



# Payment Card Industry Standard de Sécurité des Données

---

## Exigences et Procédures de Test

**Version 4.0.1**

Juin 2024

## Versions du Document

Date	Version	Description
Octobre 2008	1.2	Présenter PCI DSS v1.2 en tant que « exigences et procédures d'évaluation de la sécurité PCI DSS », en éliminant la redondance entre les documents et en apportant des modifications générales et spécifiques par rapport aux procédures d'audit de la sécurité PCI DSS v1.1. Pour obtenir des informations complètes, consultez le Récapitulatif des modifications pour le standard de sécurité des données PCI de la version 1.1 à la version 1.2 du standard PCI DSS.
Juillet 2009	1.2.1	Ajouter la phrase qui a été supprimée par erreur entre v1.1 et v1.2 du standard PCI DSS.
		Corriger « alors » par « que » dans les procédures de test 6.3.7.a et 6.3.7.b.
		Supprimer le marquage grisé pour les colonnes « en place » et « pas en place » dans la procédure de test 6.5.b.
		Pour la Feuille de travail sur les mesures de sécurité compensatoires - Exemple complété, corriger le libellé en haut de la page pour indiquer : « Utiliser cette feuille de travail pour définir des mesures de sécurité compensatoires pour toute exigence marquée comme « en place » via des mesures de sécurité compensatoires. »
Octobre 2010	2.0	Mise à jour et implémentation des modifications du v1.2.1. Voir PCI DSS – Synthèse des modifications pour la PCI DSS Version 1.2.1 à Version 2.0.
Novembre 2013	3.0	Mise à jour du v2.0. Voir PCI DSS – Synthèse des modifications pour la PCI DSS Version 2.0 à Version 3.0.
Avril 2015	3.1	Mise à jour de la PCI DSS v3.0. Voir PCI DSS – Synthèse des modifications pour la PCI DSS Version 3.0 à Version 3.1 pour de détails sur les changements.
Avril 2016	3.2	Mise à jour de la PCI DSS v3.1. Voir PCI DSS – Synthèse des modifications pour la PCI DSS Version 3.1 à Version 3.2 pour de détails sur les changements.
Mai 2018	3.2.1	Mise à jour de la PCI DSS v3.2. Voir PCI DSS – Synthèse des modifications pour la PCI DSS Version 3.2 à Version 3.2.1 pour des détails sur les changements.
Mars 2022	4.0	Remplacer le titre actuel du document par «Standard de sécurité des données de la Payment Card Industry: Exigences et Procédures de Test.» Mise à jour à partir du PCI DSS v3.2.1. Voir PCI DSS - Synthèse des modifications du standard PCI DSS Version 3.2.1 à 4.0 pour des détails concernant les modifications.
Juin 2024	4.0.1	Mise à jour depuis PCI DSS v4.0. Voir PCI DSS - Synthèse des modifications de PCI DSS version 4.0 à 4.0.1 pour plus de détails sur les modifications.

**REMERCIEMENTS :** La version anglaise de ce document, telle que mise à disposition sur le site Internet du PCI SSC, à toutes fins, est considérée comme la version officielle de ces documents et, dans la mesure où il existe des ambiguïtés ou des incohérences entre la rédaction de ce texte et du texte anglais, la version anglaise disponible à l'endroit mentionné prévaudra.

## Table des Matières

1	Introduction et Présentation du Standard de Sécurité des Données PCI .....	5
2	Informations sur les Conditions D'applicabilité du Standard PCI DSS .....	8
3	Relation entre les Standards Logiciels PCI DSS et PCI SSC .....	12
4	Périmètre des Exigences du Standard PCI DSS .....	14
5	Bonnes Pratiques pour la mise en œuvre du Standard PCI DSS dans les Processus des Affaires Courantes (Business-as-Usual ou « BAU ») .....	26
6	Pour les Auditeurs : Échantillonnage pour les Évaluations du Standard PCI DSS .....	29
7	Description des Délais Utilisés dans les Exigences PCI DSS .....	33
8	Approches pour la mise en œuvre et la Validation du Standard PCI DSS .....	36
9	Protéger les Informations Relatives à L'état de Sécurité d'une Entité .....	39
10	Méthodes de Test pour les Exigences du Standard PCI DSS .....	41
11	Instructions et Contenu du Rapport de Conformité .....	42
12	Processus D'évaluation du Standard PCI DSS .....	43
13	Autres Références .....	44
14	Versions du Standard PCI DSS .....	45
15	Exigences Détaillées du Standard PCI DSS et Procédures de Test .....	46
	Créer et Maintenir un Réseau et des Systèmes Sécurisés .....	48
	<i>Exigence 1 : Installer et Maintenir des Mesures de Sécurité du Réseau</i> .....	48
	<i>Exigence 2 : Appliquer des Configurations Sécurisées à tous les Composants Système</i> .....	70
	Protéger les Données de Carte .....	85
	<i>Exigence 3 : Protéger les Données de Carte Stockées</i> .....	85
	<i>Exigence 4 : Protéger les Données des Titulaires de Cartes Grâce à une Cryptographie Robuste Lors de la Transmission sur des Réseaux Publics Ouverts</i> .....	123
	Maintenir un Programme de Gestion des Vulnérabilités .....	132
	<i>Exigence 5 : Protéger Tous les Systèmes et Réseaux Contre les Logiciels Malveillants</i> .....	132
	<i>Exigence 6 : Développer et Maintenir des Systèmes et des Logiciels Sécurisés</i> .....	149
	Mettre en œuvre des Mesures Robustes de Contrôle D'accès .....	179

