils disposent des connaissances nécessaires en techniques de codage sécurisé.<br>**6.5.c** Examiner les archives concernant la formation pour vérifier que les développeurs ont été formés aux techniques de codage sécurisées, y compris comment éviter les vulnérabilités de codage usuelles et comprendre comment les données sensibles sont traitées dans la mémoire.<br>**6.5.d.** Vérifier la mise en place de processus pour protéger les applications, au minimum, des vulnérabilités suivantes : | La couche application comporte un risque élevé et peut être la cible de menaces internes et externes.<br>Les conditions 6.5.1 à 6.5.10 représentent les contrôles minimums qui doivent être en place et les organisations doivent incorporer les pratiques de codage sécurisées pertinentes qui sont applicables à la technologie spécifique de leur environnement.<br>Les développeurs d'application doivent être correctement formés pour identifier et résoudre les problèmes liés à ces vulnérabilités de codage courantes (et aux autres). Assurer que le personnel est compétent en matière de pratiques de codage sécurisées aidera à minimiser le nombre de vulnérabilités de la sécurité introduites par de mauvaises pratiques de codage. La formation des développeurs peut être effectuée à l'interne ou par des tiers et elle doit s'appliquer à la technologie utilisée.<br>Lorsque les pratiques de codage sécurisé, acceptées par le secteur, changent, les pratiques de codage de l'organisation doivent elles aussi être mises à jour, de même que la formation des développeurs afin de répondre aux nouvelles menaces, par exemple les attaques de déchirement de mémoire.<br>Les vulnérabilités identifiées de 6.5.1 à 6.5.10 représentent la ligne de base minimale. C'est à l'organisation de demeurer à jour vis-à-vis des tendances en matière de vulnérabilité et d'incorporer des mesures appropriées dans leurs pratiques de codage sécurisées. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| ***Remarque :*** *Les conditions 6.5.1 à 6.5.6, ci-dessous, s'appliquent à toutes les applications (internes ou externes).* | | |
| **6.5.1** Attaques par injection, notamment les injections de commandes SQL Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection. | **6.5.1** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les attaques par injection sont adressées par des techniques de codage qui comprennent :<br>• La validation d'entrée pour vérifier que les données utilisateurs ne peuvent pas modifier le sens des commandes et des requêtes.<br>• Utiliser des requêtes paramétrées. | Les attaques par injection, en particulier injection de commandes SQL, sont une méthode couramment utilisée pour compromettre des applications. Une attaque par injection se produit lorsque les données saisies par un utilisateur sont transmises à un programme d'interprétation dans le cadre d'une commande ou d'une requête. Les données hostiles du pirate trompent le programme d'interprétation pour lui faire exécuter des commandes non prévues ou modifier les données, permettant au pirate d'attaquer les composants du réseau par le biais de l'application, de lancer des attaques comme la saturation de la mémoire tampon, ou de révéler des informations confidentielles ainsi que la fonctionnalité de l'application serveur.<br>Les informations doivent être validées avant d'être transmises à l'application, par exemple en vérifiant tous les caractères alphabétiques, le mélange de caractères alphanumériques, etc. |
| **6.5.2** Saturation de la mémoire tampon | **6.5.2** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les saturations de la mémoire tampon sont adressées par des techniques de codage qui comprennent :<br>• Validation de limites de la mémoire tampon ;<br>• Troncage des chaînes d'entrées. | La saturation de la mémoire tampon se produit lorsqu'une application ne dispose pas de contrôles de limites sur l'espace de sa mémoire tampon. Ceci a pour résultat de pousser les informations de la mémoire tampon en dehors de son espace et dans l'espace exécutable de la mémoire. Lorsque cela se produit, le pirate a la possibilité d'insérer un code malveillant à une extrémité de la mémoire puis de le pousser dans l'espace exécutable de la mémoire en saturant la mémoire tampon. Le code malveillant est ensuite exécuté et permet souvent l'accès à distance du pirate, à l'application et/ou au système infecté. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.5.3** Stockage cryptographique non sécurisé | **6.5.3** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que le stockage cryptographique non sécurisé est adressé par des techniques de codage qui comprennent :<br>• Il faut prévenir les défauts cryptographiques.<br>• Utilisez des algorithmes et des clés cryptographiques robustes. | Les applications qui n'utilisent pas de robustes fonctions cryptographiques correctement pour stocker des données présentent un risque accru d'être compromises et d'exposer les justificatifs d'authentification et/ou les données du titulaire. Si un pirate est en mesure d'exploiter une faiblesse des processus cryptographiques, il peut accéder au texte clair des données cryptées. |
| **6.5.4** Communications non sécurisées | **6.5.4** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les communications non sécurisées sont adressées par des techniques de codage qui authentifient et cryptent correctement toutes les communications sensibles. | Les applications qui ne réussissent pas à correctement crypter le trafic réseau à l'aide d'une cryptographie robuste présentent un risque accru d'être compromises et d'exposer les données du titulaire. Si un pirate est en mesure d'exploiter une faiblesse des processus cryptographiques, il peut se retrouver en mesure de prendre le contrôle de l'application ou même d'accéder au texte clair des données cryptées. |
| **6.5.5** Traitement inapproprié des erreurs | **6.5.5** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que le traitement inapproprié des erreurs est résolu à l'aide de techniques de codage qui ne laissent fuir aucune information par le biais de messages d'erreur (par exemple, en retournant des détails d'erreur spécifiques plutôt que génériques). | Les applications peuvent laisser filtrer accidentellement des informations sur leur configuration ou mécanismes internes, ou exposer des informations privilégiées en raison de méthodes de traitement incorrectes. Les pirates peuvent utiliser cette faiblesse pour subtiliser des données sensibles ou pour compromettre le système dans sa globalité. Si un individu malveillant peut créer des erreurs que l'application ne gère pas correctement, il peut alors obtenir des informations système détaillées, créer des interruptions par déni de service, mettre la sécurité en échec ou entraîner une panne de serveur. Par exemple, le message selon lequel le « mot de passe saisi est incorrect » indique à un pirate que l'ID utilisateur fourni est correct et qu'il lui suffit de concentrer ses efforts sur le décryptage du mot de passe. Utiliser des messages d'erreur plus génériques, comme « Impossible de vérifier les données ». |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.5.6** Toutes les vulnérabilités à « haut risque », identifiées dans le processus d'identification de vulnérabilité (selon la condition 6.1 de la norme PCI DSS). | **6.5.6** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les techniques répondent aux vulnérabilités à « risque élevé» qui pourraient affecter l'application, telles qu'elles sont identifiées par la condition 6.1. de la norme PCI DSS. | Toutes les vulnérabilités déterminées par le processus de classement des risques de vulnérabilité d'une organisation (défini dans la condition 6.1) comme étant un « risque élevé » et qui pourrait affecter l'application doivent être identifiées et résolues pendant le développement de l'application. |
| ***Remarque :*** *Les conditions 6.5.7 à 6.5.10, ci-dessous, s'appliquent aux applications Web et aux interfaces d'application (internes ou externes) :* | | Les applications Web, internes et externes (publiques), comportent des risques de sécurité uniques dus à leur architecture, à leur manque de difficulté relatif et aux possibilités de les compromettre. |
| **6.5.7** Script inter-site (XSS) | **6.5.7** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que le script inter-site (XSS) est adressé par des techniques de codage qui comprennent :<br>• La validation de tous les paramètres avant l'inclusion<br>• L'utilisation d'un mécanisme d'échappement sensible au contexte. | Les attaques XSS se produisent chaque fois qu'une application extrait les données fournies par un utilisateur et les transmet à un navigateur Web sans d'abord les valider ou coder le contenu. Une attaque XSS permet aux pirates d'exécuter, dans le navigateur de la victime, un script qui peut détourner des sessions utilisateurs, rendre des sites Web illisibles, introduire éventuellement des vers, etc. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.5.8** Contrôle d'accès inapproprié (comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, le survol de répertoire et la non-restriction de l'accès utilisateur aux fonctions). | **6.5.8** Examiner les politiques et les procédures de développement de logiciel et interroger la personne responsable pour vérifier que le contrôle d'accès inapproprié, comme des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès URL et le survol de répertoire, est résolu à l'aide de techniques de codage qui comprennent :<br>• L'authentification correcte des utilisateurs<br>• L'assainissement des entrées<br>• Ne pas exposer les références d'objets internes aux utilisateurs<br>• Les interfaces utilisateurs qui ne permettent pas d'accéder aux fonctions non autorisées. | Une référence d'objet directe existe lorsqu'un développeur expose la référence à un objet d'implémentation interne, par exemple un fichier, un répertoire, un enregistrement de base de données ou une clé, comme une adresse URL ou un paramètre de formulaire. Les pirates peuvent manipuler ces références pour accéder à d'autres objets sans autorisation.<br>Appliquer uniformément le contrôle d'accès au niveau de la couche présentation et des modèles de traitement pour toutes les URL. Fréquemment, le seul moyen pour qu'une application protège la fonctionnalité sensible est d'empêcher l'affichage des liens ou des URL aux utilisateurs non autorisés. Les pirates peuvent exploiter cette faiblesse pour accéder à des opérations non autorisées et les exécuter en accédant directement à ces URL.<br>Un pirate peut être en mesure de détailler la structure du répertoire d'un site Web et de le parcourir (survol de répertoire), obtenant ainsi accès à des informations non autorisées ainsi que la compréhension du fonctionnement du site qu'il exploitera plus tard.<br>Si les interfaces utilisateurs donnent accès à des fonctions non autorisées, cet accès pourrait permettre à des individus non autorisés d'accéder à des justificatifs privilégiés ou à des données du titulaire. Seuls les utilisateurs autorisés doivent pouvoir accéder directement aux références d'objet de ressources sensibles. Limiter l'accès aux ressources de données aidera à empêcher que les données du titulaire ne soient présentées à des ressources non autorisées. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.5.9** Attaques CSRF (Cross-site request forgery) | **6.5.9** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les attaques de falsification de requête inter-site (CSRF) sont résolues en utilisant des techniques de codage qui assurent que les applications ne comptent pas sur des justificatifs d'autorisation et sur des jetons soumis automatiquement par les navigateurs. | Une attaque CSRF force le navigateur d'une victime connectée à envoyer une requête pré-authentifiée à une application Web vulnérable, qui permet ensuite au pirate d'effectuer les opérations de changement d'état que la victime est autorisée à effectuer (comme de mettre à jour les détails de compte, effectuer des achats ou même s'authentifier envers l'application). |
| **6.5.10** Rupture dans la gestion des authentifications et des sessions<br><br>***Remarque :*** *La condition 6.5.10 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.* | **6.5.10** Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que la rupture de la gestion des authentifications et des sessions est adressée par des techniques de codage qui comprennent :<br>• Étiqueter les jetons de session (par exemple les cookies) comme étant « sécurisés »<br>• Ne pas exposer les ID de session dans l'URL<br>• Incorporer des durées limites de session et des rotations d'ID de session avec une connexion réussie. | Sécuriser l'authentification et la gestion de session empêche les individus non autorisés de compromettre les justificatifs de compte légitimes, les clés ou les jetons de session qui, autrement, permettrait à l'intrus d'assurer l'identité d'un utilisateur autorisé. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.6** Pour les applications Web pour le public, traiter les nouvelles menaces et vulnérabilités de manière continue et veiller à ce que ces applications soient protégées contre les attaques connues à l'aide de l'une des méthodes suivantes :<br>• Examen des applications Web pour le 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.<br>***Remarque :*** *Cette évaluation est différente des scans de vulnérabilité effectuée pour la condition 11.2.*<br>• Installer une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) devant les applications web ouvertes au public pour vérifier continuellement tout le trafic. | **6.6** Pour des applications web *pour le public*, s'assurer que *l'une ou l'autre* des méthodes ci-dessous est en place comme suit :<br>• Examiner les processus documentés, interroger le personnel et examiner les archives des évaluations de sécurité de l'application pour vérifier que les applications Web pour le 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 :<br>- Au moins une fois par an<br>- Après toute modification ;<br>- Par une société spécialisée dans la sécurité des applications ;<br>- Que, au minimum, toutes les vulnérabilités de la condition 6.5 sont incluses dans l'évaluation<br>- Toutes les vulnérabilités sont corrigées ;<br>- Que l'application est réévaluée après les corrections.<br>• Examiner les réglages de configuration du système et interroger le personnel responsable pour vérifier qu'une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) est en place comme suit :<br>- Est située devant les applications Web pour le public pour détecter et empêcher les attaques basées sur le Web.<br>- Fonctionne activement et est mise à jour au besoin.<br>- Génère des journaux d'audit.<br>- Est configurée soit pour bloquer les attaques basées sur le Web ou pour générer une alerte. | Les applications Web pour le public sont les cibles principales des pirates et les applications Web à codage médiocre donnent un chemin d'accès facile pour les pirates qui cherchent à accéder aux données et aux systèmes sensibles. La condition de vérification des applications ou d'installation de pare-feu pour les applications Web est destinée à réduire le nombre d'attaques des applications Web pour le public causées par un codage médiocre ou par des pratiques de gestion d'application médiocres.<br>• Des outils ou des méthodes manuels ou automatiques d'évaluation de la sécurité et de la vulnérabilité, examinent et/ou testent les vulnérabilités de l'application<br>• Les pare-feu pour applications Web filtrent et bloquent le trafic non essentiel au niveau de la couche application. Utilisé conjointement à un pare-feu réseau, un pare-feu pour application Web correctement configuré empêche les attaques de la couche application si les applications sont mal codées ou mal configurées.<br>***Remarque :*** *« L'entreprise spécialisée dans la sécurité des applications » peut être une société tierce ou une entité interne, l'essentiel étant que le personnel chargé de réaliser la vérification soit spécialisé dans la sécurité des applications et puisse attester de sa totale indépendance vis-à-vis de l'équipe de développement.* |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **6.7** Assurer que les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de la sécurité des systèmes et des applications sont documentées, utilisées et connues de toutes les parties concernées. | **6.7** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de la sécurité des systèmes et des applications sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que les systèmes et les applications sont développés de manière sécurisée et protégées des vulnérabilités sur une base continuelle. |