<i>Exigence 7 : Limiter L'accès aux Composants Système et aux Données des Titulaires de Cartes en Fonction des Besoins de L'entreprise .....</i>	179
<i>Exigence 8 : Identifier les Utilisateurs et Authentifier L'accès aux Composants Système .....</i>	192
<i>Exigence 9 : Limiter L'accès Physique aux Données des Titulaires de Cartes .....</i>	227
Surveiller et Tester Régulièrement les Réseaux .....	251
<i>Exigence 10 : Enregistrer et Surveiller tous les Accès aux Composants Système et aux Données des Titulaires de Cartes .....</i>	251
<i>Exigence 11 : Tester Régulièrement la Sécurité des Systèmes et des Réseaux .....</i>	275
Maintenir une Politique de Sécurité de L'information .....	307
<i>Exigence 12 : Appuyer la Sécurité de l'Information sur des Politiques et des Programmes Organisationnels .....</i>	307
<b>Annexe A Autres Exigences du Standard PCI DSS .....</b>	<b>350</b>
Annexe A1 : Autres Exigences du Standard PCI DSS pour les Prestataires de Services Mutualisés .....	350
Annexe A2 : Autres Exigences du Standard PCI DSS pour les Entités Utilisant SSL et/ou les Versions Obsolètes du Protocole TLS pour les Connexions de Terminaux POS POI Avec Carte .....	356
Annexe A3 : Validation Complémentaire des Entités Désignées (DESV) .....	360
<b>Annexe B Mesures de Sécurité Compensatoires .....</b>	<b>384</b>
<b>Annexe C Fiche D'Identification des Mesures Compensatoires .....</b>	<b>386</b>
<b>Annexe D Approche Personnalisée .....</b>	<b>387</b>
<b>Annexe E Exemples de Modèles pour Soutenir une Approche Personnalisée .....</b>	<b>389</b>
<b>Annexe F Utiliser le Cadre de Sécurité Logicielle PCI pour Répondre à L'exigence 6 .....</b>	<b>390</b>
<b>Annexe G Glossaire des Termes, Abréviations et Acronymes du Standard PCI DSS .....</b>	<b>393</b>

# 1 Introduction et Présentation du Standard de Sécurité des Données PCI

Le standard de sécurité des données Payment Card Industry (PCI DSS) a été développée afin d'encourager et d'améliorer la sécurité des données relatives aux comptes de paiement, et de faciliter l'adoption à grande échelle de mesures cohérentes de sécurité des données à l'échelle mondiale. PCI DSS fournit une base d'exigences techniques et opérationnelles conçues pour protéger les données de carte. Bien que spécifiquement conçue pour se focaliser sur les environnements contenant des données de comptes de paiement, le standard PCI DSS peut également être utilisé pour se protéger contre les menaces et sécuriser d'autres éléments de l'écosystème de paiement.

Le tableau 1 présente les 12 principales exigences du standard PCI DSS.

**Tableau 1. Principales Exigences du Standard PCI DSS**

Standard de Sécurité des Données PCI - Aperçu de Haut Niveau	
<b>Créer et Maintenir un Réseau et des Systèmes Sécurisés</b>	<ol style="list-style-type: none"> <li>1. Installer et Maintenir des Mesures de sécurité de Sécurité du Réseau.</li> <li>2. Appliquer des Configurations Sécurisées à Tous les Composants du Système.</li> </ol>
<b>Protéger les Données de Carte</b>	<ol style="list-style-type: none"> <li>3. Protéger les données de carte pendant leur conservation</li> <li>4. Protéger les Données des Titulaires de Carte Grâce à une Cryptographie Robuste lors de la Transmission sur des Réseaux Publics Ouverts.</li> </ol>
<b>Maintenir un Programme de Gestion des Vulnérabilités</b>	<ol style="list-style-type: none"> <li>5. Protéger Tous les Systèmes et Réseaux Contre les Logiciels Malveillants.</li> <li>6. Développer et Maintenir des Systèmes et des Logiciels Sécurisés.</li> </ol>
<b>Mettre en œuvre des Mesures Robustes de Contrôle D'accès</b>	<ol style="list-style-type: none"> <li>7. Limiter l'Accès aux Composants Système et aux Données des Titulaires de Cartes en Fonction des Besoins de l'Entreprise.</li> <li>8. Identifier les Utilisateurs et Authentifier l'Accès aux Composants Système.</li> <li>9. Limiter l'Accès Physique aux Données des Titulaires des Cartes.</li> </ol>
<b>Surveiller et Tester Régulièrement les Réseaux</b>	<ol style="list-style-type: none"> <li>10. Enregistrer et Surveiller Tous les Accès aux Composants Système et aux Données des Titulaires de Cartes.</li> <li>11. Tester Régulièrement la Sécurité des Systèmes et des Réseaux.</li> </ol>
<b>Maintenir une Politique de Sécurité des Informations</b>	<ol style="list-style-type: none"> <li>12. Renforcer la Sécurité des Informations à l'aide de Politiques et des Programmes Organisationnels.</li> </ol>

Le document « Exigences du standard de sécurité des données de la Payment Card Industry et procédures de test », comprend les 12 exigences principales du standard PCI DSS, les exigences détaillées de sécurité, les procédures de test correspondantes et d'autres informations pertinentes à chaque exigence. Les sections suivantes fournissent des directives détaillées et de bonnes pratiques afin d'aider

les entités à se préparer, à mener et à rapporter les résultats d'une évaluation du standard PCI DSS. Les exigences de PCI DSS et les procédures de test commencent à la page 41.

Le standard PCI DSS comprend un ensemble minimum d'exigences pour la protection des données de carte et peut être amélioré par des mesures de sécurité et des pratiques supplémentaires afin d'atténuer davantage les risques et d'incorporer les lois et réglementations locales, régionales et sectorielles. En outre, la législation ou les exigences réglementaires peuvent exiger une protection spécifique des informations à caractère personnel ou d'autres éléments de données (par ex., le nom du titulaire de la carte).

### ***Limites***

Si l'une des exigences contenues dans cette standard est en conflit avec les lois nationales, étatiques ou locales, la loi nationale, étatique ou locale s'appliquera.

## **Ressources sur le Standard PCI DSS**

Le site Web du Conseil des standards de sécurité PCI (PCI SSC) ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) fournit les ressources supplémentaires suivantes afin d'aider les entreprises dans leurs évaluations et validations du standard PCI DSS :

- Bibliothèque de documents, notamment :
  - PCI DSS Récapitulatif des Modifications
  - Guide de Référence Rapide PCI DSS
  - Compléments D'information et Directives
  - Approche Priorisée pour le Standard PCI DSS
  - Modèle de Rapport et Instructions pour le Rapport sur la Conformité (ROC)
  - Questionnaires D'auto-évaluation (SAQ) et les Instructions et Directives pour les Remplir
  - Attestations de Conformité (AOCs)
- Questions Fréquemment Posées (FAQ)
- PCI pour les sites Web des Petits Commerçants
- Cours de Formation et ébinaires d'information liés à PCI
- Liste des Auditeurs de Sécurité Qualifiés (QSA) et des Prestataires de Services D'investigations Agréés (ASV)
- Listes des périphériques, applications et solutions approuvés par la PCI

Il existe plus de 60 guides et compléments d'informations disponibles sur le site Web du PCI SSC qui fournissent des conseils et des considérations spécifiques pour le standard PCI DSS. Des exemples comportent :

- Des Conseils pour le Cadrage du Périmètre PCI DSS et la Segmentation du Réseau
- Des Directives du PCI SSC sur le Cloud Computing
- Des Conseils sur L'authentification à Plusieurs Facteurs
- Une Assurance de Sécurité de Tiers
- Des Conseils sur la Surveillance Efficace des Journaux Quotidiens
- Des Conseils sur les Tests de Pénétration
- Des Bonnes Pratiques pour la mise en œuvre d'un Programme de Sensibilisation à la Sécurité
- Des Bonnes Pratiques pour Maintenir la Conformité au Standard PCI DSS
- Le Standard PCI DSS pour les Grandes Entreprises
- Des Informations sur L'utilisation de SSL/TLS et Impact sur les Analyses des ASV
- Des Informations sur L'utilisation de SSL/TLS pour les Connexions de Terminaux POS POI
- Des Directives de Sécurité des Produits de Création de "Jetons"
- Des Conseils pour Protéger les Données des Cartes de Paiement par Téléphone

Se reporter à la Bibliothèque de Documents sur le site [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) afin d'obtenir des informations sur ces ressources et d'autres documents complémentaires.

De plus, se reporter à *l'Annexe G* pour les définitions des termes du standard PCI DSS.

**Remarque :** Les Compléments D'informations Complètent le Standard PCI DSS et identifient des considérations et des recommandations supplémentaires pour répondre aux exigences du Standard PCI DSS. Les compléments d'informations n'annulent, ne remplacent ni n'étendent le Standard PCI DSS ou l'une de ses exigences.

## 2 Informations sur les Conditions D'applicabilité du Standard PCI DSS

Le standard PCI DSS est destiné à toutes les entités qui stockent, traitent ou transmettent des données de titulaires de cartes (CHD) et/ou des données d'authentification sensibles (SAD) ou qui pourraient avoir une incidence sur les données des titulaires de cartes et/ou les données d'authentification sensibles. Cela inclut toutes les entités impliquées dans le traitement des données de cartes de paiement, y compris les commerçants, les processeurs, les acquéreurs, les émetteurs et autres prestataires de services.

Le fait qu'une entité soit tenue de se conformer ou de valider sa conformité au standard PCI DSS reste à la discrétion des entreprises qui gèrent les programmes de conformité (telles que les réseaux internationaux et les acquéreurs). Contacter ces entreprises pour tout critère supplémentaire.

### Définition des Données de Carte, des Données de Titulaires de Cartes et des Données D'authentification Sensibles

Les données de titulaires de cartes et les données d'authentification sensibles sont considérées comme des données de carte et sont définies comme suit :

**Tableau 2. Données de carte**

Données de Carte	
Les Données des Titulaires de Cartes Comprennent :	Les Données D'authentification Sensibles Comprennent :
<ul style="list-style-type: none"><li>• Le Numéro de compte primaire (PAN)</li><li>• Le Nom du titulaire de carte</li><li>• La Date d'expiration</li><li>• Le Code de service</li></ul>	<ul style="list-style-type: none"><li>• Les données de piste complète (données de la piste magnétique ou équivalent sur une puce)</li><li>• Le Code de vérification de la carte</li><li>• Les "PINs/PIN blocs"</li></ul>

Les exigences du standard PCI DSS s'appliquent aux entités travaillant sur des environnements dans lesquels les données de carte (données des titulaires de cartes et/ou données d'authentification sensibles (SAD)) sont stockées, traitées ou transmises, et aux entités avec des environnements qui peuvent avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles. Certaines exigences du standard PCI DSS peuvent également s'appliquer aux entités dont les environnements ne stockent, ne traitent ni ne transmettent les données de carte ; par exemple, les entités qui externalisent les opérations de paiement ou la gestion de leur Environnement

de données de titulaires de carte (CDE)<sup>1</sup>. Les entités qui sous-traitent leurs environnements de paiement ou leurs opérations de paiement à des tiers restent responsables de la protection par ledit tiers des données de carte conformément aux exigences applicables du standard PCI DSS.