# Mise en œuvre de mesures de contrôle d'accès strictes

### *Condition 7 : Restreindre l'accès aux données du titulaire 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 | DIRECTIVES |
|---|---|---|
| **7.1** Restreindre l'accès aux composants du système et aux données du titulaire aux seuls individus qui doivent y accéder pour mener à bien leur travail. | **7.1** Examiner la politique écrite de contrôle des accès et vérifier que la politique comprend les points 7.1.1 à 7.1.4 comme suit :<br>• Définir les besoins d'accès et les affectations de privilèges pour chaque rôle.<br>• La restriction d'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail<br>• L'affectation d'accès basée sur la classification et la fonction professionnelles de chaque employé<br>• L'approbation documentée (électroniquement ou par écrit) par les parties autorisées pour tous les accès, y compris la liste de tous les privilèges spécifiques approuvés. | Plus le nombre de personnes ayant accès aux données du titulaire est élevé, plus il y a de risques que le compte d'un utilisateur soit utilisé de manière frauduleuse. Restreindre l'accès aux seuls individus qui ont une raison professionnelle légitime aide l'entreprise à prévenir la manipulation des données du titulaire par des utilisateurs inexpérimentés ou malveillants. |
| **7.1.1** Définir les besoins d'accès pour chaque rôle, y compris :<br>• Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste<br>• Le niveau de privilège requis (par exemple utilisateur, administrateur, etc.) pour accéder aux ressources. | **7.1.1** Sélectionner un échantillon de rôles et vérifier que les besoins d'accès de chaque rôle sont définis et comprennent :<br>• Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste ;<br>• Identification des privilèges nécessaires pour chaque rôle à accomplir dans leur fonction professionnelle. | Afin de limiter l'accès aux données du titulaire aux seuls individus qui ont besoin de cet accès, il est tout d'abord nécessaire de définir les besoins d'accès de chaque rôle (par exemple administrateur de système, personnel du centre d'appel, agent de magasin), les systèmes/dispositifs/données auxquels chaque rôle a besoin d'accéder et le niveau de privilège nécessaire à chaque rôle pour effectuer efficacement les tâches assignées. Une fois que les rôles et les besoins d'accès correspondant ont été définis, l'accès peut être accordé aux individus en fonction. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **7.1.2** Restreindre l'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail | **7.1.2.a** Interroger le personnel responsable de l'affectation des accès pour vérifier que l'accès aux ID utilisateurs privilégiés est :<br>• Uniquement affecté aux rôles qui nécessitent spécifiquement ce type d'accès privilégié<br>• Restreints aux privilèges les plus faibles nécessaires pour la réalisation du travail | Lors de l'affectation d'ID privilégiée, il est important d'affecter uniquement les privilèges dont les individus ont besoin pour accomplir leur travail (le « moins de privilèges »). Par exemple, l'administrateur de base de données ou l'administrateur de sauvegarde ne doivent pas bénéficier des mêmes privilèges que l'administrateur du système global.<br>*(suite à la page suivante)* |
| | **7.1.2.b** Sélectionner un échantillon d'ID utilisateur avec accès privilégié et interroger le personnel de direction responsable pour vérifier que les privilèges assignés sont :<br>• Nécessaires pour les fonctions du travail de cette personne<br>• Restreints aux privilèges les plus faibles nécessaires pour la réalisation du travail | L'affectation du moins de privilèges possible aide à empêcher les utilisateurs qui ne connaissent pas suffisamment l'application de modifier sa configuration accidentellement ou de manière incorrecte, ou de modifier ses réglages de sécurité. Appliquer le moins de privilèges aide à minimiser la portée des dommages si une personne non autorisée obtient l'accès à un ID utilisateur. |
| **7.1.3** Affecter l'accès basé sur la classification et la fonction professionnelles de chaque employé | **7.1.3** Sélectionner un échantillon d'ID utilisateur et interroger le personnel de direction responsable pour vérifier que les privilèges assignés sont basés sur la classification et la fonction professionnelles de cette personne. | Une fois que les besoins sont définis pour les rôles d'utilisateur (selon la condition 7.1.1 de la norme PCI DSS), il est facile d'attribuer les droits d'accès individuels en fonction de la classification et de la fonction professionnelles en utilisant les rôles déjà créés. |
| **7.1.4** Demander l'approbation documentée des parties responsables spécifiant les privilèges requis. | **7.1.4** Sélectionner un échantillon d'ID utilisateur et comparer avec les approbations documentées pour vérifier que :<br>• L'approbation documentée existe pour les privilèges assignés ;<br>• L'approbation provenait des parties autorisées ;<br>• Que les privilèges spécifiques correspondent aux rôles affectés à l'individu. | Les approbations documentées (par exemple, par écrit ou électroniquement) assurent que ceux qui détiennent ces accès et ces privilèges sont connus et autorisés par la direction et que leur accès est nécessaire pour l'accomplissement de leur fonction professionnelle. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **7.2** Établir un système de contrôle d'accès pour les composants de systèmes qui limitent l'accès aux seuls utilisateurs qui doivent accéder aux données et qui est configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés.<br>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 : | Sans un mécanisme de restriction de l'accès en fonction du besoin d'en connaître d'un utilisateur, celui-ci peut, sans le savoir, se voir accorder l'accès aux données du titulaire. Un système de contrôle d'accès automatise le processus de restriction d'accès et l'affectation de privilèges. De plus, un réglage « tout refuser » par défaut assure que personne ne puisse obtenir l'accès à moins qu'une règle établie spécialement n'accorde cet accès.<br>***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.* |
| **7.2.1** 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 leurs fonctions 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 fonctions professionnelles. | |
| **7.2.3** Configuration par défaut du paramètre « Refuser tout ». | **7.2.3** Confirmer que les systèmes de contrôle d'accès intègrent un paramètre par défaut « Refuser tout ». | |
| **7.3** Assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données du titulaire sont documentées, utilisées et connues de toutes les parties concernées. | **7.3** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données du titulaire sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que l'accès est contrôlé et basé sur le besoin de savoir et le moins de privilèges sur une base continuelle. |

## *Condition 8 : Identifier et authentifier l'accès aux composants du système*

En affectant un identifiant (ID) unique à chaque personne ayant un accès, on s'assure que chaque individu sera personnellement responsable de ses actes. Lorsque cette responsabilité est en place, les actions prises sur des données et des systèmes stratégiques sont effectuées par, et peuvent être retracées, des utilisateurs et des processus connus et autorisés.

L'efficacité d'un mot de passe est fortement déterminée par la conception et l'implémentation du système d'authentification, particulièrement, la fréquence avec laquelle les tentatives de mot de passe peuvent être faites par un pirate et les méthodes de sécurité utilisées pour protéger les mots de passe au point d'entrée, pendant la transmission et le stockage.

***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. Ceux-ci comprennent les comptes utilisés par les fournisseurs et les autres tiers (par exemple, pour l'assistance ou l'entretien)*

*Cependant, les conditions 8.1.1, 8.2, 8.5, 8.2.3 à 8.2.5 et 8.1.6 à 8.1.8 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 | DIRECTIVES |
|---|---|---|
| **8.1** Définir et mettre en œuvre des politiques et des procédures pour assurer la gestion appropriée de l'identification des utilisateurs pour les utilisateurs non consommateurs et pour les administrateurs sur tous les composants de système comme suit : | **8.1.a** Examiner les procédures et confirmer qu'elles définissent les processus pour chacun des éléments ci-dessous de 8.1.1 à 8.1.8 | En s'assurant que chaque utilisateur est identifié de manière unique, au lieu d'utiliser un ID unique pour plusieurs employés, une entreprise peut gérer la responsabilité des actes de chaque individu et effectuer une vérification à rebours efficace par employé. Cela accélérera la résolution des problèmes et en limitera les conséquences en cas d'erreur ou d'intentions malveillantes. |
| | **8.1.b** Vérifier que les procédures sont mises en œuvre pour la gestion de l'identification des utilisateurs, en accomplissant ce qui suit : | |
| **8.1.1** Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants du système ou aux données du titulaire. | **8.1.1** Interroger le personnel administratif pour confirmer que tous les utilisateurs ont un ID unique pour accéder aux composants du système ou aux données de titulaires de carte. | |
| **8.1.2** Contrôler l'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiants. | **8.1.2** Pour un échantillon d'ID d'utilisateur privilégiés et d'ID d'utilisateur génériques, examiner les autorisations associées et observer les réglages de système pour vérifier que chaque ID utilisateur et chaque ID utilisateur privilégié a été mise en œuvre avec seulement les privilèges spécifiés sur l'approbation documentée. | Pour assurer que les comptes utilisateur ayant accès aux systèmes sont tous des utilisateurs valides et reconnus, des processus robustes doivent gérer tous les changements d'ID utilisateur et d'autres justificatifs d'authentification, y compris l'ajout de nouveaux justificatifs et la modification ou la suppression de justificatifs existants. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.1.3** Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société. | **8.1.3.a** Sélectionner un échantillon d'employés qui ont quitté la société au cours des six derniers mois, et passer en revue les listes d'accès pour examiner à la fois l'accès local et l'accès distant, afin de vérifier que leur ID ont été désactivées ou supprimées de la liste d'accès. | Si un employé a quitté la société et a toujours accès au réseau par son compte d'utilisateur, des accès inutiles ou malveillants aux données du titulaire pourraient se produire, soit par un ancien employé soit par un individu malveillant qui exploite le vieux compte inutilisé. Pour empêcher les accès non autorisés, les justificatifs d'utilisateur et les autres méthodes d'authentification doivent donc être révoqués rapidement (dès que possible) après le départ d'un employé. |
| | **8.1.3.b** Vérifier que toutes les méthodes d'authentification physiques, telles que les cartes électroniques, jetons, etc., ont été rendues ou désactivées. | |
| **8.1.4** Supprimer/désactiver les comptes d'utilisateur inactifs au moins tous les 90 jours. | **8.1.4** Observer les comptes utilisateur pour vérifier que les comptes inactifs depuis plus de 90 jours sont supprimés ou désactivés. | Les comptes qui ne sont pas utilisés régulièrement sont souvent les cibles d'attaques puisqu'il est moins probable que les modifications (telles que les changements de mot de passe) soient remarquées. Ainsi, ces comptes seront plus facilement exploités et utilisés pour accéder aux données du titulaire. |
| **8.1.5** Gérer les ID utilisés par les fournisseurs pour accéder, prendre en charge ou maintenir les composants de système par accès à distance comme suit :<br>• Activés uniquement pendant la période de temps nécessaire et désactivés lorsqu'ils ne sont pas utilisés.<br>• Surveillés lorsqu'ils sont utilisés. | **8.1.5.a** Interroger le personnel et observer les processus de gestion des comptes utilisés par les fournisseurs pour accéder, prendre en charge ou maintenir les composants de système pour vérifier que les comptes utilisés par les fournisseurs pour l'accès à distance sont :<br>• Désactivés lorsqu'ils ne sont pas utilisés<br>• Activés uniquement lorsqu'ils sont nécessaires pour le fournisseur et désactivés lorsqu'ils ne sont pas utilisés. | Autoriser les fournisseurs à accéder à un réseau 24h/24 et 7 jours sur 7 au cas où ils auraient besoin d'intervenir sur les systèmes, augmente les risques d'accès non autorisé, de la part d'un utilisateur, appartenant à l'environnement du fournisseur ou d'un individu malveillant, qui découvre et exploite ce point d'entrée toujours disponible sur le réseau. Permettre l'accès uniquement pour la période de temps nécessaire et le désactiver dès qu'il n'est plus nécessaire aide à empêcher les utilisations malveillantes de ces connexions.<br>La surveillance des accès de fournisseur donne l'assurance que les fournisseurs accèdent uniquement aux systèmes nécessaires, et uniquement pendant les périodes de temps approuvées. |
| | **8.1.5.b** Interroger le personnel et observer les processus pour vérifier que les comptes d'accès à distance du fournisseur sont surveillés pendant leur utilisation. | |
| **8.1.6** Limiter les tentatives d'accès répétées en verrouillant l'ID d'utilisateur après six tentatives au maximum. | **8.1.6.a** Pour un échantillon de composants du système, inspecter les réglages de configuration 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. | Sans des mécanismes de blocage de compte, un pirate peut en permanence tenter de deviner un mot de passe à l'aide d'outils manuels ou automatiques (par exemple, craquage de mots de passe), jusqu'à ce qu'il réussisse et l'utilise pour accéder au compte |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | **8.1.6.b** ***Procédures de test supplémentaires pour les prestataires de services*** **:** Examiner les processus internes et la documentation des clients/utilisateurs et observer les processus mis en œuvre pour vérifier que les comptes des utilisateurs non clients sont provisoirement verrouillés après six tentatives d'accès non valides au maximum. | d'un utilisateur. |
| **8.1.7** Régler la durée de verrouillage sur 30 minutes au minimum ou jusqu'à ce que l'administrateur active l'ID d'utilisateur. | **8.1.7** Pour un échantillon de composants du système, inspecter 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 compte. | Si un compte est bloqué parce que quelqu'un a essayé à plusieurs reprises d'en deviner le mot de passe, des contrôles retardant la réactivation de ce compte empêchent l'individu malveillant de poursuivre (il devra s'arrêter pendant au moins 30 minutes jusqu'à la réactivation du compte). De plus, si la réactivation doit être demandée, l'administrateur ou le bureau d'aide peuvent valider qu'il s'agisse bien du propriétaire du compte qui demande sa réactivation. |
| **8.1.8** Si une session reste inactive pendant plus de 15 minutes, demander à l'utilisateur de s'authentifier de nouveau pour réactiver le terminal ou la session. | **8.1.8** Pour un échantillon de composants du système, inspecter 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. | Lorsque les utilisateurs s'éloignent de leur ordinateur allumé ayant accès au réseau critique ou aux données du titulaire, cette machine peut être utilisée par d'autres en l'absence de l'utilisateur pour accéder sans autorisation à un compte et/ou l'utiliser à des fins frauduleuses.<br>La réauthentification peut être appliquée au niveau du système pour protéger toutes les sessions en cours sur cette machine, ou au niveau de l'application. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.2** En plus de l'affectation d'un ID unique, s'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants du système en employant au moins une des méthodes suivantes pour identifier tous les utilisateurs :<br>• Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ;<br>• Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ;<br>• Quelque chose que vous détenez, 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/phrase de passe) pour accéder à l'environnement des données du titulaire, procéder comme suit :<br>• Examiner la documentation qui décrit les méthodes d'authentification utilisées.<br>• 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. | Ces méthodes d'authentification, lorsqu'elles sont utilisées en plus des ID uniques, protègent les ID uniques des utilisateurs et évitent qu'ils ne soient compromis, puisque la personne qui en responsable de cette tentative doit connaître l'ID unique et le mot de passe (ou tout autre élément d'authentification utilisé). Remarquer qu'un certificat numérique est une option valable comme forme d'authentification du type « quelque chose de détenu », tant qu'il reste unique pour un utilisateur spécifique.<br>Dans la mesure où, l'une des premières mesures qu'un individu malveillant prendra pour compromettre un système étant d'exploiter la faiblesse ou l'absence de mots de passe, il est important de mettre en place des processus appropriés pour la gestion de l'authentification. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.2.1** Utiliser une cryptographie robuste, rendre tous les justificatifs d'authentification (tels que les mots/phrases de passe) illisibles pendant la transmission et le stockage sur tous les composants du système. | **8.2.1.a** Examiner la documentation du fournisseur et les réglages de configuration du système pour vérifier que les mots de passe sont protégés avec une cryptographie robuste pendant la transmission et le stockage. | De nombreux dispositifs et applications réseau transmettent des mots de passe non cryptés et lisibles sur le réseau et/ou stockent les mots de passe sans cryptage. Un individu malveillant peut facilement intercepter les mots de passe non cryptés durant leur transmission à l'aide d'un « renifleur », ou accéder directement aux mots de passe non cryptés, dans les fichiers où ils sont stockés et utiliser ces données pour accéder sans autorisation au réseau. |
| | **8.2.1.b** Pour un échantillon de composants du système, examiner les fichiers de mots de passe pour vérifier que les mots de passe sont illisibles pendant le stockage. | |
| | **8.2.1.c** Pour un échantillon de composants du système, examiner les transmissions de données pour vérifier que les mots de passe sont illisibles pendant la transmission. | |
| | **8.2.1.d** ***Procédures de test supplémentaires pour les prestataires de services*** **:** Observer les fichiers de mots de passe pour vérifier que les mots de passe des clients sont illisibles pendant le stockage. | |
| | **8.2.1.e** ***Procédures de test supplémentaires pour les prestataires de services :*** Observer les transmissions de données pour vérifier que les mots de passe des clients sont illisibles pendant la transmission. | |