Le numéro de compte primaire (PAN) est le facteur déterminant pour les données des titulaires de cartes. Le terme « données de carte » couvre donc les éléments suivants : le PAN complet, tout autre élément de données du titulaire de carte présent avec le PAN et tout élément de données d'authentification sensibles.

Si le nom du titulaire de la carte, le code de service et/ou la date d'expiration sont stockés, traités ou transmis avec le PAN, ou sont autrement présents dans le CDE, ils doivent être protégés conformément aux exigences du standard PCI DSS applicables aux données du titulaire de carte.

Si une entité stocke, traite ou transmet le PAN, il existe alors un CDE auquel les exigences du standard PCI DSS s'appliqueront. Il se peut que certaines exigences ne puissent pas être applicables ; par exemple, si l'entité ne stocke pas le PAN, alors les exigences relatives à la protection du PAN stocké, dans l'exigence 3, ne seront pas applicables à l'entité.

Même si une entité ne stocke, ne traite ou ne transmet pas de PAN, certaines exigences du standard PCI DSS peuvent toujours s'appliquer. Prendre en compte les éléments suivants :

- Si l'entité stocke les SAD, les exigences spécifiquement liées au stockage des SAD dans l'Exigence 3 seront applicables.
- Si l'entité engage des prestataires de services tiers pour stocker, traiter ou transmettre le PAN en son nom, les exigences relatives à la gestion des prestataires de services de l'exigence 12 seront applicables.
- Si l'entité peut avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles car la sécurité de l'infrastructure d'une entité peut avoir une incidence sur la façon dont les données du titulaire de carte sont traitées (par exemple, via un serveur Web qui contrôle la génération d'un formulaire ou d'une page de paiement), certaines exigences seront applicables.
- Si les données du titulaire de carte ne sont présentes que sur des supports physiques (par exemple, du papier), les exigences relatives à la sécurité et à l'élimination des supports physiques de l'Exigence 9 seront applicables.
- Les exigences relatives à un plan de réponse aux incidents sont applicables à toutes les entités, afin de garantir l'existence de procédures à suivre en cas de violation présumée ou avérée de la confidentialité des données du titulaire de carte.

---

<sup>1</sup> Conformément à ces entreprises qui gèrent les programmes de conformité (telles que les réseaux internationaux et les acquéreurs) ; les entités doivent contacter ces entreprises pour plus de détails.

## ***Utilisation des Données de Carte, Données D'authentification Sensibles, Données du Titulaire de Carte et Numéro de Compte Principal dans le Standard PCI DSS***

PCI DSS comporte des exigences qui font spécifiquement référence aux données de carte, aux données du titulaire de carte et aux données d'authentification sensibles. Il est important de noter que chacun de ces types de données est différent et que les termes ne sont pas interchangeables. Les références spécifiques dans les exigences relatives aux données de carte, aux données de titulaire de carte ou aux données d'authentification sensibles sont utiles, et lesdites exigences s'appliquent spécifiquement au type de données référencées.

## Éléments de Données de Carte et Exigences Relatives au Stockage

Le tableau 3 identifie les éléments des données de titulaire de carte et des données d'authentification sensibles, si le stockage de chaque élément de données est autorisé ou interdit, et si chaque élément de données doit être rendu illisible (par exemple, avec une cryptographie robuste) lorsqu'il est stocké. Ce tableau n'est pas exhaustif et est présenté uniquement aux fins d'illustrer la manière dont les exigences énoncées s'appliquent aux différents éléments de données.

**Tableau 3. Exigences Relatives au Stockage des Éléments de Données de Carte**

		Élément de Données	Restrictions Concernant le Stockage	Requises pour Rendre les Données Stockées Illisibles
Données de Carte	Données Relatives au Titulaire de Carte	Le numéro de compte primaire (PAN)	Le stockage est réduit au minimum tel que défini dans l'exigence 3.2	Oui, tel que défini dans l'exigence 3.5
		Le nom du titulaire de carte		
		Le code de service	Le stockage est réduit au minimum tel que défini dans l'exigence 3.2 <sup>2</sup>	Non
		La date d'expiration		
	Données D'authentification Sensibles	Les données de suivi complet	Ne peuvent pas être stockées après autorisation tel que défini dans l'exigence 3.3.1 <sup>3</sup>	Oui, les données stockées jusqu'à ce que l'autorisation soit terminée doivent être protégées par une cryptographie robuste tel que défini dans l'exigence 3.3.2
	Le code de vérification de la carte			
	Le bloc PIN/PIN			

Si le PAN est stocké avec d'autres éléments des données du titulaire de carte, seul le PAN doit être rendu illisible conformément à l'exigence 3.5.1 du standard PCI DSS.

Les données d'authentification sensibles ne doivent pas être stockées après autorisation, même si elles sont chiffrées. Cela s'applique même pour les environnements où il n'y a pas de PAN présent.

<sup>2</sup> Où les données existent dans le même environnement que le PAN.

<sup>3</sup> Sauf autorisation pour les émetteurs et les entreprises qui prennent en charge les services d'émission. Les exigences pour les émetteurs et les services d'émission sont définies séparément dans l'exigence 3.3.3.

### 3 Relation entre les Standards Logiciels PCI DSS et PCI SSC

Le standard PCI SSC prend en charge l'utilisation de logiciels de paiement sécurisés dans les environnements de données des titulaires de carte (CDE) via le cadre de logiciel de sécurité (SSF), qui se compose du standard de logiciel sécurisé et du cycle de vie du logiciel sécurisé (Secure SLC). Un logiciel qui est validé et répertorié selon le standard PCI SSC fournit l'assurance que le logiciel a été développé en utilisant des pratiques sécurisées et a satisfait à un ensemble défini d'exigences en termes de sécurité logicielle.