| **8.2.2** Vérifier l'identité de l'utilisateur avant de modifier tout justificatif d'authentification, par exemple, lors des réinitialisations de mot de passe, la délivrance de nouveaux jetons ou la création de nouvelles clés. | **8.2.2** Examiner les procédures d'authentification pour modifier les justificatifs d'authentification et observer le personnel responsable de la sécurité pour vérifier que, si 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 avant la modification du justificatif d'authentification. | De nombreux individus malveillants utilisent « l'ingénierie sociale », par exemple en appelant un service d'assistance et en agissant comme un utilisateur légitime, afin d'obtenir un changement de mot de passe de sorte qu'ils puissent utiliser un ID utilisateur. Envisager l'utilisation d'une « question secrète » à laquelle seul le vrai utilisateur peut répondre, afin d'aider les administrateurs à identifier l'utilisateur avant de reconfigurer ou de modifier les justificatifs d'authentification. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.2.3** les mots/phrases de passe doivent respecter les critères suivants :<br>• Exiger une longueur minimale d'au moins sept caractères.<br>• Comporter à la fois des caractères numériques et des caractères alphabétiques.<br>Autrement, les mots/phrases de passe doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus. | **8.2.3.a** Pour un échantillon de composants du système, inspecter les paramètres de configuration du système pour vérifier que les paramètres de mot de passe utilisateur sont configurés de manière à exiger au moins la robustesse/complexité suivante :<br>• Exiger une longueur minimale d'au moins sept caractères.<br>• Comporter à la fois des caractères numériques et des caractères alphabétiques. | Des mots/phrases de passe robustes sont la première ligne de défense d'un réseau, puisque les individus malveillants rechercheront d'abord les comptes dont les mots de passe sont faibles ou inexistants. Si les mots de passe sont courts, faciles à deviner il est relativement facile pour un individu malveillant de découvrir ces comptes faibles et de compromettre un réseau sous couvert d'un ID utilisateur valide.<br>Cette condition spécifie que les mots/phrases de passe doivent être d'une longueur minimum de sept caractères et utiliser à la fois des caractères numériques et des caractères alphabétiques. Pour les cas où ce minimum ne peut pas être respecté en raison de limitations techniques, les entités peuvent utiliser une « force équivalente » pour évaluer leur alternative. NIST SP 800-63-1 définit « l'entropie » comme « une mesure de la difficulté de deviner ou de déterminer un mot de passe ou une clé ». Ce document et les autres documents qui traitent de « l'entropie de mot de passe » peuvent être consultés pour obtenir de plus amples informations sur la valeur d'entropie applicable et pour comprendre les variabilités de force de mot de passe équivalent pour les mots/phrases de passe de formats différents. |
| | **8.2.3.b** ***Procédures de test supplémentaires pour les prestataires de services*** **:** Examiner les processus internes et la documentation des clients/utilisateurs pour vérifier qu'il est demandé aux utilisateurs non clients de définir des mots de passe d'une robustesse/complexité respectant au moins les critères suivants :<br>• Exiger une longueur minimale d'au moins sept caractères.<br>• Comporter à la fois des caractères numériques et des caractères alphabétiques. | |
| **8.2.4** Modifier les mots/phrases de passe utilisateur au moins tous les 90 jours. | **8.2.4.a** Pour un échantillon de composants du système, inspecter les paramètres de configuration pour vérifier que les paramètres de mots de passe utilisateur sont configurés de manière à demander aux utilisateurs de modifier leur mot de passe au moins tous les 90 jours. | Les mots/phrases de passe qui sont valides pour longtemps sans être changés donnent aux individus malveillants plus de temps pour travailler à les découvrir. |
| | **8.2.4.b** ***Procédures de test supplémentaires pour les prestataires de services*** *: Examiner les processus* internes et la documentation de client/utilisateur pour vérifier que :<br>• Les mots de passe utilisateur non consommateur doivent changer régulièrement et<br>• Les utilisateurs non consommateur sont guidés quant au moment et aux circonstances dans lesquelles les mots de | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | passe doivent être changés. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.2.5** Interdire à un utilisateur de soumettre un nouveau mot/phrase de passe identique à l'un de quatre derniers mots de passe qu'il a utilisés. | **8.2.5.a** Pour un échantillon de composants du système, obtenir et inspecter les paramètres de configuration du système pour vérifier que les paramètres de mot de passe sont configurés pour exiger que les nouveaux mots de passe ne puissent pas être les mêmes que les mots de passe précédemment utilisés. | Si l'historique de mot de passe n'est pas maintenu, l'efficacité du changement de mot de passe est réduite, dans la mesure où il est possible de réutiliser indéfiniment les mots de passe précédents. Demander à ce que les mots de passe ne puissent pas être réutilisés pendant une certaine période de temps réduit la possibilité que des mots de passe qui ont été devinés ou forcés soient utilisés à l'avenir. |
| | **8.2.5.b** ***Procédures de test supplémentaires pour les prestataires de services :*** 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 mots de passe utilisés. | |
| **8.2.6** Définir des mots/phrases de passe pour la première utilisation et suite à réinitialisation pour une valeur unique pour chaque utilisateur et changent immédiatement après la première utilisation. | **8.2.6** Examiner les procédures relatives aux mots de passe et observer le personnel responsable 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 configurés sur une valeur unique à chaque utilisateur et qu'ils sont modifiés après leur première utilisation. | Si le même mot de passe est utilisé pour chaque nouvel utilisateur, un utilisateur interne, un ancien employé ou un individu malveillant peuvent connaître ou facilement découvrir ce mot de passe et l'utiliser pour accéder aux comptes. |
| **8.3** Incorporer une authentification à deux facteurs pour les accès à distance du personnel issu de l'extérieur du réseau (y compris pour les utilisateurs et les administrateurs) et pour tous les tiers (y compris l'accès du fournisseur à fin d'assistance ou de maintenance).<br><br>***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.*<br><br>*Les exemples de technologies à deux facteurs comprennent l'authentification à distance et service de renseignements par téléphone (RADIUS) avec jetons ; les* | **8.3.a** Examiner les configurations du système pour les systèmes et serveurs d'accès à distance afin de vérifier que l'authentification à deux facteurs est requise pour :<br>• Tous les accès à distance du personnel ;<br>• Tous les accès à distance de tiers/fournisseur (y compris les accès aux composants et systèmes des applications à fin d'assistance ou de maintenance). | L'authentification à deux facteurs requiert deux formes d'authentification pour les accès à haut risque, tels que ceux provenant de l'extérieur du réseau.<br><br>Cette condition est destinée à être appliquée à la totalité du personnel, y compris les utilisateurs de nature générale, les administrateurs et les fournisseurs (à fin d'assistance ou de maintenance) ayant un accès à distance au réseau, lorsque cet accès à distance peut permettre de pénétrer dans l'environnement des données de titulaires de carte.<br><br>Si un accès à distance s'effectue vers le réseau d'une entité possédant une segmentation appropriée, ces utilisateurs à distance ne peuvent accéder ni affecter l'environnement des données du titulaire et une authentification à deux facteurs pour l'accès à distance à ce réseau ne sera pas exigée. Cependant, l'authentification à deux facteurs est exigée pour tout accès à distance à des réseaux ayant eux-mêmes accès à l'environnement des |
| | **8.3.b** Observer un échantillon du personnel (par exemple les utilisateurs et les administrateurs) qui se connectent à distance au réseau et vérifier qu'au moins deux des trois méthodes d'authentification sont utilisées. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| *systèmes de contrôle d'accès au contrôleur d'accès du terminal (TACACS) avec jetons et les autres technologies permettant une authentification à deux facteurs.* | | données du titulaire et elle est recommandée pour tout accès à distance aux réseaux de l'entreprise. |
| **8.4** Documenter et communiquer les procédures et les politiques d'authentification à tous les utilisateurs, y compris :<br>• Des directives concernant la sélection de justificatifs d'authentification robustes ;<br>• Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ;<br>• Des instructions stipulant qu'il ne faut pas réutiliser les mots de passe ayant déjà été utilisés ;<br>• Des instructions expliquant comment changer les mots de passe si l'on soupçonne que le mot de passe est compromis. | **8.4.a** Examiner les procédures et interroger le personnel pour vérifier que les politiques et procédures d'authentification sont distribuées à tous les utilisateurs.<br><br>**8.4.b** Examiner les procédures et les politiques d'authentification qui sont distribuées aux utilisateurs et vérifier qu'elles comprennent :<br>• Des directives concernant la sélection de justificatifs d'authentification robustes ;<br>• Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ;<br>• Des instructions stipulant que les utilisateurs ne doivent pas réutiliser les mots de passe ayant déjà été utilisés ;<br>• Des instructions expliquant comment changer les mots de passe si l'on soupçonne que le mot de passe est compromis.<br><br>**8.4.c** Interroger un échantillon d'utilisateurs pour vérifier qu'ils connaissent les politiques et les procédures d'authentification. | Communiquer les procédures de mot de passe/authentification à tous les utilisateurs aide ces utilisateurs à comprendre et à respecter les politiques.<br><br>Par exemple, les directives sur la sélection de mots de passe robustes peuvent inclure des suggestions pour aider le personnel à sélectionner des mots de passe difficiles à deviner qui ne contiennent pas de mots du dictionnaire et qui ne contiennent pas d'informations concernant l'utilisateur (telles que l'ID utilisateur, les noms de membres de sa famille, date de naissance, etc.). Les directives pour la protection des justificatifs d'authentification peuvent inclure l'interdiction d'écrire les mots de passe ou de les enregistrer dans des fichiers non sécurisés, et ainsi que de rester vigilants au cas où un individu malveillant tenterait d'exploiter leurs mots de passe (par exemple, en appelant un employé pour lui demander son mot de passe en vue de « résoudre un problème »).<br><br>Demander aux utilisateurs de changer leur mot de passe s'il existe une possibilité que le mot de passe ne soit plus sécurisé peut empêcher aux utilisateurs malveillants d'utiliser un mot de passe légitime pour obtenir un accès non autorisé. |
| **8.5** Ne pas utiliser de méthode d'authentification par groupe, partagé ou de mots de passe d'ID génériques comme suit :<br>• Les ID d'utilisateur génériques sont désactivés ou supprimés.<br>• Les ID d'utilisateur partagés n'existent pas pour les fonctions | **8.5.a** Pour un échantillon de composants du système, examiner les listes d'ID d'utilisateur pour vérifier les points suivants :<br>• Les ID d'utilisateur génériques sont désactivés ou supprimés.<br>• Il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ;<br>• Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration du moindre composant du système. | Si plusieurs utilisateurs partagent les mêmes justificatifs d'authentification (par exemple, le même compte utilisateur et le même mot de passe), il devient impossible de retracer l'accès au système et les activités jusqu'à un individu. Cette caractéristique empêche à une entité de déterminer les responsabilités ou d'avoir un journal efficace des actions individuelles, dans la mesure où une action |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| d'administration du système et les autres fonctions critiques.<br>• Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration du moindre composant du système. | **8.5.b** Examiner les politiques/procédures d'authentification pour vérifier que les mots de passe ou autres méthodes d'authentification collectives et partagées sont interdites de façon explicite. | donnée pourrait avoir été accomplie par n'importe quelle personne du groupe ayant connaissance des justificatifs d'authentification. |
| | **8.5.c** Interroger les administrateurs système pour vérifier que les ID et/ou mots de passe ou autre méthode d'authentification de groupes et partagés ne sont pas distribuées, même en cas de demande. | |
| **8.5.1** ***Conditions supplémentaires pour les prestataires de services :*** Les prestataires de services ayant un accès à distance aux installations des clients (par exemple, pour l'assistance des systèmes ou des serveurs de POS) doivent utiliser un justificatif d'authentification unique (tel qu'un mot/phrase de passe) pour chaque client.<br><br>***Remarque :*** *Cette condition n'est pas prévue pour s'appliquer aux fournisseurs d'hébergement partagé qui accèdent à leur propre environnement d'hébergement, où de multiples environnements de client sont hébergés.*<br><br>***Remarque :*** *La condition 8.5.1 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.* | **8.5.1** ***Procédures de test supplémentaires pour les prestataires de services :*** Examiner les politiques et les procédures d'authentification et interroger le personnel pour vérifier que différentes authentifications sont utilisées pour accéder à chaque client. | Pour empêcher que de multiples clients soient compromis en utilisant un seul ensemble de justificatifs, les fournisseurs ayant des comptes d'accès à distance aux environnements de client doivent utiliser un justificatif d'authentification différent pour chaque client.<br><br>Les technologies, telles que les mécanismes à deux facteurs, qui donnent un justificatif unique pour chaque connexion (par exemple, au moyen d'un mot de passe unique) doivent toujours remplir le but de cette condition. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **8.6** Lorsque les autres mécanismes d'authentification sont utilisés (par exemple, des jetons de sécurité logiques ou physiques, des cartes électroniques, certificats, etc.), l'utilisation de ces mécanismes doit être assignée comme suit :<br>• Les mécanismes d'authentification doivent être affectés à un compte individuel et non pas partagés par de multiples comptes.<br>• Les contrôles logiques et/ou physiques doivent être en place pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès. | **8.6.a** Examiner les politiques et procédures d'authentification pour vérifier que les procédures des mécanismes d'authentification, comme les jetons de sécurité physique, les cartes électroniques et les certificats, soient définis et comprennent :<br>• Les mécanismes d'authentification ne sont affectés qu'à un seul compte individuel et non pas partagés par de multiples comptes.<br>• Les contrôles logiques et/ou physiques sont définis pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès. | Si les mécanismes d'authentification d'utilisateur, tels que les jetons, les cartes électroniques et les certificats, peuvent être utilisés par de multiples comptes, il pourrait être possible d'identifier l'individu qui utilise le mécanisme d'authentification. Appliquer des contrôles physiques et/ou logiques (par exemple un code PIN, des données biométriques ou un mot de passe) pour identifier de manière unique l'utilisateur du compte empêchera les utilisateurs non autorisés d'obtenir l'accès en utilisant un mécanisme d'authentification partagé. |
| | **8.6.b** Interroger le personnel responsable de la sécurité pour vérifier que les mécanismes d'authentification sont affectés à un compte et ne sont pas partagés par de multiples comptes. | |
| | **8.6.c** Examiner les réglages de configuration de système et/ou les contrôles physiques, s'il y a lieu, pour vérifier que les contrôles sont mis en œuvre pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès. | |
| **8.7** Tous les accès à n'importe quelle base de données contenant des données du titulaire (y compris les accès par les applications, administrateurs et autres utilisateurs) sont restreints comme suit :<br>• Tous les accès d'utilisateur, demandes d'utilisateur et actions d'utilisateur sur les bases de données ont lieu au moyen de méthodes de programmation.<br>• Seuls administrateurs de bases de données ont la possibilité d'accéder directement aux bases de données ou d'effectuer des demandes sur les | **8.7.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. | Sans une authentification des utilisateurs pour accéder aux bases de données et aux applications, les risques d'accès non autorisés ou à des fins malveillantes augmentent et ceux-ci ne peuvent pas être consignés dans les journaux puisque l'utilisateur n'a pas été authentifié et, par conséquent, est inconnu du système. En outre, l'accès aux bases de données doit être autorisé par un programme seulement (par exemple, par le biais de procédures stockées), plutôt qu'un accès direct des utilisateurs finaux à la base de données (à l'exception des DBA, qui peuvent nécessiter un accès direct dans le cadre de leurs tâches administratives). |
| | **8.7.b** Examiner les paramètres de configuration de la base de données et de l'application pour vérifier 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). | |
| | **8.7.c** Examiner les paramètres de contrôle d'accès à la base de données et les paramètres de configuration de la base de données de l'application et vérifier que tous les accès directs aux bases de données et toutes les consultations sont restreints aux | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| bases de données.<br>• Les ID d'application pour les applications de base de données peuvent uniquement être utilisés par les applications (et non par des utilisateurs individuels ou d'autres processus). | administrateurs de base de données. | |
| | **8.7.d** Examiner les paramètres de contrôle d'accès à la base de données, les paramètres de configuration d'application de base de données et les ID de l'application connexe pour vérifier que les ID d'application peuvent uniquement être utilisées par les applications (et non par des utilisateurs individuels ou d'autres processus). | |
| **8.8** Assurer que les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont documentées, utilisées et connues de toutes les parties concernées. | **8.8** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la gestion des identifications et des authentifications sur une base continuelle. |

## *Condition 9 : Restreindre l'accès physique aux données du titulaire*

Dans la mesure où tout accès physique à des données ou à des systèmes hébergeant des données du titulaire 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 du titulaire.

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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 du titulaire. | **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 du titulaire.<br>• Vérifier que l'accès est contrôlé par des lecteurs de badge et autres dispositifs tels que des badges autorisés, des clés et des cadenas.<br>• 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 du titulaire, et vérifier que ces consoles sont « verrouillées » pour empêcher toute utilisation non autorisée. | Sans contrôles d'accès physiques, tels que des systèmes de badge et des contrôles de porte, les personnes non autorisées pourraient potentiellement accéder à l'installation pour voler, désactiver, perturber ou détruire des systèmes critiques et des données du titulaire.<br>Le blocage des écrans de connexion sur les consoles empêche les personnes non autorisées d'accéder aux informations sensibles, d'altérer les configurations de système, d'introduire des vulnérabilités dans le réseau ou de détruire des archives. |
| **9.1.1** Installer des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès pour surveiller l'accès | **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. | Lors des enquêtes sur les violations physiques, ces contrôles peuvent aider à identifier les individus qui accèdent physiquement aux zones sensibles, ainsi |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| physique des individus aux zones sensibles. Examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi.<br><br>***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 du titulaire. Cette définition exclut les zones face au public où seuls les terminaux de point de vente sont présents, tels que les zones de caisse dans un magasin.* | **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. | que quand ils y entrent ou en sortent.<br><br>Les personnes malveillantes qui cherchent à obtenir un accès physique aux zones sensibles essayeront souvent de désactiver ou de contourner les contrôles de surveillance. Pour protéger ces contrôles des manipulations malveillantes, les caméras vidéos doivent être placées hors de portée et/ou surveillées pour détecter toute manipulation indésirable. De même, les mécanismes de contrôle d'accès pourraient être surveillés ou être munis de protections physiques pour les empêcher d'être endommagés ou désactivés par des individus malveillants.<br><br>*(suite à la page suivante)* |
| | **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. | Les exemples de zones sensibles comprennent les salles des serveurs de base de données de l'entreprise, les bureaux d'arrière-salle d'un point de vente au détail contenant des données du titulaire et les lieux de stockage d'un volume important de données du titulaire. Les zones sensibles doivent être identifiées par chaque organisation pour garantir que les surveillances physiques appropriées sont mises en œuvre. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.1.2** Mettre en œuvre des contrôles physiques et/ou logiques pour restreindre l'accès physique aux prises réseau accessibles au public.<br><br>*Par exemple, les prises de réseau situées dans les zones publiques et les zones accessibles aux visiteurs doivent être désactivées et uniquement activées lorsque l'accès au réseau est accepté de manière explicite. Autrement, des processus doivent être mis en œuvre pour assurer que les visiteurs sont accompagnés à tout moment dans les zones contenant des prises réseau actives.* | **9.1.2** Interroger le personnel responsable et observer les emplacements de prises réseau accessibles au public pour vérifier que des contrôles physiques et/ou logiques sont en place pour restreindre l'accès des prises réseau accessibles au public. | Restreindre l'accès aux prises réseau (ou aux ports réseau) empêchera les individus malveillants de se brancher aux prises réseau disponibles et d'accéder aux ressources des réseaux internes.<br><br>Qu'il s'agisse de contrôles logiques ou physiques, ou d'une combinaison des deux, ces contrôles doivent être suffisants pour empêcher un individu ou un dispositif qui n'est pas explicitement autorisé de pouvoir se connecter au réseau. |
| **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. | Sans mécanismes de sécurité couvrant les composants et les équipements sans fil, des utilisateurs malveillants pourraient utiliser les équipements sans fil de l'entreprise, laissés sans surveillance, pour accéder aux ressources du réseau, voire même connecter leurs propres équipements au réseau sans fil, obtenant ainsi un accès non autorisé. En outre, la sécurisation du réseau et du matériel de communications empêche les individus malveillants d'intercepter le trafic sur le réseau ou de connecter physiquement leurs propres dispositifs aux ressources réseau câblées. |
| **9.2** Développer des procédures pour distinguer facilement le personnel du site des visiteurs, en incluant :<br>• L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple)<br>• En changeant les conditions d'accès<br>• La révocation ou l'élimination de l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à | **9.2.a** Examiner les processus documentés pour vérifier que les procédures sont définies pour identifier et pour distinguer le personnel du site et les visiteurs.<br><br>Vérifier que les procédures comprennent les points suivants :<br>• L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple) ;<br>• Changement des conditions d'accès ;<br>• La révocation de l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à expiration (telle que les badges d'identification). | Identifier les visiteurs autorisés de manière à les distinguer facilement du personnel du site empêche les visiteurs non autorisés de bénéficier d'un accès à des zones contenant des données du titulaire. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| expiration (telle que les badges d'identification). | **9.2.b** Examiner les procédures pour identifier et pour distinguer le personnel du site et les visiteurs, afin de vérifier que :<br>• Les visiteurs sont clairement identifiés et<br>• Il est facile de distinguer le personnel du site des visiteurs. | |
| | **9.2.c** Vérifier que l'accès au processus d'identification (tel que le système de badge) est limité au personnel autorisé. | |
| | **9.2.d** Examiner les méthodes d'identification utilisées (telles que les badges ID) pour vérifier qu'elles identifient clairement les visiteurs et qu'il est facile de distinguer ces derniers du personnel du site. | |
| **9.3** Contrôler l'accès physique du personnel du site aux zones sensibles comme suit :<br>• L'accès doit être autorisé est basé sur les fonctions professionnelles individuelles.<br>• L'accès est immédiatement révoqué à la cessation de fonction de l'employé et tous les mécanismes d'accès physique, tels que les clés, cartes d'accès, etc., sont rendus ou désactivés. | **9.3.a** Pour un échantillon du personnel du site ayant un accès physique au CDE, interroger le personnel responsable et observer les listes de contrôle d'accès pour vérifier que :<br>• L'accès au CDEE est autorisé.<br>• L'accès est nécessaire pour les fonctions professionnelles de cette personne. | Le contrôle de l'accès physique au CDE aide à assurer que seul le personnel autorisé ayant un besoin professionnel légitime peut obtenir l'accès.<br>Lorsqu'un employé quitte l'organisation, tous les mécanismes d'accès physiques doivent être rendus ou désactivés promptement (dès que possible) après son départ, pour garantir que l'employé ne peut pas obtenir un accès physique au CDE après la cessation de ses fonctions. |
| | **9.3.b** Observer l'accès du personnel au CDE pour vérifier que la totalité du personnel est autorisée avant d'obtenir l'accès au CDE. | |
| | **9.3.c** Sélectionner un échantillon d'employé ayant récemment cessé leurs activités et examiner le contrôle d'accès pour vérifier que ce personnel n'a pas un accès physique au CDE. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.4** Mettre en œuvre des procédures pour identifier et autoriser les visiteurs.<br><br>Les procédures doivent inclure les points suivants : | **9.4** Vérifier que des autorisations de visiteurs et les contrôles d'accès sont en place comme suit : | Les contrôles de visiteurs sont d'une grande importance pour réduire la capacité des personnes non autorisées ou malveillantes à accéder aux installations (et éventuellement aux données du titulaire).<br><br>Les contrôles de visiteurs assurent que ceux-ci sont identifiables en tant que visiteurs de sorte que le personnel puisse surveiller leurs activités et que leur accès est limité à la durée de leur visite légitime.<br><br>Assurer que les badges de visiteurs soient retournés après expiration ou une fois la visite terminée empêchera les individus malveillants d'utiliser un passe autorisé précédemment pour obtenir un accès physique au bâtiment une fois que la visite est terminée.<br><br>Un registre des visiteurs comportant un minimum d'informations concernant le visiteur est une manière facile et peu onéreuse qui aidera à identifier les accès physiques aux bâtiments ou aux salles et les accès potentiels aux données du titulaire. |
| **9.4.1** Les visiteurs sont autorisés avant d'entrer et accompagnés en permanence dans les zones ou sont traitées et conservées les données du titulaire. | **9.4.1.a** Observer les procédures et interroger le personnel pour vérifier que les visiteurs doivent être autorisés avant d'entrer et accompagnés en permanence dans les zones où sont traitées et conservées les données du titulaire. | |
| | **9.4.1.b** Observer l'utilisation des badges de visiteur ou d'autres formes d'identification afin de vérifier qu'un badge jeton physique ne permet pas d'accéder sans accompagnement aux zones physiques où les données du titulaire sont stockées ou traitées. | |
| **9.4.2** Les visiteurs sont identifiés et un badge ou autre forme d'identification leur est remis avec une date limite d'utilisation, qui distingue clairement les visiteurs du personnel du site. | **9.4.2.a** Observer les gens au sein de l'établissement afin de vérifier l'utilisation des badges visiteur et pour assurer qu'ils permettent de clairement distinguer les visiteurs du personnel du site. | |
| | **9.4.2.b** Vérifier que les badges des visiteurs, ou autres formes d'identification, portent une date d'expiration. | |
| **9.4.3** Les visiteurs doivent rendre le badge ou autre forme d'identification physique avant de quitter les locaux ou à la date d'expiration. | **9.4.3** Observer les visiteurs qui quittent les locaux pour vérifier qu'on leur demande de restituer leur badge ou autre forme d'identification à la sortie ou à l'expiration. | |
| **9.4.4** Un registre des visites est utilisé pour maintenir un suivi d'audit de l'activité des visiteurs aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données du titulaire.<br><br>Y consigner le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son | **9.4.4.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 du titulaire. | |
| | **9.4.4.b** Vérifier que ce qui suit est consigné dans le journal :<br>• Le nom du visiteur,<br>• La société représentée et<br>• Le personnel du site qui autorise l'accès physique. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| accès physique.<br>Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi. | **9.4.4.c** Vérifier que le journal est conservé pendant au moins trois mois. | |
| **9.5** Assurer la sécurité physique de tous les supports. | **9.5** Vérifier que les procédures de protection des données du titulaire 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). | Les contrôles de la sécurité physique des supports sont destinés à empêcher les personnes non autorisées d'accéder aux données de carte contenues sur n'importe quel type de support. Les données du titulaire sont susceptibles d'être consultées, copiées ou scannées sans autorisation si elles se trouvent sur un support portable ou amovible, sont imprimées ou sont laissées sur le bureau d'un employé, sans protection. |
| **9.5.1** Ranger les sauvegardes sur support en lieu sûr, de préférence hors des locaux de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an. | **9.5.1.a** Observer la sécurité physique du site de stockage afin de confirmer que le stockage des supports de sauvegarde est sécurisé. | Si elles sont stockées dans un local non sécurisé, les sauvegardes contenant les données du titulaire peuvent être facilement perdues, volées ou copiées à des fins malveillantes. |
| | **9.5.1.b** Vérifier que la sécurité physique du site de stockage est passée en revue au moins une fois par an. | Un examen régulier du site de stockage permet à l'organisation de minimiser les risques de sécurité identifiés avec promptitude et de minimiser les risques potentiels. |
| **9.6** Assurer un contrôle strict de la distribution interne ou externe de tout type de support, notamment ce qui suit : | **9.6** 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. | Envisager de mettre en place des procédures et des processus de protection des données du titulaire se trouvant sur les supports distribués à des utilisateurs internes et/ou externes. En l'absence de telles procédures, ces données peuvent être perdues, volées ou utilisées à des fins frauduleuses. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.6.1** Classer les supports afin de déterminer la sensibilité des données qu'ils contiennent. | **9.6.1** Vérifier que tous les supports sont classés afin de déterminer la sensibilité des données qu'ils contiennent. | Il est important que les supports soient identifiés de manière à ce que ce statut de classification soit facilement identifié. S'ils ne sont pas identifiés comme confidentiels, les supports peuvent ne pas être protégés de la manière appropriée ou être perdus ou volés.<br>***Remarque :*** *Cela ne signifie par que les médias ont besoin d'être ornés d'étiquettes « confidentielles », l'objectif de cette condition est que l'organisation ait des supports identifiés contenant les données sensibles afin qu'elle puisse les protéger.* |
| **9.6.2** Envoyer les supports par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis. | **9.6.2.a** Interroger le personnel et examiner les archives pour vérifier que tous les supports expédiés à l'extérieur des locaux 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. | S'ils sont envoyés sans suivi, par exemple par courrier postal normal, les supports risquent d'être perdus ou volés. L'utilisation des services d'un coursier sécurisé pour l'envoi de tout support contenant des données du titulaire permet à l'organisation d'utiliser son système de suivi afin d'inventorier et localiser chaque envoi. |
| | **9.6.2.b** Choisir un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports, et vérifier que les informations de suivi sont consignées. | |
| **9.6.3** Assurer que les responsables approuvent le déplacement de tout support déplacé d'une zone sécurisée (en particulier s'ils sont distribués à des individus). | **9.6.3** Sélectionner un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports. En examinant les registres et en interrogeant le personnel responsable, vérifier que l'autorisation correcte des responsables est obtenir pour le déplacement de tout support déplacé d'une zone sécurisée (y compris lorsque les supports sont distribués à des individus). | Sans un processus ferme pour garantir que tous les mouvements de support sont approuvés avant que le support ne soit enlevé de zones sécurisées, le support ne sera pas suivi ou protégé correctement et son emplacement sera inconnu, ce qui pourrait mener à des supports perdus ou volés. |
| **9.7** Assurer un contrôle strict du stockage et de l'accessibilité des supports. | **9.7** 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. | Sans des méthodes d'inventaire et de contrôles du stockage méticuleux, le vol ou l'absence de supports pourraient passer inaperçus pendant une période indéterminée.<br>Si les supports ne font pas l'objet d'un inventaire, leur vol ou leur absence pourraient passer inaperçus pendant une période indéterminée ou même jamais. |
| **9.7.1** Tenir de manière appropriée les journaux d'inventaire de tous les supports et effectuer un inventaire des supports au moins une fois par an. | **9.7.1** Examiner les journaux d'inventaire des supports pour vérifier qu'ils sont maintenus et que les inventaires de support sont réalisés au moins une fois par an. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.8** Détruire les supports lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou légales comme suit : | **9.8** Examiner la politique de destruction périodique des supports et vérifier qu'elle couvre tous les supports et définit des conditions pour les points suivants :<br>• Les documents papier doivent être déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être constitués.<br>• Les conteneurs de stockage utilisés pour les documents qui sont détruits doivent être sécurisés.<br>• Les données du titulaire 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), ou par destruction physique du média. | Si les mesures nécessaires ne sont pas prises pour détruire les informations contenues sur les supports, disques durs, lecteurs portables, CD ou DVD ou papier, avant leur élimination, des individus malveillants peuvent être en mesure de récupérer des informations sur les supports éliminés et la sécurité des données s'en trouverait compromise. Par exemple, des individus malveillants peuvent utiliser une technique dénommée le « dumpster diving », qui consiste à fouiller les poubelles et les corbeilles, afin d'y rechercher des informations utiles pour lancer une attaque.<br>Les containers de stockage sécurisés utilisés pour le stockage des documents qui vont être détruits empêchent que les informations sensibles ne soient capturées lorsque les documents sont récoltés. Par exemple, les containers de documents « à déchiqueter » doivent être munis de cadenas pour empêcher l'accès à leur contenu ou un alliage physique prévient l'accès à l'intérieur du container.<br>L'effacement, la démagnétisation ou la destruction physique (comme le broyage ou l'effacement définitif du disque dur) sont des exemples de méthodes permettant la destruction sécurisée de supports électroniques. |
| **9.8.1** Déchiqueter, brûler ou réduire en pâte les documents papier de sorte que les données du titulaire ne puissent pas être reconstituées. Sécuriser les conteneurs de stockage utilisés pour les documents qui doivent être détruits. | **9.8.1.a** Interroger le personnel et examiner les procédures pour 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. | |
| | **9.8.1.b** Examiner les conteneurs dans lesquels sont stockées les documents à détruire afin de vérifier qu'ils sont sécurisés. | |
| **9.8.2** Rendre les données du titulaire sur support électronique irrécupérables de sorte que les informations ne puissent pas être reconstituées. | **9.8.2** Vérifier que les données du titulaire 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 du support. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.9** Protéger les dispositifs qui capturent les données de carte de paiement par interaction physique directe avec la carte des manipulations malveillantes et des substitutions.<br><br>***Remarque :*** *Ces conditions s'appliquent aux dispositifs de lecture de carte utilisés dans les transactions pour lesquelles la carte est présente (c'est-à-dire, une lecture de piste ou de puce) au point de vente. Cette condition n'est pas destinée à être appliquée pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.*<br><br>***Remarque :*** *La condition 9.9 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.* | **9.9** Examiner les politiques et procédures documentées pour vérifier que les points suivants sont inclus :<br>• Maintenir une liste des appareils ;<br>• Inspecter régulièrement les appareils pour s'assurer qu'ils n'ont pas été manipulés ou substitués ;<br>• Former le personnel pour qu'il soit conscient des comportements suspects et pour signaler les manipulations ou la substitution des appareils. | Les personnes malveillantes malveillantes essayent de voler les données du titulaire en volant et/ou en manipulant les appareils de lecture de carte et les terminaux. Par exemple, ils essayeront de voler les appareils afin de pouvoir apprendre comment y pénétrer et ils essayeront souvent de remplacer les appareils légitimes par des appareils frauduleux qui leur envoient les informations de carte de paiement dès que la carte est entrée dans l'appareil. Les personnes malveillantes essayeront également « d'écrémer » les composants à l'extérieur de l'appareil qui sont conçus pour capturer les détails de carte de paiement avant même qu'ils n'entrent dans l'appareil, par exemple, en ajoutant un lecteur de carte supplémentaire pour que les détails de carte de paiement soient capturés deux fois, une fois par le composant d'une personne malveillante et une fois par le composant légitime de l'appareil. De cette manière, les transactions peuvent tout de même avoir lieu sans interruption lorsque la personne malveillante « écrème » les informations de carte de paiement pendant le procédé.<br><br>Cette condition est recommandée, mais elle n'est pas requise pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.<br><br>Les meilleures pratiques supplémentaires pour la prévention de l'écrémage sont disponibles sur le site Web du PCI SSC. |
| **9.9.1** Maintenir une liste d'appareils à jour. La liste doit inclure les points suivants :<br>• Marque et modèle de l'appareil ;<br>• L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve | **9.9.1.a** Examiner la liste des appareils pour vérifier qu'elle comprend les éléments suivants :<br>• Marque et modèle de l'appareil ;<br>• L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve l'appareil) ;<br>• Le numéro de série de l'appareil ou autre méthode d'identification unique. | Conserver une liste des appareils à jour aide une organisation à suivre les emplacements où les appareils sont censés être et à identifier rapidement les appareils manquants ou perdus.<br><br>La méthode de maintenance d'une liste des appareils peut être automatisée (par exemple, à l'aide d'un système de gestion des appareils) ou |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| l'appareil) ;<br>• Le numéro de série de l'appareil ou autre méthode d'identification unique. | **9.9.1.b** Sélectionner un échantillon d'appareils sur la liste et vérifier que la liste est précise et maintenue à jour.<br><br>**9.9.1.c** Interroger le personnel pour vérifier que la liste des appareils est maintenue à jour lorsque des appareils sont ajoutés, déplacés, retirés du service, etc. | manuelle (par exemple, documentée sur support électronique ou papier). Pour les appareils sur la route, l'emplacement peut inclure le nom de l'employé auquel l'appareil est affecté. |
| **9.9.2** Inspecter régulièrement la surface des appareils pour voir si elle présente des signes de manipulations malveillantes (par exemple, l'ajout de | **9.9.2.a** Examiner les procédures documentées pour vérifier que des processus sont définis pour inclure les points suivants :<br>• Procédures d'inspection des appareils ;<br>• Fréquence des inspections. | Les inspections régulières aideront les organisations à détecter plus rapidement les manipulations malveillantes ou le remplacement d'un appareil, et donc de minimiser l'impact |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| copieur de carte sur l'appareil), ou de substitution (par exemple, en inspectant le numéro de série ou autre caractéristique de l'appareil pour vérifier qu'il n'a pas été substitué par un appareil frauduleux).<br><br>***Remarque :*** *Les exemples de signes qu'un appareil aurait pu être la victime de manipulations malveillantes ou substitué comprennent les fixations de câble ou de dispositifs inattendus à l'appareil, les étiquettes de sécurité manquantes ou modifiées, un boîtier cassé ou de couleur différente, ou un changement du numéro de série ou autres marques externes.* | **9.9.2.b** Interroger le personnel responsable et examiner les processus d'inspection pour vérifier que :<br><br>• Le personnel est conscient des procédures d'inspection des appareils.<br>• Tous les appareils sont inspectés régulièrement pour découvrir les évidences de manipulation malveillantes ou de substitutions. | potentiel de l'utilisation d'appareils frauduleux.<br><br>Le type d'inspection dépendra de l'appareil, par exemple, les photographies d'appareil dont on sait qu'ils sont sécurisés peuvent être utilisées pour comparer l'aspect actuel de l'appareil à son aspect d'origine afin de voir s'il a changé. Une autre option pourrait être d'utiliser un marqueur, tel qu'une marque UV légère, pour marquer les surfaces des appareils et les orifices de l'appareil afin que toute manipulation malveillante ou tout remplacement soit apparent. Souvent, les personnes malveillantes remplaceront le boîtier extérieur d'un appareil pour dissimuler leurs manipulations malveillantes et ces méthodes peuvent aider à détecter ce type d'activité. Les fournisseurs d'appareil doivent également être capables de donner des consignes de sécurité et des guides de « comment faire » pour aider à déterminer si l'appareil a été victime de manipulations malveillantes.<br><br>La fréquence des inspections dépendra des facteurs tels que l'emplacement de l'appareil et si l'appareil est ou non sous surveillance. Par exemple, les appareils laissés sans supervision dans les zones publiques par le personnel de l'organisation ont plus de chances de subir des inspections fréquentes que les appareils qui sont conservés dans des zones sécurisées ou qui sont supervisés lorsqu'ils sont accessibles au public. Le type et la fréquence des inspections sont déterminés par le type de commerçant, ainsi que le définit le processus annuel d'évaluation des risques. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.9.3** Assurer la formation du personnel afin qu'il soit conscient des tentatives de manipulation malveillantes ou de remplacement des appareils. La formation doit inclure les points suivants :<br>• Vérifier l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils.<br>• Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification.<br>• Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues).<br>• Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité). | **9.9.3.a** Examiner les documents de formation pour le personnel au point de vente pour vérifier qu'ils comprennent la formation à ce qui suit :<br>• La vérification de l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils.<br>• Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification.<br>• Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues).<br>• Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité).<br><br>**9.9.3.b** Interroger un échantillon du personnel au point de vente pour vérifier qu'il a reçu la formation adéquate et qu'il connaît les procédures pour ce qui suit :<br>• La vérification de l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils.<br>• Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification.<br>• Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues).<br>• Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité). | Souvent les personnes malveillantes prétendent être des agents de maintenance afin d'accéder aux appareils de POS. Tous les tiers demandant à avoir accès à l'appareil doivent toujours être vérifiés avant d'obtenir cet accès, par exemple, en vérifiant avec la direction, ou en contactant la société chargée de la maintenance (telle que le fournisseur ou l'acquéreur) au POS à fin de vérification. De nombreuses personnes malveillantes essayeront de tromper le personnel en s'habillant pour l'occasion (par exemple, en transportant des caisses à outil et en portant des vêtements de travail) et il est également possible qu'ils connaissent l'emplacement des appareils, il est donc important que le personnel soit formé pour qu'il suive en tout temps les procédures.<br><br>Une autre technique utilisée par les personnes malveillantes consiste à substituer un « nouveau » système de point de vente avec des instructions pour la substitution dans un système légitime et de « renvoyer » le système légitime à une adresse spécifiée. Les personnes malveillantes peuvent même fournir une enveloppe de retour de courrier, dans la mesure où ils sont fort désireux d'obtenir ces appareils. Le personnel vérifie toujours avec son responsable ou son fournisseur que l'appareil est légitime et qu'il provient d'une source approuvée avant de l'installer ou de l'utiliser dans l'entreprise. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **9.10** Assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données du titulaire sont documentées, utilisées et connues de toutes les parties concernées. | **9.10** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès physique aux données du titulaire sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour restreindre l'accès physique aux données du titulaire et aux systèmes CDE sur une base continuelle. |