Les programmes logiciels sécurisés conformément au standard PCI SSC comportent des listes de logiciels de paiement et de fournisseurs de logiciels qui ont été validés comme répondant aux standards logiciels applicables du standard PCI SSC.

- Logiciel Validé** : Les Logiciels de Paiement Répertoriés sur le site Web PCI SSC en tant qu'application de Paiement Validée (PA-DSS) ou Logiciels de Paiement Validés (le Standard des Logiciels Sécurisés) ont été analysés par un auditeur qualifié pour confirmer que lesdits logiciels répondent aux exigences de sécurité de ce standard. Les exigences de sécurité de ces standards sont axées sur la protection de l'intégrité et de la confidentialité des transactions de paiement et des données de carte.
- Fournisseurs de Logiciels Qualifiés** : Le Standard Secure SLC définit les exigences de sécurité pour les fournisseurs de logiciels afin qu'ils intègrent des pratiques de développement de logiciels sécurisés tout au long du cycle de vie desdits logiciels. Les fournisseurs de logiciels qui ont été validés comme répondant à le standard Secure SLC sont répertoriés sur le site Web du standard PCI SSC en tant que fournisseur Qualifié Secure SLC.

Pour plus d'informations sur le SSF ou la PA-DSS, reportez-vous aux guides des programmes respectifs sur [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

Tous les logiciels qui stockent, traitent ou transmettent des données de carte, ou qui pourraient avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles, font partie du champ d'application de l'évaluation du standard PCI DSS d'une entité. Bien que l'utilisation d'un logiciel de paiement approuvé prenne en charge la sécurité du CDE d'une entité, l'utilisation d'un tel logiciel ne rend pas en soi une entité conforme au standard PCI DSS. L'évaluation du standard PCI DSS par l'entité doit inclure la vérification que le logiciel est correctement configuré et mis en œuvre en toute sécurité pour prendre en charge les exigences applicables du standard PCI DSS. De plus, si le logiciel de paiement classé PCI a été personnalisé, un examen plus approfondi sera nécessaire lors de l'évaluation du standard PCI DSS, car le logiciel peut ne plus être représentatif de la version initialement validée.

Étant donné que les menaces de sécurité évoluent constamment, les logiciels qui ne sont plus pris en charge par le fournisseur (par exemple, identifiés par le fournisseur comme « en fin de vie ») peuvent ne pas offrir le même niveau de sécurité que les versions prises en charge. Les entités sont fortement encouragées à maintenir leur logiciel actuel et à jour avec les dernières versions du logiciel disponibles.

**Remarque :** Le standard PA-DSS et le programme connexe ont été retirés en octobre 2022. Reportez-vous à la liste des applications de paiement validées du standard PCI SSC pour connaître les dates d'expiration des applications validées par le standard PA-DSS. Depuis la date d'expiration, les applications seront répertoriées comme « acceptables uniquement pour les déploiements préexistants ». La possibilité pour une entité de continuer à utiliser une application conforme au standard PA-DSS avec une liste expirée est à la discréTION des entreprises qui gèrent les programmes de conformité (telles que les réseaux internationaux et les acquéreurs) ; les entités doivent contacter ces entreprises pour plus de détails.

Les entités qui développent leur propre logiciel sont encouragées à se reporter aux standards de sécurité logicielle du PCI SSC et à prendre en compte les exigences qu'elles contiennent comme de meilleures pratiques à utiliser dans leurs environnements de développement. Un logiciel de paiement sécurisé mis en œuvre dans un environnement conforme au standard PCI DSS aidera à minimiser la possibilité de failles de sécurité conduisant à des compromissions des données de carte et à des fraudes. Voir [Logiciels sur Mesure et Personnalisés](#).

## Applicabilité du Standard PCI DSS aux Fournisseurs de Logiciels de Paiement

Le standard PCI DSS peut s'appliquer à un fournisseur de logiciels de paiement si le fournisseur est également un prestataire de services qui stocke, traite ou transmet des données de carte, ou a accès aux données de carte de ses clients ; par exemple, dans le rôle d'un prestataire de services de paiement ou via accès à distance à un environnement consommateur. Les fournisseurs de logiciels auxquels le standard PCI DSS peut s'appliquer incluent ceux qui proposent des services de paiement, ainsi que les fournisseurs de services cloud proposant des terminaux de paiement dans le cloud, des logiciels en tant que service (SaaS), le commerce électronique dans le cloud et d'autres services de paiement via le cloud.

## Logiciels sur Mesure et Personnalisés

Tous les logiciels sur mesure et personnalisés qui stockent, traitent ou transmettent des données de carte, ou qui pourraient avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles, font partie du champ d'application de l'évaluation du standard PCI DSS d'une entité.

Les logiciels sur mesure et personnalisés qui n'ont pas été développés et maintenus conformément à l'un des standards du cadre de sécurité logicielle du PCI SSC (le standard logiciel sécurisé ou le standard SLC sécurisé) aidera une entité à répondre à l'exigence 6 du standard PCI DSS.

Voir [Annexe F](#) pour plus de détails.

**Remarque :** L'exigence 6 du standard PCI DSS s'applique pleinement aux logiciels sur mesure et personnalisés qui n'ont pas été développés et maintenus conformément à l'une des standards du cadre de sécurité logicielle du PCI SSC. Les entités qui utilisent des fournisseurs de logiciels pour développer des logiciels sur mesure ou personnalisés qui pourraient avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles sont responsables de s'assurer que ces fournisseurs de logiciels développent le logiciel conformément à l'exigence 6 du standard PCI DSS.