# Surveillance et test réguliers des réseaux

### *Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données du titulaire*

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 | DIRECTIVES |
|---|---|---|
| **10.1** Implémenter des cheminements d'audit pour relier tous les accès aux composants du système à chaque utilisateur individuel. | **10.1** Vérifier, par l'observation et en interrogeant l'administrateur du système, que :<br>• Les cheminements d'audit sont activés et actifs pour les composants du système.<br>• L'accès aux composants du système est relié aux utilisateurs individuels. | Il est essentiel de disposer d'un processus ou d'un système qui établissent le lien entre l'accès d'un utilisateur et les composants du système auxquels il a accédé. Ce système génère des registres d'audit et permet de retracer les activités suspectes jusqu'à un utilisateur particulier. |
| **10.2** Mettre en œuvre des vérifications à rebours automatisées pour tous les composants du système afin de reconstituer les événements suivants : | **10.2** En interrogeant le personnel responsable, en observant les journaux d'audit et les paramètres de ces journaux d'audit, prendre les mesures décrites ci-après : | La vérification à rebours des activités suspectes alerte l'administrateur système, envoie les données à d'autres mécanismes de surveillance (comme des systèmes de détection d'intrusion) et établissent un historique pour le suivi après incident. Consigner les événements suivants permet à l'organisation d'identifier et de retracer des activités potentiellement malveillantes. |
| **10.2.1** Tous les accès des utilisateurs individuels aux données du titulaire | **10.2.1** Vérifier que tous les accès des utilisateurs aux données du titulaire sont consignés. | Les individus malveillants peuvent avoir connaissance d'un compte utilisateur et obtenir l'accès aux systèmes de l'environnement des données du titulaire ou créer un nouveau compte, non autorisé, afin d'accéder à ces données. Enregistrer tous les accès individuels aux données du titulaire permet d'identifier les comptes compromis ou utilisés de manière illicite. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **10.2.2** Toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur | **10.2.2** Vérifier que toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur sont consignées. | Les comptes possédant des privilèges accrus, comme les comptes « administrateur » ou « racine », sont potentiellement plus dangereux pour la sécurité ou la fonctionnalité opérationnelle d'un système s'ils venaient à être compromis. Sans un journal des activités exécutées, une organisation est incapable de retracer tout problème provoqué par une erreur administrative ou d'une utilisation illicite d'un privilège à l'action et à l'individu spécifiques. |
| **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. | Des utilisateurs malveillants tentent souvent de modifier les journaux d'audit afin de dissimuler leurs activités et un enregistrement des accès permet à une organisation de retracer toutes les incohérences ou altérations potentielles des journaux pour un compte individuel. Avoir accès aux journaux identifiant les changements, les additions et les suppressions pourrait aider à retracer les étapes suivies par le personnel non autorisé. |
| **10.2.4** Tentatives d'accès logique non valides | **10.2.4** Vérifier que les tentatives d'accès logique non valides sont consignées. | Les individus malveillants font souvent plusieurs tentatives pour accéder aux systèmes ciblés. De multiples tentatives infructueuses de connexion peuvent indiquer qu'un utilisateur non autorisé tente d'utiliser la « force brute » ou de deviner un mot de passe. |
| **10.2 5** L'utilisation et la modification des mécanismes d'identification et d'authentification, y compris notamment la création de nouveaux comptes et l'élévation de privilèges, et toutes les modifications, additions, suppressions aux comptes avec privilèges racines ou administratifs | **10.2.5.a** Vérifier que l'utilisation des mécanismes d'identification et d'authentification est consignée.<br>**10.2.5.b** Vérifier que toutes les élévations de privilège sont consignées.<br>**10.2.5.c** Vérifier que tous les changements, additions ou suppressions apportés à un compte avec privilèges racine ou administrateur sont consignées. | Sans savoir qui était connecté au moment d'un incident, il est impossible d'identifier les comptes qui ont pu être utilisés. En outre, les utilisateurs malveillants peuvent tenter de manipuler les contrôles d'authentification avec l'intention de les contourner ou d'usurper un compte valide. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **10.2.6** Initialisation, interruption ou pause des journaux d'audit | **10.2.6** Vérifier que ce qui suit est consigné dans le journal :<br>• L'initialisation des journaux d'audit ;<br>• L'Interruption ou pause des journaux d'audit. | La désactivation (ou pause) des journaux d'audit avant de se livrer à des activités illicites est une pratique courante des individus mal intentionnés souhaitant éviter d'être détectés. L'initialisation des journaux d'audit peut indiquer que la fonction de journalisation a été désactivée par un utilisateur pour dissimuler son activité. |
| **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 du système sont consignées. | Souvent, un logiciel malveillant crée ou remplace des objets au niveau système, sur le système visé, afin de prendre le contrôle d'une fonction particulière ou de l'activité de ce système. En effectuant les enregistrements dans le journal lorsque les objets au niveau du système, tels que les tableaux de base de données ou les procédures enregistrées, sont créés ou supprimés, il sera plus facile de déterminer si ces modifications ont été autorisées. |
| **10.3** Consigner dans les vérifications à rebours au moins les entrées suivantes pour chaque événement : | **10.3** En interrogeant le personnel et en observant les journaux d'audit pour chaque évènement vérifiable (à partir du point 10.2), et accomplissez ce qui suit : | Enregistrer ces détails pour les événements vérifiables au point 10.2 permet d'identifier rapidement une intrusion éventuelle, avec suffisamment de détails pour connaître l'auteur, l'objet, l'emplacement, le moment et la méthode employée. |
| **10.3.1** Identification de l'utilisateur | **10.3.1** Vérifier que l'identification d'utilisateur est incluse 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 de 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 de journaux. | |
| **10.3.5** Origine de l'événement | **10.3.5** Vérifier que l'origine de l'événement est incluse dans les entrées de 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 de journaux. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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.<br><br>***Remarque :*** *Le protocole Network Time Protocol (NTP -Protocole d'Heure Réseau) est un exemple de technologie de synchronisation temporelle.* | **10.4** Examiner les normes et les processus de configuration pour vérifier que la technologie de synchronisation de temporelle est mise en œuvre et conservée à jour selon les conditions 6.1 et 6.2 de la norme PCI DSS. | La technologie de synchronisation temporelle permet de synchroniser les horloges de systèmes multiples. Lorsque les horloges ne sont pas correctement synchronisées, il peut être difficile voire impossible, de comparer les fichiers journaux de systèmes différents et l'établissement de la séquence exacte d'un événement (un point crucial pour les analyses légales en cas de violation du système). Pour les équipes légales enquêtant après un incident, la précision et l'uniformité de l'heure sur l'ensemble des systèmes et celle de chaque activité sont essentielles pour déterminer la manière dont les systèmes ont été compromis. |
| **10.4.1** L'heure des systèmes critiques est correcte et la même pour tous. | **10.4.1.a** Examiner le processus d'acquisition et de distribution et de stockage de l'heure juste dans l'organisation pour vérifier que :<br>• Seuls le ou les serveurs d'heure centrale désignée reçoivent des signaux de sources externes et que ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné).<br>• Lorsqu'il y a plus d'un serveur d'heure désigné, les serveurs d'heure se basent l'un sur l'autre pour conserver une heure précise.<br>• Les systèmes reçoivent les informations concernant l'heure uniquement à partie des serveurs d'heure centrale désignés. | |
| | **10.4.1.b** Observer les réglages de paramètre de système liés à l'heure sur un échantillon de composants du système pour vérifier :<br>• Seuls le ou les serveurs d'heure centrale désignée reçoivent des signaux de sources externes et que ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné).<br>• Lorsqu'il y a plus d'un serveur d'heure désigné, le ou les serveurs d'heure centrale se basent l'un sur l'autre pour conserver une heure précise.<br>• Les systèmes reçoivent l'heure uniquement à partir des serveurs d'heure centrale désignés. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **10.4.2** Les données temporelles sont protégées. | **10.4.2.a** Examiner les configurations du système et des paramètres de synchronisation temporelle pour 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 configurations du système, les paramètres, journaux et processus 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** Examiner les configurations des systèmes pour 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 les administrateurs de système et examiner les autorisations et configurations de système pour vérifier que les cheminements d'audit sont sécurisés pour qu'ils ne puissent pas être modifiés comme suit : | Un individu malveillant, ayant pénétré sur le réseau, tentera souvent de modifier les journaux d'audit afin de dissimuler ses activités. Sans une protection adéquate des journaux d'audit, il ne sera pas possible d'en garantir l'intégralité, l'exactitude et l'intégrité et ils seront inutiles en tant qu'outil d'investigation une fois le système compromis. |
| **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** Seul un individu qui en a un besoin professionnel réel peut consulter les fichiers de journaux de vérification. | Une protection adéquate des journaux d'audit comprend un contrôle d'accès robuste (accès limité aux journaux en fonction du « besoin d'en connaître ») et l'utilisation d'un mécanisme d'isolation interne pour qu'il soit plus difficile de trouver et modifier les journaux.<br>Sauvegarder rapidement les fichiers journaux sur |
| **10.5.2** Protéger les fichiers de vérifications à rebours contre toute modification non autorisée. | **10.5.2** Les fichiers de piste d'audits sont protégés contre toute modification non autorisée par des mécanismes de contrôle d'accès, leur isolation physique et/ou l'isolation du réseau. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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** Les fichiers de piste d'audit sont rapidement sauvegardés sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer. | un serveur ou un support centralisé difficile à altérer conserve les journaux protégés même si le système qui génère les journaux est compromis. |
| **10.5.4** Inscrire les journaux pour les technologies orientées vers l'extérieur sur un serveur de journal interne centralisé et sécurisé, ou sur un dispositif de support. | **10.5.4** Les registres des technologies orientées vers l'extérieur (par exemple, sans-fil, pare-feu, DNS, messagerie) sont écrits sur un serveur de journal interne centralisé et sécurisé ou un support. | Renseigner les journaux depuis des technologies orientées vers l'extérieur, comme le sans-fil, les pare-feu, les serveurs DNS et les serveurs de messagerie, réduit les risques de perte ou de modification de ces journaux, car ils sont mieux protégés au sein du réseau interne.<br>Les journaux peuvent être écrits directement, issus ou copiés des systèmes externes, sur le système ou support interne sécurisé. |
| **10.5.5** Analyser les journaux à l'aide d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte). | **10.5.5** Examiner les paramètres de système, les fichiers surveillés et les résultats des activités de surveillance pour vérifier l'utilisation de la surveillance d'intégrité des fichiers ou de logiciel de détection de changement sur les journaux. | La surveillance d'intégrité des fichiers ou les systèmes de détection des changements inspectent les modifications apportées aux fichiers critiques et signalent les modifications. Pour surveiller l'intégrité des fichiers, une entreprise vérifie généralement les fichiers qui ne sont pas régulièrement modifiés, mais dont la modification indique une intrusion possible. |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **10.6** Examiner les journaux et les évènements de sécurité de tous les composants du système pour identifier les anomalies ou les activités suspectes.<br><br>***Remarque :*** *Des outils de journalisation, d'analyse et d'alerte peuvent être utilisés pour respecter cette condition.* | **10.6** Effectuez les tâches suivantes : | De nombreuses violations se produisent des jours ou des mois avant d'être détectées. La vérification quotidienne des journaux réduit la durée et l'exposition à une violation potentielle.<br><br>Les examens réguliers des journaux par le personnel ou automatiquement peuvent identifier et résoudre de manière proactive les accès non autorisés à l'environnement de données du titulaire.<br><br>Le processus d'examen des journaux ne doit pas forcément être manuel. L'utilisation d'outils de journalisation, d'analyse et d'alerte peut aider à faciliter le processus en identifiant les événements du journal qui doivent être examinés. |
| **10.6.1** Examiner les points suivants au moins une fois par jour :<br>• Tous les évènements de sécurité<br>• Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD, ou qui pourraient avoir un impact sur la sécurité des CHD ou SAD<br>• Les journaux de tous les composants critiques du système<br>• Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de | **10.6.1.a** Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour l'examen des points suivants au moins une fois par jour, manuellement ou à l'aide d'outils de journalisation :<br>• Tous les évènements de sécurité<br>• Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD, ou qui pourraient avoir un impact sur la sécurité des CHD ou SAD<br>• Les journaux de tous les composants critiques du système<br>• Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) | De nombreuses violations se produisent des jours ou des mois avant d'être détectées. La vérification quotidienne des journaux réduit la durée et l'exposition à une violation potentielle.<br><br>Des examens quotidiens des évènements de sécurité, par exemple, les notifications ou les alertes en cas d'identification d'activités suspectes ou anormales, ainsi que des journaux de composants critiques du système et des journaux de systèmes qui remplissent des fonctions de sécurité, tels que les pare-feu, IDS/IPS, systèmes de surveillance d'intégrité de fichier (FIM), etc. sont nécessaires pour identifier les problèmes potentiels. Remarquer que la détermination d'un « évènement de sécurité » variera pour chaque organisation et peut inclure une prise en compte |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) | **10.6.1.b** Observer les processus et interroger le personnel pour vérifier que des procédures suivantes sont mises en œuvre :<br>• Tous les évènements de sécurité<br>• Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD, ou qui pourraient avoir un impact sur la sécurité des CHD ou SAD<br>• Les journaux de tous les composants critiques du système<br>• Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) | du type de technologie, de l'emplacement et des fonctions de l'appareil. Les organisations peuvent aussi souhaiter maintenir une ligne de base de trafic « normal » pour aider à identifier les comportements anormaux. |
| **10.6.2** Examiner régulièrement les journaux de tous les autres composants du système conformément aux politiques et à la stratégie de gestion des risques de l'organisation, ainsi que le détermine l'évaluation de risque annuelle de l'organisation. | **10.6.2.a** Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour l'examen régulier des journaux de tous les autres composants du système, manuellement ou à l'aide d'outils de journalisation, conformément aux politiques et à la stratégie de gestion des risques de l'organisation. | Les journaux de tous les autres composants du système doivent également être examinés régulièrement pour identifier les indications de problèmes potentiels ou de tentatives d'accès aux systèmes sensibles par le biais de systèmes moins sensibles. La fréquence des examens doit être déterminée par une évaluation annuelle des risques effectuée par l'organisation. |
| | **10.6.2.b** Examiner la documentation d'évaluation des risques de l'entreprise et interroger le personnel pour vérifier que les examens sont effectués conformément aux politiques et à la stratégie de gestion des risques de l'organisation. | |
| **10.6.3** Suivi des exceptions et des anomalies identifiées pendant le processus d'examen. | **10.6.3.a** Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour le suivi des exceptions et des anomalies identifiées pendant le processus d'examen. | Si les exceptions et les anomalies identifiées pendant le processus d'examen de journal ne donnent pas lieu à une enquête, l'organisation serait susceptible d'ignorer les activités non autorisées et potentiellement malveillantes qui se produisent sur son propre réseau. |
| | **10.6.3.b** Observer les processus et interroger le personnel pour vérifier que le suivi des exceptions et des anomalies est effectué. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **10.7** Conserver l'historique des audits pendant une année au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, à fin d'analyse (par exemple, disponible en ligne, dans des archives ou pouvant être restaurés à partir d'une sauvegarde). | **10.7.a** Examiner les politiques et procédures pour vérifier qu'elles définissent les points suivants :<br>• Politiques de conservation des journaux d'audit<br>• Procédures de conservation des journaux d'audit pendant une année au moins, en gardant les journaux des trois derniers mois disponibles immédiatement en ligne. | Les journaux doivent être conservés pendant une année au moins puisqu'il faut un certain temps avant de s'apercevoir d'une violation et cela permet de donner aux enquêteurs un historique des informations de volume suffisant pour déterminer la durée d'une violation potentielle et du ou des systèmes éventuellement affectés. En gardant immédiatement à disposition les journaux des trois derniers mois au moins, une analyse peut rapidement identifier et minimiser l'impact d'une violation des données. Le stockage des journaux hors ligne peut empêcher qu'ils soient facilement accessibles à la lecture et provoquer des durées plus longues pour la restauration des données de journaux, la performance des analyses et l'identification des systèmes ou données affectés. |
| | **10.7.b** Interroger le personnel et examiner les journaux d'audit pour vérifier qu'ils sont disponibles pendant un an au moins. | |
| | **10.7.c** Interroger le personnel et examiner les processus pour vérifier que les journaux des trois derniers mois au moins peuvent être immédiatement restaurés pour analyse. | |
| **10.8** Assurer que les politiques de sécurité et les procédures opérationnelles pour la surveillance de tous les accès aux ressources du réseau et aux données du titulaire sont documentées, utilisées et connues de toutes les parties concernées. | **10.8** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la surveillance de tous les accès aux ressources du réseau et aux données du titulaire sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles quotidiennes pour la surveillance de tous les accès aux ressources du réseau et aux données du titulaire sur une base continuelle. |

## *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 | DIRECTIVES |
|---|---|---|
| **11.1** Mettre en œuvre des processus pour tester la présence de points d'accès sans-fil (802.11) ; détecter et identifier tous les points d'accès sans-fil autorisés et non autorisés sur une base trimestrielle.<br><br>***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.*<br><br>*Quelles que soient les méthodes utilisées, elles doivent être suffisantes pour détecter et identifier les appareils autorisés ainsi que les appareils non autorisés.* | **11.1.a** Examiner les politiques et les procédures pour vérifier que des processus sont définis pour la détection et l'identification des points d'accès sans-fil autorisés et non autorisés sur une base trimestrielle.<br><br>**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 :<br>• Cartes WLAN insérées dans les composants du système ;<br>• Appareils portables ou mobiles reliés à un composant du système pour créer un point d'accès sans-fil (par exemple, par USB, etc.) ;<br>• Périphériques sans fil branchés sur un port réseau ou à un périphérique réseau.<br><br>**11.1.c** Examiner le résultat des scans de réseau sans-fil récents pour vérifier que :<br>• Les points d'accès autorisés et non autorisés sont identifiés ; et<br>• Le scan est effectué au moins une fois par trimestre pour tous les composants et toutes les installations du système.<br><br>**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 informer le personnel. | La mise en œuvre et/ou l'exploitation de la technologie sans fil sur un réseau font partie des voies les plus fréquentes utilisées par les utilisateurs malveillants pour accéder au réseau et aux données du titulaire. Si un périphérique ou un réseau sans fil est installé à l'insu d'une société, il peut permettre à un pirate de pénétrer facilement sur le réseau, à l'insu de tous. Des dispositifs sans-fil non autorisés peuvent être dissimulés dans, ou connectés à, un ordinateur ou à un autre composant du système, ou encore être directement connectés à un port ou à un dispositif du réseau, comme un commutateur ou un routeur. Un tel dispositif non autorisé peut constituer un point d'accès non autorisé à l'environnement.<br><br>Savoir quels sont les appareils sans fil qui sont autorisés peut aider les administrateurs à identifier rapidement les appareils non autorisés et répondre à l'identification de points d'accès sans-fil aide à minimiser de manière proactive l'exposition du CDE aux individus malveillants.<br><br>En raison de la facilité avec laquelle un point d'accès sans fil peut être connecté à un réseau, de la difficulté à détecter leur présence et du risque accru associé aux équipements sans fil non autorisés, ces processus doivent être exécutés même s'il existe une politique interdisant l'usage de la technologie sans fil.<br><br>La taille et la complexité d'un environnement particulier déterminent les outils et processus appropriés à utiliser afin de fournir une garantie suffisante qu'un point d'accès mal intentionné n'a |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| | | pas été installé dans l'environnement.<br>*(suite à la page suivante)* |
| **11.1.1** Maintenir un registre des points d'accès sans-fil autorisés comprenant une justification commerciale documentée. | **11.1.1** Examiner les archives documentées pour vérifier qu'un registre des points d'accès sans-fil autorisés est maintenu et que la justification commerciale est documentée pour tous les points d'accès sans-fil documentés. | ***Par exemple :*** *Dans le cas d'un simple terminal autonome dans un centre commercial, où tous les composants de communication sont contenus dans des boîtiers inviolables et, comportant des dispositifs pour rendre les effractions évidentes, une inspection physique détaillée du terminal lui-même peut suffire à s'assurer qu'aucun point d'accès frauduleux n'y a été branché ni installé. Cependant, dans un environnement comportant des nœuds multiples (comme un grand magasin de détail, un centre d'appels, une salle de serveur ou un centre de données), il est plus difficile d'effectuer une inspection physique détaillée. Dans ce cas, diverses méthodes peuvent être combinées afin de remplir les conditions, par exemple, effectuer des inspections physiques du système conjointement aux résultats d'un analyseur sans fil.* |
| **11.1.2** Mettre en œuvre des procédures de réponse aux incidents au cas où des points d'accès non autorisés sont détectés. | **11.1.2.a** Examiner le plan de réponse aux incidents de l'organisation (Condition 12.10) pour vérifier qu'il définit et exige une réponse au cas où un point d'accès sans-fil non autorisé est détecté. | |
| | **11.1.2.b** Interroger le personnel responsable et/ou inspecter les derniers scans de réseau sans-fil et les réponses connexes pour vérifier que des mesures sont prises lorsqu'un point d'accès sans-fil non autorisé est découvert. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **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).<br><br>***Remarque :*** *De multiples rapports de scan peuvent être combinés pour que le processus de scan trimestriel montre que tous les systèmes ont été scannés et que toutes les vulnérabilités applicables ont été traitées. Une documentation supplémentaire peut être requise pour vérifier que les vulnérabilités qui n'ont pas été résolues sont en phase de l'être.*<br><br>*Pour la conformité initiale à la norme PCI DSS, il n'est pas obligatoire que quatre scans trimestriels aient été réalisées avec succès si l'évaluateur vérifie que 1) le résultat du dernier scan était réussi, 2) l'entité a documenté les politiques et les procédures exigeant l'exécution de scans trimestriels et 3) toutes les vulnérabilités relevées dans les résultats ont été corrigées, comme indiqué lors de la réexécution du scan. Pour les années qui suivent la vérification PCI DSS initiale, quatre scans trimestriels réussis ont été réalisées.* | **11.2** Examiner les rapports de scan et la documentation connexe pour vérifier que les scans de vulnérabilité internes et externes sont effectués comme suit : | Un scan de vulnérabilité est un outil automatisé exécuté sur les équipements et les serveurs internes et externes du réseau, conçu pour exposer les vulnérabilités potentielles qui pourraient être détectées et exploitées par des individus malveillants.<br><br>Il existe trois types de scans de vulnérabilité requis pour la norme PCI DSS :<br><br>• Le scan de vulnérabilité interne trimestriel effectué par un personnel qualifié (l'utilisation d'un fournisseur de service de scan approuvé (ASV) n'est pas recommandée)<br>• Le scan de vulnérabilité externe trimestriel, qui doit être effectué par un ASV.<br>• Les scans internes et externes sont requis après tout changement d'importance.<br><br>Une fois ces faiblesses identifiées, l'organisation les corrige et répète le scan jusqu'à ce que toutes les vulnérabilités aient été corrigées.<br><br>Identifier les vulnérabilités et y remédier en temps opportun réduit la probabilité qu'elles soient exploitées et permettent de compromettre un composant de système ou des données du titulaire. |
| **11.2.1** Effectuer le scan de vulnérabilité interne trimestriel et recommencer si nécessaire, jusqu'à ce que les | **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. | Un processus établi d'identification des vulnérabilités sur des systèmes internes exige que les scans de vulnérabilité soient effectués |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| vulnérabilités à « haut risque » (identifiées par la condition 6.1) soient résolues. Les scans doivent être exécutés par un personnel qualifié. | **11.2.1.b** Examiner les rapports de scan et vérifier que le processus de scan comprend les nouveaux scans jusqu'à ce que toutes les vulnérabilités à « haut risque », définies à la condition 6.1 de la norme PCI DSS, aient été résolues. | trimestriellement. Les vulnérabilités constituant le risque le plus important pour l'environnement (par exemple, celles classées à « haut risque » aux termes de la condition 6.1) doivent être résolues en priorité absolue.<br>Les scans de vulnérabilité interne peuvent être exécutées par un personnel interne qualifié, raisonnablement indépendant du ou des composants de système analysés (par exemple, un administrateur de pare-feu ne doit pas être chargé du scan de pare-feu), ou une entreprise peut choisir de faire exécuter ces scans de vulnérabilité interne par un prestataire de services spécialisé dans l'analyse des vulnérabilités. |
| | **11.2.1.c** Interroger le personnel pour vérifier que le scan 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). | |
| **11.2.2** Des analyses de vulnérabilité externe doivent être effectuées une fois par trimestre par un prestataire de services de scan agréé par le PCI SSC (Payment Card Industry Security Standards Council -Conseil des normes de sécurité PCI). Recommencer le scan si nécessaire, jusqu'à ce que les scans soient réussis.<br>***Remarque :*** *Les scans de vulnérabilité externe doivent être effectués une fois par trimestre par un prestataire de services de scan agréé (ASV) par le PCI SSC (Payment Card Industry Security Standards Council-Conseil des normes de sécurité PCI).*<br>*Consulter le Guide de programme ASV publié sur le site Web du PCI SSC pour connaître les responsabilités du client vis-à-vis du scan, la préparation du scan, etc.* | **11.2.2.a** Examiner les résultats des quatre scans trimestriels de vulnérabilité externe les plus récents et vérifier qu'ils ont tous eu lieu au cours des 12 derniers mois. | Les réseaux externes étant plus exposés, le scan trimestriel de vulnérabilités externes doit être exécuté par un prestataire de services d'analyse agréé (ASV) par le PCI SSC. |
| | **11.2.2.b** Examiner les résultats de chacun des quatre scans trimestriels pour s'assurer qu'ils 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 de scan pour vérifier que les scans ont été réalisées par un prestataire de services de scan agréé (ASV) par le PCI SSC. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **11.2.3** Effectuer les scans internes et externes et recommencez si nécessaire, après tout changement d'importance. Les scans doivent être exécutés par un personnel qualifié. | **11.2.3.a** Inspecter et mettre en corrélation la documentation de changement de contrôle et les rapports de scan afin de vérifier que les composants du système sujets à un changement d'importance ont été scannés. | Déterminer ce qui constitue un changement significatif dépend considérablement de la configuration d'un environnement donné. Si une mise à jour ou une modification touche uniquement les données du titulaire ou affecte la sécurité de l'environnement de données du titulaire, elle doit être considérée comme significative.<br>L'analyse d'un environnement, après avoir apporté des modifications d'importance à ce dernier, garantit que les modifications ont été réalisées de la manière appropriée et que la sécurité de l'environnement n'a pas été compromise à la suite de ces modifications. Tous les composants du système affectés par les modifications doivent être scannés. |
| | **11.2.3.b** Examiner les rapports d'analyse et vérifier que le processus d'analyse stipule de nouvelles analyses jusqu'à ce que :<br>• Pour les scans externes, aucune vulnérabilité supérieure à la note 4.0 du CVSS n'existe.<br>• Pour les scans internes, toutes les vulnérabilités à « haut risque », définies dans la condition 6.1 de la norme PCI DSS sont résolues. | |
| | **11.2.3.c** Confirmer que le scan 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** Mettre en œuvre une méthodologie pour le test de pénétration qui inclut ce qui suit :<br>• Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115)<br>• Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques<br>• Comprend un test depuis l'intérieur et l'extérieur du système<br>• Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée.<br>• Définit les tests de pénétration de couche d'application pour qu'ils comprennent, au minimum les | **11.3** Examiner la méthodologie de test de pénétration et interroger le personnel responsable pour vérifier qu'une méthodologie est mise en œuvre qui comprend les points suivants :<br>• Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115)<br>• Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques<br>• Test depuis l'intérieur et l'extérieur du système<br>• Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée.<br>• Définit les tests de pénétration de couche d'application pour qu'ils comprennent, au minimum les vulnérabilités indiquées dans la Condition 6.5.<br>• Définit les tests de pénétration de couche d'application pour qu'ils comprennent les composants qui prennent en | L'objectif d'un test de pénétration est de simuler une attaque en conditions réelles dans le but d'identifier jusqu'où un pirate pourrait pénétrer dans un environnement donné. Ceci permet à une entreprise d'avoir une meilleure compréhension de son exposition éventuelle au risque et de développer une stratégie de défense contre les attaques.<br>Un test de pénétration diffère d'un scan de vulnérabilité, dans la mesure où le test de pénétration est un processus actif pouvant comprendre l'exploitation de vulnérabilités identifiées. Exécuter un scan de vulnérabilité peut être l'une des premières étapes effectuées par le test de pénétration afin de planifier la stratégie de test, bien que ce ne soit pas la seule étape. Même si le scan de vulnérabilité ne détecte pas de |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| vulnérabilités indiquées dans la Condition 6.5.<br>• Définit les tests de pénétration de couche d'application pour qu'ils comprennent les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation.<br>• Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois<br>• Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation.<br><br>***Remarque :*** *Cette mise à jour à la condition 11.3 est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation. Les conditions de la norme PCI DSS v2.0 pour le test de pénétration doivent être suivies jusqu'à ce que la v3.0 soit en place.* | charge les fonctions réseau, tels que les systèmes d'exploitation.<br>• Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois<br>• Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation. | vulnérabilités connues, la personne exécutant le test de pénétration obtiendra suffisamment d'informations sur le système pour identifier les lacunes éventuelles dans la sécurité.<br><br>Le test de pénétration est généralement un processus en grande partie manuel. Bien qu'il soit possible d'utiliser certains outils automatisés, la personne réalisant le test doit utiliser sa connaissance des systèmes pour pénétrer dans un environnement. Souvent elle appliquera plusieurs types d'exploits ensemble dans le but de franchir plusieurs couches de défenses. Par exemple, si elle trouve un moyen d'accéder à un serveur d'application, elle utilisera ensuite le serveur compromis comme point de départ pour lancer une nouvelle attaque en fonction des ressources auxquelles le serveur a accès. De cette manière, la personne effectuant le test est en mesure de simuler les méthodes utilisées par un pirate afin d'identifier les zones de faiblesse potentielles dans l'environnement.<br><br>*Les techniques de test de pénétration seront différentes pour les différentes organisations et le type, la profondeur et la complexité des tests dépendront de l'environnement spécifique et de l'évaluation des risques de l'organisation.* |
| **11.3.1** Effectuer des tests de pénétration *externe* au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement). | **11.3.1.a** Examiner la portée du travail et les résultats du dernier test de pénétration externe pour vérifier qu'un tel test est effectué comme suit :<br>• Selon la méthodologie définie<br>• Au moins une fois par an<br>• Après les changements significatifs de l'environnement.<br><br>**11.3.1.c** Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que l'organisation du testeur est bien indépendante (pas obligatoirement être un QSA ou un ASV). | Les tests de pénétration effectués régulièrement et après les changements significatifs apportés à l'environnement constituent une mesure de sécurité proactive qui aide à minimiser les risques d'accès potentiel au CDE par des individus malveillants.<br><br>Déterminer ce qui constitue un changement ou significatif ou une mise à jour significative dépend considérablement de la configuration d'un environnement donné. Si une mise à jour ou une modification touche uniquement les données du |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **11.3.2** Effectuer des tests de pénétration *internes* au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement). | **11.3.2.a** Examiner la portée du travail et les résultats du dernier test de pénétration interne pour vérifier qu'un tel test est effectué au moins une fois par an et après tout changement significatif de l'environnement.<br>• Selon la méthodologie définie<br>• Au moins une fois par an<br>• Après les changements significatifs de l'environnement. | titulaire ou affecte la sécurité de l'environnement de données du titulaire, elle doit être considérée comme significative. Les tests de pénétration après les mises à jour et les modifications du réseau permettent d'assurer que tous les contrôles en place fonctionnent toujours aussi efficacement après le déploiement de la mise à niveau ou de la modification. |
| | **11.3.2.b** Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que l'organisation du testeur est bien indépendante (pas obligatoirement être un QSA ou un ASV). | |
| **11.3.3** Les vulnérabilités exploitables découvertes pendant le test de pénétration sont corrigées et les tests sont recommencés pour vérifier les corrections. | **11.3.3** Examiner les résultats de test de pénétration pour vérifier que les vulnérabilités exploitables ont été corrigées et que les nouveaux tests ont confirmés que la vulnérabilité a été corrigée. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **11.3.4** Si la segmentation est utilisée pour isoler le CDE des autres réseaux, effectuer des tests de pénétration au moins une fois par an après toute modification de méthode/contrôle de segmentation pour vérifier que les méthodes de segmentation sont opérationnelles et efficaces, et isoler les systèmes hors de portée des systèmes inclus dans la portée. | **11.3.4.a** Examiner les contrôles de segmentation et examiner la méthodologie de test de pénétration pour vérifier que les procédures de test de pénétration sont définies pour qu'elles testent toutes les méthodes de segmentation afin de confirmer qu'elles sont opérationnelles et efficaces, et isoler les systèmes hors de portée des systèmes inclus dans la portée. | Les tests de pénétration sont un outil important pour confirmer que toutes les segmentations en place pour isoler le CDE des autres réseaux sont efficaces. Les tests de pénétration doivent se concentrer sur les contrôles de segmentation, à la fois depuis l'extérieur du réseau de l'entité et de l'intérieur du réseau, mais hors du CDE, pour confirmer qu'ils ne peuvent pas passer les contrôles de segmentation pour accéder au CDE. Par exemple, les tests de réseau et/ou les scans de ports ouverts pour vérifier l'absence de connectivité entre les réseaux dans la portée et les réseaux hors de portée. |
| | **11.3.4.b** Examiner les résultats du dernier test de pénétration externe pour vérifier que les tests de pénétration confirment que la segmentation :<br>• Est réalisée au moins une fois par an et après toute modification aux méthodes/contrôles de segmentation.<br>• Couvre toutes les méthodes/contrôles de segmentation utilisées.<br>• Vérifie que les méthodes de segmentation sont opérationnelles et efficaces, et isole les systèmes hors de portée des systèmes dans la portée. | |
| **11.4** Utiliser les techniques d'intrusion-détection et/ou d'intrusion-prévention pour détecter et/ou empêcher les intrusions dans le réseau. Surveiller la totalité du trafic au périmètre de l'environnement de données du titulaire, ainsi qu'aux points critiques de l'environnement des données du titulaire et alerter le personnel en cas de soupçons de compromis.<br>Tenir à jour tous les moteurs d'intrusion-détection et de prévention, les lignes de base et les signatures. | **11.4.a** Examiner les configurations de système et les diagrammes de réseau pour vérifier que des techniques (telles que les systèmes d'intrusion-détection et/ou des systèmes d'intrusion/prévention) sont en place pour la surveillance du trafic :<br>• Au périmètre de l'environnement de données du titulaire ;<br>• Aux points critiques de l'environnement de données du titulaire. | Les techniques de détection d'intrusion et/ou de prévention d'intrusion (telles qu'IDS/IPS) comparent le trafic entrant sur le réseau avec des « signatures » connues et/ou des comportements de milliers de types de violations (outils de piratage, chevaux de Troie et autres logiciels malveillants), envoient des alertes et/ou bloquent la tentative. Sans une approche proactive à la détection des activités non autorisées, les attaques (ou l'utilisation frauduleuse) des ressources d'un ordinateur pourraient passer inaperçues au moment où elles se produisent. Les alertes de sécurité générées par ces techniques doivent être surveillées de manière à pouvoir bloquer les tentatives d'intrusion. |
| | **11.4.b** Examiner les configurations du système et interroger le personnel responsable pour confirmer que les techniques d'intrusion-détection et/ou d'intrusion-prévention alertent le personnel en cas de soupçon de compromis. | |
| | **11.4.c** Examiner les configurations IDS/IPS et la documentation du fournisseur pour vérifier que les techniques d'intrusion/détection et/ou d'intrusion/prévention sont configurées, maintenues et mises à jour selon les instructions du fournisseur afin d'assurer une protection optimale. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **11.5** Déployer des mécanismes de détection de changement (par exemple, des outils de surveillance de l'intégrité des fichiers) pour alerter le personnel de toute modification non autorisée des fichiers critiques du système, fichiers de configuration ou fichiers de contenu et configurer le logiciel pour qu'il effectue des comparaisons de fichier critique au moins une fois par semaine.<br><br>***Remarque :*** *Pour la détection des changements, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les mécanismes de détection des changements tels que les produits de surveillance d'intégrité de fichier sont généralement préconfigurés avec les fichiers critiques pour le système d'exploitation connexe. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).* | **11.5.a** Vérifier l'utilisation de mécanismes de détection des changements dans l'environnement des données du titulaire en examinant les paramètres système et les fichiers contrôlés, ainsi que les résultats des activités de surveillance.<br><br>Exemples de fichiers qui doivent être contrôlés :<br>▪ Exécutables du système ;<br>▪ Exécutables des applications ;<br>▪ Fichiers de configuration et de paramètres ;<br>▪ Fichiers d'historique, d'archive, de registres et d'audit stockés à un emplacement centralisé.<br>▪ Les fichiers critiques supplémentaires déterminés par l'entité (par exemple, avec l'évaluation de risque ou par d'autres moyens). | Les solutions de détection de changement comme les outils de surveillance d'intégrité des fichiers (FIM) vérifient et signalent les modifications apportées aux fichiers stratégiques. S'ils ne sont pas mis en œuvre correctement et que les résultats de la solution de détection de changement sont contrôlés, un individu malveillant pourrait altérer la configuration des contenus de fichier, des programmes de système d'exploitation ou d'exécutables d'application. Les modifications non autorisées, si elles ne sont pas détectées, peuvent rendre inutiles les contrôles de sécurité existants et/ou aboutir au vol des données du titulaire sans aucun impact perceptible au niveau du traitement normal. |
| | **11.5.b** Vérifier que le mécanisme est configuré 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. | |
| **11.5.1** Mettre en œuvre un processus pour répondre à n'importe quelle alerte générée par la solution de détection de changement. | **11.5.1** Interroger le personnel pour vérifier que les alertes sont contrôlées et résolues. | |