## 4 Périmètre des Exigences du Standard PCI DSS

Les exigences du standard PCI DSS s'appliquent :

- À l'environnement de données des titulaires de cartes (CDE), qui comprend :
  - Aux composants du système, aux personnes et aux processus qui stockent, ou traitent et transmettent les données de titulaires de cartes et/ou des données d'authentification sensibles, et
  - Aux composants du système qui ne peuvent pas stocker, traiter ou transmettre des CHD/SAD mais qui ont une connectivité illimitée aux composants système qui stockent, traitent ou transmettent les CHD/SAD.

ET

- Aux composants du système, aux personnes et aux processus susceptibles d'avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles.<sup>4</sup>

Les « composants système » comprennent les périphériques réseau, les serveurs, les périphériques informatiques, les composants virtuels, les composants cloud et les logiciels. Des exemples de composants système comportent, sans toutefois s'y limiter :

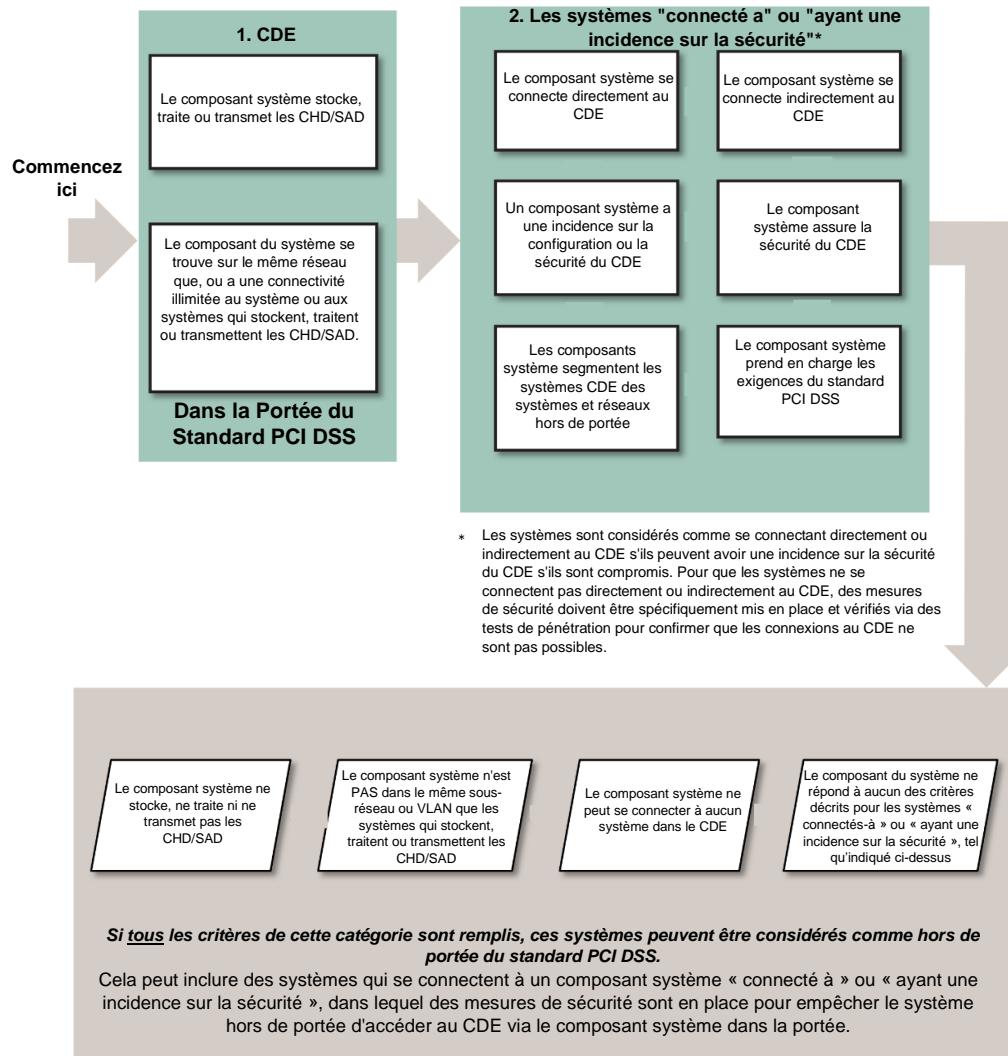
- Les systèmes qui stockent, traitent ou transmettent des données de carte (par exemple, les terminaux de paiement, les systèmes d'autorisation, les systèmes de compensation, les systèmes middleware de paiement, les systèmes back-office de paiement, les paniers d'achat et les vitrines de magasins, les systèmes de passerelles/commutation de paiement, les systèmes de surveillance de la fraude).
- Les systèmes qui fournissent des services de sécurité (par exemple, serveurs d'authentification, serveurs de contrôle d'accès, systèmes de gestion des informations et des événements de sécurité (SIEM), systèmes de sécurité physique (par exemple, accès par badge ou vidéosurveillance), systèmes d'authentification à plusieurs facteurs, systèmes contre les logiciels malveillants).
- Les systèmes qui facilitent la segmentation (par exemple, les mesures de sécurité de sécurité du réseau interne).
- Les systèmes susceptibles d'avoir un impact sur la sécurité des données de carte ou du CDE (par exemple, la résolution de noms ou les serveurs de redirection (web) de commerce électronique).
- Les composants de virtualisation tels que les machines virtuelles, les commutateurs/routeurs virtuels, les appareils virtuels, les applications/bureaux virtuels et les hyperviseurs.