| CONDITIONS PCI DSS | PROCÉDURES DE TEST | DIRECTIVES |
|---|---|---|
| **11.6** Assurer que les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sont documentées, utilisées et connues de toutes les parties concernées. | **11.6** Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sont :<br>• Documentées,<br>• Utilisées et<br>• Connues de toutes les parties concernées. | Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sur une base continuelle. |

# Gestion d'une politique de sécurité des informations

### *Condition 12 : Maintenir une politique qui adresse les informations de sécurité 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 du titulaire.

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.1** Établir, publier, maintenir et diffuser une politique de sécurité. | **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). | La politique de sécurité des informations d'une entreprise génère la feuille de route de l'application des mesures de sécurité afin de protéger ses ressources les plus précieuses. Tout le personnel doit être sensibilisé au caractère confidentiel des données et à ses responsabilités dans la protection de ces informations. |
| **12.1.1** Examiner la politique de sécurité au moins une fois par an et mettre la politique à jour lorsque l'environnement change. | **12.1.1** 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. | Les menaces à la sécurité et les méthodes de protection évoluent rapidement. Sans une mise à jour de la politique de sécurité afin de refléter ces changements, les nouvelles mesures de protection contre ces menaces sont inutiles. |
| **12.2** Mettre en œuvre un processus d'évaluation des risques qui :<br>• Est effectué au moins une fois pas an et à la suite des changements | **12.2.a** Vérifier qu'un le processus annuel d'évaluation des risques est documenté qui identifie les actifs, les menaces et les vulnérabilités, et donne lieu à évaluation formelle des risques. | Une évaluation des risques permet à une organisation d'identifier les menaces et les vulnérabilités associées, pouvant avoir un impact négatif sur son activité. Des ressources peuvent |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| significatifs apportés à l'environnement (par exemple acquisition, intégration, déménagement, etc.)<br>• Identifie les actifs critiques, les menaces et vulnérabilités, et<br>• Donne lieu à une évaluation formelle des risques.<br>*Les exemples de méthodologies d'évaluation des risques comprennent entre autres les directives OCTAVE, ISO 27005 et NIST SP 800-30.* | **12.2.b** Examiner la documentation d'évaluation des risques, afin de vérifier que le processus d'évaluation des risques est exécuté au moins une fois par an et suite aux changements significatifs de l'environnement. | alors être effectivement affectées pour mettre en place des contrôles qui réduisent la probabilité et/ou l'impact potentiel de la menace.<br>Effectuer des évaluations du risque au moins une fois par an et suite aux changements significatifs permet à l'organisation de rester à jour en ce qui concerne les changements organisationnels et l'évolution des menaces, des tendances et des technologies. |
| **12.3** Développer les politiques d'utilisation des technologies critiques et définir l'utilisation adéquate de ces technologies.<br>***Remarque :*** *Les exemples de technologies critiques comprennent notamment l'accès à distance et les technologies sans fil, les ordinateurs portables, les tablettes, les supports électroniques amovibles, l'utilisation d'e-mail et d'Internet.*<br>S'assurer que ces politiques d'utilisation exigent ce qui suit : | **12.3** Examiner les politiques d'utilisation des technologies critiques et interroger le personnel responsable pour vérifier que les politiques suivantes sont mises en œuvre et respectées : | Les politiques d'utilisation par le personnel peuvent interdire l'usage de certains équipements et autres technologies si c'est la politique de la société, ou donner au personnel des directives d'utilisation et d'application appropriées. Si ces politiques d'utilisation n'existent pas, le personnel peut utiliser des technologies enfreignant la politique de la société, permettant ainsi à des individus malveillants d'accéder aux systèmes stratégiques et aux données du titulaire. |
| **12.3.1** Approbation explicite des responsables | **12.3.1** Vérifier que les politiques d'utilisation comprennent des processus pour l'approbation explicite des parties autorisées pour l'utilisation des technologies. | Si l'approbation appropriée d'application de ces technologies n'est pas exigée, un employé peut, en toute innocence, installer une solution dont il estime avoir besoin pour son activité, mais ouvrir en même temps une brèche importante qui expose les données et les systèmes stratégiques à des individus malveillants. |
| **12.3.2** Authentification pour l'utilisation des technologies | **12.3.2** Vérifier que les politiques d'utilisation comprennent des processus pour que toute utilisation de la technologie soit identifiée avec l'ID utilisateur et le mot de passe, ou tout autre élément d'identification (par exemple, un jeton). | Si la technologie est mise en œuvre sans une authentification appropriée (ID utilisateur et mots de passe, jetons, VPN, etc.), des individus malveillants peuvent facilement utiliser cette technologie non protégée pour accéder aux systèmes stratégiques et aux données du titulaire. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.3.3** Liste de tous les périphériques et du personnel disposant d'un accès | **12.3.3** Vérifier que les politiques d'utilisation définissent une liste de tous les périphériques et personnel autorisé à utiliser ce matériel. | Des individus malveillants peuvent violer la sécurité physique et placer leurs propres équipements sur le réseau sous forme de « porte dérobée ». Le personnel peut également contourner les procédures et installer ses propres dispositifs. L'inventaire précis des équipements, avec un étiquetage approprié, permet d'identifier rapidement les installations non approuvées. |
| **12.3.4** Une méthode permettant de déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils) | **12.3.4** Vérifier que les politiques d'utilisation définissent une méthode pour déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils) | Des individus malveillants peuvent violer la sécurité physique et placer leurs propres équipements sur le réseau sous forme de « porte dérobée ». Le personnel peut également contourner les procédures et installer ses propres dispositifs. L'inventaire précis des équipements, avec un étiquetage approprié, permet d'identifier rapidement les installations non approuvées. Envisager d'établir une convention de dénomination officielle des appareils et de consigner tous les appareils aux contrôles d'inventaires mis en place. L'étiquetage logique peut être utilisé pour des informations comme des codes pouvant établir le lien entre un dispositif et son propriétaire, indiquer ses coordonnées et son objectif. |
| **12.3.5** Usages acceptables de la technologie | **12.3.5** Vérifier que les politiques d'utilisation définissent les utilisations acceptables de la technologie. | En définissant l'usage professionnel acceptable et l'emplacement des équipements et des technologies approuvés par la société, cette dernière pourra mieux gérer et contrôler les failles des configurations et des contrôles opérationnels, afin de s'assurer qu'aucune « porte dérobée » n'est ouverte pour permettre l'accès d'un individu malveillant aux systèmes stratégiques et aux données du titulaire. |
| **12.3.6** Emplacements acceptables des technologies sur le réseau | **12.3.6** Vérifier que les politiques d'utilisation définissent les 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 comprennent 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 | **12.3.8.a** Vérifier que les politiques d'utilisation exigent la déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique. | Les technologies d'accès à distance constituent souvent des « portes dérobées » vers les ressources stratégiques et données du titulaire. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| spécifique | **12.3.8.b** Examiner les configurations des technologies d'accès à distance pour vérifier que les sessions d'accès à distance sont automatiquement déconnectées après une période d'inactivité spécifique. | Déconnecter ces technologies à distance lorsqu'elles ne sont pas utilisées (par exemple, celles qui sont utilisées pour la maintenance des systèmes par les fournisseurs de POS et autres ou les partenaires commerciaux), permet de réduire l'accès au réseau et le risque afférent. |
| **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. | |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.3.10** Lors de l'accès du personnel aux données du titulaire au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données du titulaire sur des disques durs locaux et des supports électroniques amovibles, sauf autorisation expresse pour un besoin professionnel défini.<br><br>Lorsqu'il existe un besoin professionnel autorisé, la politique d'utilisation doit exiger que les données soient protégées selon toutes les conditions applicables de la norme PCI DSS. | **12.3.10.a** Vérifier que les politiques d'utilisation interdisent la copie, le déplacement ou le stockage des données du titulaire 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. | Pour assurer que l'ensemble du personnel est conscient qu'il ne doit pas stocker ni copier les données du titulaire sur un ordinateur local personnel ni sur aucun autre support, votre politique doit clairement interdire ces activités, sauf pour le personnel qui y est expressément autorisé. Le stockage ou la copie des données du titulaire sur un disque dur local ou un autre support doit être effectué conformément à toutes les conditions applicables de la norme PCI DSS. |
| | **12.3.10.b** Pour le personnel dûment autorisé, vérifier que les politiques d'utilisation exigent la protection des données du titulaire 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 matière de sécurité. | **12.4.a** Vérifier que les politiques de sécurité des informations définissent clairement les responsabilités de tout le personnel en matière de sécurité. | Sans une définition claire des responsabilités et des rôles en matière de sécurité, l'interaction avec le groupe chargé de la sécurité peut être incohérente, conduisant alors au déploiement non sécurisé de technologies ou à l'usage de technologies obsolètes ou non sécurisées. |
| | **12.4.b** Interroger un échantillon du personnel responsable pour vérifier qu'il comprend les politiques de sécurité. | |
| **12.5** Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations : | **12.5** Examiner les politiques et procédures concernant la sécurité pour vérifier :<br>• L'assignation formelle de la sécurité des informations à un chef de la sécurité ou tout autre membre compétent de la direction.<br>• Les responsabilités suivantes de gestion de la sécurité des informations sont attribuées de manière spécifique et formelle : | Chaque individu ou équipe responsable de la gestion de la sécurité des informations doit avoir parfaitement conscience de ses responsabilités et des tâches associées, grâce à une politique spécifique. Sans cette responsabilisation, les lacunes dans les processus peuvent donner accès aux ressources stratégiques et aux données du titulaire. |
| **12.5.1** Définir, documenter et diffuser les politiques et les procédures de sécurité. | **12.5.1** Vérifier que la responsabilité de l'établissement, de la documentation et de la distribution des procédures et politiques de sécurité est formellement attribuée. | |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **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 de la surveillance, de l'analyse des alertes de sécurité, et de la diffusion des informations aux chefs de division 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, de la documentation et de la distribution de la réponse aux incidents de sécurité et les procédures d'escalade est formellement assignée. | |
| **12.5.4** Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification des comptes | **12.5.4** Vérifier que la responsabilité de l'administration des comptes d'utilisateur (l'ajout, la suppression et la modification) et de la gestion des authentifications est formellement assignée. | |
| **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. | |
| **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 du titulaire. | **12.6.a** Examiner le programme de sensibilisation à la sécurité pour vérifier qu'il sensibilise la totalité du personnel à l'importance de la sécurité des données du titulaire. | Si le personnel n'est pas sensibilisé à ses responsabilités en matière de sécurité, les processus et les protections mis en place peuvent s'avérer inefficaces en raison des erreurs commises ou d'actes délibérés. |
| | **12.6.b** Examiner les procédures et la documentation du programme de sensibilisation à la sécurité, et procéder comme suit : | |
| **12.6.1** Former le personnel au moment du recrutement et au moins une fois par an.<br><br>***Remarque :*** *Les méthodes varient selon les postes occupés et le niveau d'accès du personnel aux données du titulaire.* | **12.6.1.a** 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). | Si le programme de sensibilisation à la sécurité ne comporte pas de sessions annuelles de mise à niveau, les processus et procédures essentiels de sécurité pourront être oubliés ou ignorés, exposant alors des ressources stratégiques et des données du titulaire. |
| | **12.6.1.b** Vérifier que le personnel participe aux formations de sensibilisation à la sécurité au moment de son recrutement et au moins une fois par an. | |
| | **12.6.1.c** Interroger un échantillon du personnel pour vérifier qu'ils ont effectué une formation de sensibilisation et qu'ils sont conscients de l'importance de la sécurité des données du titulaire. | |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **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. | Exiger une reconnaissance écrite ou par voie électronique permet de s'assurer que les politiques et procédures de sécurité ont bien été lues et comprises et de l'engagement passé et futur du personnel à les respecter. |
| **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.)<br><br>***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 des contrôles des antécédents (dans les restrictions imposées par la loi) pour le personnel qui aura accès aux données du titulaire ou à l'environnement de ces données. | La vérification approfondie des antécédents avant toute embauche de personnel amené à accéder aux données du titulaire réduit le risque d'une utilisation non autorisée des PAN et autres données du titulaire par des individus avec des antécédents de personnes malveillantes ou discutables. |
| **12.8** Maintenir et mettre en œuvre des politiques et des procédures de gestion des prestataires de services avec lesquelles les données du titulaire sont partagées, ou qui pourraient affecter la sécurité des données du titulaire comme suit : | **12.8** En observant et en examinant les politiques et procédures et la documentation connexe, vérifier que les processus sont mis en œuvre pour gérer les prestataires de services avec lesquels les données du titulaire sont partagées, ou qui pourraient affecter la sécurité des données du titulaire (par exemple les installations de stockage de sauvegarde, les prestataires de services gérés tels que les sociétés d'hébergement Web ou les prestataires de services de sécurité, ceux qui reçoivent les données à fin de modelage de fraude, etc.), comme suit : | Si un commerçant ou un prestataire de services partage des données du titulaire avec un autre prestataire de services, certaines conditions s'appliquent afin de garantir que la continuité de la protection de ces données sera respectée par ces prestataires de services. |