<sup>4</sup> Pour plus d'informations, reportez-vous au *Complément d'informations : Conseils pour le cadrage du standard PCI DSS et la segmentation du réseau* sur le site Web du PCI SSC.

- Les infrastructures et composants cloud, à la fois externes et sur place, et comprenant des instantiations de conteneurs ou d'images ; les clouds privés virtuels, la gestion des identités et des accès dans le cloud, le CDE sur place ou dans le cloud, des services maillés avec des applications conteneurisées et des outils d'orchestration de conteneurs.
- Les composants réseau, y compris, sans toutefois s'y limiter, les mesures de sécurité de sécurité réseau, les commutateurs, les routeurs, les périphériques réseau VoIP, les points d'accès sans fil, les appareils réseau et autres appareils de sécurité.
- Les types de serveur, y compris, sans toutefois s'y limiter, Web, d'applications, de bases de données, d'authentification, de courrier, proxy, protocole de synchronisation réseau (NTP) et système de noms de domaine (DNS).
- Les appareils des utilisateurs finaux, tels que les ordinateurs, les ordinateurs portables, les postes de travail, les postes de travail administratifs, les tablettes et les appareils mobiles.
- Les imprimantes et les périphériques multifonctions qui numérisent, impriment et télécopient.
- Le stockage des données de carte dans n'importe quel format (par exemple, papier, fichiers de données, fichiers audios, images et enregistrements vidéo).
- Les applications, les logiciels et composants logiciels, les applications sans serveur, y compris tous les logiciels achetés, souscrits (par exemple, Logiciel en tant que service), sur mesure et personnalisés, y compris les applications internes et externes (par exemple, Internet).
- Les outils, les référentiels de code et les systèmes qui implémentent la gestion de la configuration logicielle ou pour le déploiement d'objets au CDE ou sur des systèmes pouvant avoir un impact sur le CDE.

La figure 1 montre les considérations relatives à la définition du périmètre des composants système pour le standard PCI DSS.

**Figure 1. Comprendre le Périmètre du Standard PCI DSS**



## Confirmation Annuelle du Périmètre PCI DSS

Pour l'entité, la première étape de la préparation d'une évaluation du standard PCI DSS consiste à déterminer avec précision le périmètre de l'évaluation. L'entité évaluée doit confirmer l'exactitude du périmètre qu'elle souhaite appliquer au standard PCI DSS conformément à l'exigence du standard PCI DSS 12.5.2 en identifiant tous les emplacements et flux de données de carte, et en identifiant tous les systèmes qui sont connectés ou, s'ils sont compromis, pourraient avoir une incidence sur le CDE (par exemple, serveurs d'authentification, serveurs d'accès distant, serveurs de journalisation) afin de s'assurer qu'ils sont inclus dans le périmètre du standard PCI DSS. Tous les types de systèmes et d'emplacements doivent être pris en compte lors du processus de définition du périmètre, y compris les sites de sauvegarde/restauration et les systèmes de basculement.

Les étapes minimales pour qu'une entité confirme l'exactitude du périmètre PCI DSS de son environnement sont spécifiées dans l'exigence 12.5.2 du standard PCI DSS. L'entité est censée conserver la documentation pour montrer la façon dont le périmètre du standard PCI DSS a été déterminée. La documentation est conservée pour examen par l'auditeur et pour référence lors de la prochaine activité de confirmation du périmètre du standard PCI DSS de l'entité. Pour chaque évaluation du standard PCI DSS, l'auditeur valide que l'entité a défini et documenté avec précision le périmètre de l'évaluation.

**Remarque :** *Cette confirmation annuelle de son périmètre PCI DSS est définie dans l'exigence 12.5.2 du standard PCI DSS et est une activité qui doit être exécutée par l'entité. Cette activité n'est pas la même, ni destinée à être remplacée par la confirmation de périmètre effectuée par l'auditeur de l'entité lors de l'évaluation.*

## Segmentation

La segmentation (ou l'isolement) du CDE du reste du réseau d'une entité n'est pas une exigence du standard PCI DSS. Cependant, elle est fortement recommandée comme méthode qui peut réduire :

- Le périmètre de l'évaluation du standard PCI DSS
- Le coût de l'évaluation du standard PCI DSS
- Le coût et la difficulté de la mise en œuvre et de la maintenance des mesures de sécurité du standard PCI DSS
- Le risque pour une entreprise lié aux données de compte de paiement (réduit en consolidant ces données dans des emplacements moins nombreux et mieux contrôlés)