| **12.8.1** Tenir une liste des prestataires de services. | **12.8.1** Vérifier qu'une liste des prestataires de services est tenue. | Conserver un suivi de tous les prestataires de services permet d'identifier jusqu'où s'étendent les risques potentiels à l'extérieur de l'entreprise. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.8.2** Maintenir un accord écrit par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données du titulaire qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données du titulaire.<br><br>***Remarque :*** *La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.* | **12.8.2** Examiner les accords écrits et confirmer qu'ils comprennent une reconnaissance par laquelle les prestataires de services admettent qu'ils sont responsables de la sécurité des données du titulaire qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données du titulaire. | Par cet accord, les prestataires de services reconnaissent leur engagement à assurer la sécurité appropriée des données du titulaire obtenues auprès de leurs clients.<br><br>En conjonction avec la condition 12.9, cette exigence d'accord écrit entre les organisations et les prestataires de services est destinée à promouvoir un niveau d'entente constant entre les parties concernant les responsabilités qui leur incombent dans le cadre de la norme PCI DSS. Par exemple, l'accord peut inclure les conditions applicables de la norme PCI DSS à maintenir dans le cadre de la prestation de service. |
| **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 documentées et mises en œuvre, notamment le contrôle préalable à l'engagement de tout prestataire de services. | Ce processus garantit que le choix du prestataire de services a été vérifié en interne par l'organisation, et doit comporter une analyse des risques avant d'établir une relation formelle quelconque avec ce prestataire.<br><br>Les processus et les objectifs de diligence spécifique seront différents pour chaque organisation. Les exemples de considération peuvent inclure les pratiques de rapport du prestataire, les procédures de notification d'infraction et de réponse aux incidents, les détails de la manière avec laquelle les responsabilités de la norme PCI DSS sont affectées entre chaque partie, comment le prestataire valide sa conformité à la norme PCI DSS et quelles preuves il peut fournir, etc. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.8.4** Maintenir un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an. | **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. | Connaître le statut du prestataire de services en termes de conformité à la norme PCI DSS permet de s'assurer et de tenir compte du fait qu'il doit respecter les mêmes conditions que votre organisation. Si le prestataire de services offre des services divers, cette condition doit s'appliquer aux services réellement fournis au client et aux services qui sont dans le champ d'application de l'évaluation PCI DSS du client.<br><br>Les informations spécifiques conservées par une organisation dépendront de l'accord spécifique passé avec ses prestataires, du type de service, etc. Le but est que l'organisation évaluée comprenne les conditions de la norme PCI DSS que ses prestataires doivent respecter. |
| **12.8.5** Maintenir les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation. | **12.8.5** Vérifier que l'organisation conserve les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation. | |
| **12.9** ***Conditions supplémentaires pour les prestataires de services*** **:** Les prestataires de services reconnaissent par écrit qu'ils sont responsables de la sécurité des données du titulaire qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données du titulaire.<br><br>***Remarque :*** *Cette condition est considérée comme une meilleure pratique jusqu'au 30 juin 2015, après quoi ce sera une obligation.*<br><br>***Remarque :*** *La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.* | **12.9** ***Procédures de test supplémentaires pour les prestataires de services :*** Examiner les politiques et procédures du prestataire de service et observez les modèles d'accord écrit pour confirmer que le prestataire de service reconnaît par écrit aux clients qu'il respectera toutes les conditions applicables de la norme PCI DSS dans la mesure où il traite, a accès, stocke ou transmet les données du titulaire du client ou autres données d'identification sensibles ; ou gère l'environnement de données du titulaire du client de la part d'un client. | Cette condition s'applique lorsque l'organisation évaluée est un prestataire de service. En conjonction avec la Condition 12.8.2, cette condition est destinée à promouvoir un niveau de compréhension constant entre les prestataires de services et leurs clients, concernant les responsabilités applicables de la norme PCI DSS. Par cet accord, les prestataires de services reconnaissent leur engagement à assurer la sécurité appropriée des données du titulaire obtenues auprès de leurs clients.<br><br>La méthode par laquelle le prestataire de service peut effectuer cette reconnaissance par écrit doit être convenue entre le prestataire et ses clients. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.10** Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système. | **12.10** Examiner le plan de réponse aux incidents et les procédures connexes pour vérifier que l'organisation est prête à répondre immédiatement à une faille du système, comme suit : | Sans un plan détaillé de réponse aux incidents, correctement diffusé, lu et compris par les parties responsables, une certaine confusion et l'absence de réponses unifiées pourraient entraîner une interruption des activités de l'entreprise, avec une publicité inutile de la part des médias publics, ainsi que de nouvelles responsabilités légales. |
| **12.10.1** Élaborer le plan de réponse aux incidents à mettre en place en cas d'intrusion dans le système. S'assurer que le plan prévoit au moins les points suivants :<br>• Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ;<br>• Les procédures de réponse aux incidents spécifiques ;<br>• Les procédures de continuité et de reprise des affaires ;<br>• Processus de sauvegarde des données ;<br>• Analyse des exigences légales en matière de signalement des incidents ;<br>• Couverture et réponses de tous les composants stratégiques du système ;<br>• Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement. | **12.10.1.a** Vérifier que le plan de réponse aux incidents inclut :<br>• Les rôles, les responsabilités et les stratégies de communication en cas d'incident, notamment la notification des marques de cartes de paiement, au minimum ;<br>• Les procédures de réponse aux incidents spécifiques ;<br>• Les procédures de continuité et de reprise des affaires ;<br>• Processus de sauvegarde des données ;<br>• 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) ;<br>• La couverture et les réponses de tous les composants stratégiques du système ;<br>• Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement. | Le plan de réponse aux incidents doit être complet et comporter tous les éléments essentiels permettant à la société de réagir efficacement en cas de violation susceptible d'affecter les données du titulaire. |
| | **12.10.1.b** Interroger le personnel et 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. | |
| **12.10.2** Tester le plan au moins une fois par an. | **12.10.2** Vérifier que le plan est testé au moins une fois par an. | Sans des tests appropriés, des étapes essentielles peuvent être omises et entraîner une exposition accrue durant un incident. |

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **12.10.3** Désigner le personnel spécifique disponible 24 heures sur 24 et sept jours sur sept pour répondre aux alertes. | **12.10.3** À travers l'observation, l'examen des politiques et les contacts avec le personnel responsable, vérifier que le personnel désigné est disponible 24 heures sur 24 et sept jours sur sept pour répondre aux incidents 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. | Sans une équipe de réponse aux incidents bien formée et disponible, à tout moment, le réseau peut être gravement endommagé, et les données et les systèmes stratégiques peuvent être « pollués » par une manipulation inappropriée des systèmes ciblés. Cela peut empêcher l'enquête réalisée après un incident d'aboutir. |
| **12.10.4** Organiser la formation appropriée du personnel responsable de la réponse aux violations de la sécurité. | **12.10.4** Vérifier par l'observation, l'examen des politiques et les contacts avec le personnel responsable que le personnel chargé de la réponse aux violations de la sécurité reçoit une formation périodique. | |
| **12.10.5** Inclure les alertes des systèmes de surveillance de sécurité, notamment les systèmes d'intrusion-détection, intrusion-prévention, les pare-feu et les systèmes de surveillance de l'intégrité des fichiers. | **12.10.5** À travers l'observation et l'examen des processus, vérifier que la surveillance et la réponse aux alertes émises par les systèmes de surveillance de sécurité, y compris la détection des points d'accès sans-fil non autorisés, sont couverts dans le plan de réponse aux incidents. | Ces systèmes de surveillance, axés sur les risques potentiels encourus par les données, sont essentiels pour agir rapidement afin de prévenir une violation et ils doivent être intégrés aux processus de réponse aux incidents. |
| **12.10.6** Définir un processus de modification et de développement du plan de réponse aux incidents en fonction des leçons apprises, et tenir compte de l'évolution du secteur. | **12.10.6** À travers l'observation, l'examen des politiques et les contacts avec le personnel, 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. | Intégrer au plan de réponse aux incidents les « leçons tirées » après un problème permet de garder ce plan à jour et de réagir face aux nouvelles menaces et tendances en matière de sécurité. |

# 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 du titulaire*

Comme il est indiqué dans les conditions 12.8 et 12.9, tous les prestataires de services qui ont accès aux données du titulaire (notamment les prestataires de services d'hébergement partagé) doivent respecter la norme PCI DSS. En outre, la condition 2.6 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.

| Conditions | Procédures de test | Directive |
|---|---|---|
| **A.1** Protéger les données et l'environnement hébergés de chaque entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité), conformément aux conditions A.1.1 à A.1.4 :<br><br>Un prestataire de services d'hébergement doit satisfaire à ces conditions ainsi qu'aux conditions de toutes les autres rubriques pertinentes de la norme PCI DSS.<br><br>***Remarque :*** *Même si un prestataire de services d'hébergement peut satisfaire à ces conditions, la conformité de l'entité qui a recours au prestataire de services d'hébergement n'est pas garantie. Chaque entité doit se conformer à la norme PCI DSS et doit valider cette conformité comme applicable.* | **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 : | *L'annexe A* de la norme PCI DSS est destinée aux prestataires de services d'hébergement partagé qui souhaitent fournir à leurs clients commerçants et/ou prestataires de services un environnement d'hébergement conforme à cette norme. |

| Conditions | Procédures de test | Directive |
|---|---|---|
| **A.1.1** S'assurer que chaque entité ne met en œuvre que les processus qui ont accès à l'environnement des données du titulaire 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 :<br>• Aucune entité sur le système ne peut utiliser un ID d'utilisateur partagé sur le serveur Web.<br>• Tous les scripts CGI utilisés par une entité doivent être créés et exécutés sous l'ID d'utilisateur unique de l'entité. | Si un commerçant ou un prestataire de services est autorisé à exécuter ses propres applications sur le serveur partagé, il doit le faire avec l'ID utilisateur du commerçant ou du prestataire de services, et non en tant qu'utilisateur privilégié. |
| **A.1.2** Restreindre l'accès et les privilèges de chaque entité à son propre environnement de données du titulaire. | **A.1.2.a** Vérifier que l'ID d'utilisateur de tout processus d'application n'est pas un utilisateur avec des privilèges (racine/admin). | Pour s'assurer que l'accès et les privilèges sont restreints de telle sorte que chaque commerçant et prestataire de services ne puisse accéder qu'à son propre environnement, tenir compte des facteurs suivants :<br>1. Privilèges de l'ID utilisateur de serveur Web du prestataire de service ou du commerçant ;<br>2. Permissions accordées pour lire, écrire et exécuter des fichiers ;<br>3. Permissions accordées pour écrire les systèmes binaires ;<br>4. Permissions accordées aux fichiers de journalisation de prestataire de service et de commerçant ; et<br>5. Contrôles pour assurer qu'un commerçant ou un prestataire de service ne puisse pas monopoliser les ressources du système. |
| | **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.).<br>**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 :<br>• Espace disque,<br>• Bande passante,<br>• Mémoire,<br>• Processeur. | |

| Conditions | Procédures de test | Directive |
|---|---|---|
| **A.1.3** S'assurer que la journalisation et les vérifications à rebours sont activées, uniques à l'environnement des données du titulaire 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 :<br>• Les journaux sont activés pour les applications tierces courantes ;<br>• Les journaux sont activés par défaut ;<br>• Les journaux peuvent être consultés par l'entité à laquelle ils appartiennent ;<br>• Les emplacements des journaux sont clairement communiqués à l'entité propriétaire. | Dans un environnement d'hébergement partagé, des journaux doivent être disponibles afin que les commerçants et les prestataires de services puissent accéder et examiner les journaux spécifiques à leur environnement de données du titulaire. |
| **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. | Les fournisseurs d'hébergement partagé doivent disposer de processus permettant une réponse rapide et simple en cas d'enquête légale après incident, et permettant un niveau de détail approprié, allant jusqu'à comprendre les informations sur le commerçant ou le prestataire de services à titre individuel. |

# Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux conditions de la norme PCI DSS comme 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 déployé, des contrôles de sécurité associés et de la configuration du contrôle proprement dit. Les sociétés doivent avoir conscience qu'un contrôle compensatoire particulier ne sera pas efficace dans tous les environnements.*

   a) Les 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 restreindre 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 du titulaire 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 clause 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 clauses :**

| | 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 clause :** *8.1.1 – Tous les utilisateurs sont-ils identifiés avec un ID utilisateur unique leur permettant d'accéder aux composants du système et aux données du titulaire ?*

| | 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 « racine ». La société XYZ ne peut pas gérer le nom d'utilisateur « racine » ni consigner toutes les activités de chaque utilisateur « racine ».* |
| **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 unique 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 ordinateur de bureau à l'aide de la commande « SU » (substitut d'utilisateur). Cette commande autorise les utilisateurs à accéder au compte « racine » et à exécuter des actions sous ce compte, tout en leur permettant de consigner leurs activités dans le répertoire du journal SU. De cette manière, les actions de chaque utilisateur peuvent être suivies grâce au compte SU, le mot de passe « racine » étant partagé par les utilisateurs.* |
| **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 toutes les activités effectuées par ces individus en utilisant la commande sont consignées afin d'identifier que l'individu effectue des actions en utilisant les privilèges du compte racine.* |
| **6. Gestion** | Définir les processus et les contrôles en place pour la | *La société XYZ décrit les processus et les procédures mis en place pour éviter la* |

| | | |
|---|---|---|
| | gestion des contrôles compensatoires. | *modification, l'altération ou la suppression des configurations SU de sorte que des utilisateurs individuels puissent exécuter des commandes racines sans que leurs activités soient consignées et suivies.* |

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