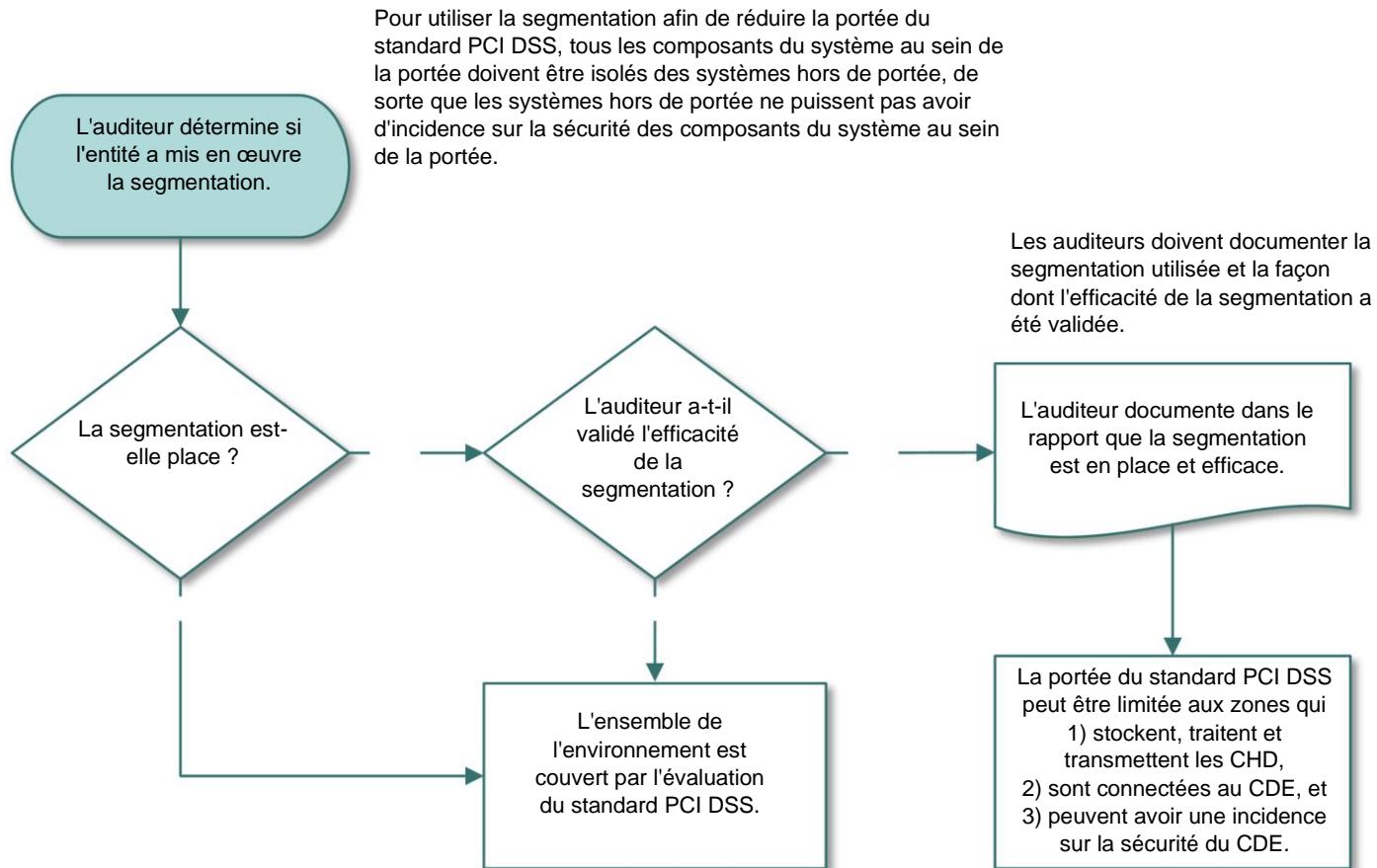
Sans segmentation adéquate (parfois appelée « réseau à plat »), l'ensemble du réseau est couvert par l'évaluation du standard PCI DSS. La segmentation peut être réalisée à l'aide d'un certain nombre de méthodes physiques ou logiques, telles que des mesures de sécurité de réseau internes adéquatement configurés, des routeurs dotés de listes de contrôle d'accès robustes ou d'autres technologies qui limitent l'accès à un segment particulier d'un réseau. Pour être considéré comme hors du périmètre PCI DSS, un composant système doit être correctement segmenté (isolé) du CDE, de telle sorte que le composant système hors du périmètre ne puisse pas avoir d'impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensible, même si ce composant a été compromis.

Une condition préalable importante pour réduire le périmètre du CDE est une compréhension claire des besoins et des processus commerciaux liés au stockage, au traitement et à la transmission des données de carte. Limiter les données de carte a aussi peu d'emplacements que possible en éliminant les données inutiles et en consolidant les données nécessaires peut nécessiter une réingénierie des pratiques commerciales de longue date.

La documentation des flux de données de carte via un diagramme de flux de données aide une entité à comprendre parfaitement comment les données de carte arrivent dans une entreprise, où elles résident au sein de l'entreprise et comment elles traversent divers systèmes au sein de l'entreprise. Les diagrammes de flux de données illustrent également tous les emplacements dans lesquels les données de carte sont stockées, traitées et transmises. Ces informations soutiennent une entité mettant en œuvre la segmentation et peuvent également aider à la confirmer que la segmentation est utilisée pour isoler le CDE des réseaux hors du périmètre.

Si la segmentation est utilisée pour réduire le périmètre de l'évaluation du standard PCI DSS, l'auditeur doit vérifier que la segmentation est adéquate pour réduire le périmètre de l'évaluation, comme illustré à la figure 2. À un niveau élevé, une segmentation adéquate isole les systèmes qui stockent, traitent ou transmettent des données de carte de ceux qui ne le font pas. Cependant, l'adéquation de la mise en œuvre d'une segmentation spécifique est très variable et dépend de plusieurs facteurs tels que la configuration d'un réseau donné, les technologies déployées et d'autres mesures de sécurité qui peuvent être mis en œuvre.

**Figure 2. Segmentation et Impact sur le Périmètre du Standard PCI DSS**



## Technologie sans Fil

Si la technologie sans fil est utilisée pour stocker, traiter ou transmettre des données de carte (par exemple, des dispositifs de point de vente sans fil), ou si un réseau local sans fil (WLAN) fait partie ou est connectée au CDE, les exigences du standard PCI DSS et les procédures de test pour sécuriser les environnements sans fil s'appliquent et doivent être effectuées.

La détection d'accès sans fil non autorisé doit être effectuée conformément à l'exigence 11.2.1 du standard PCI DSS même lorsque la technologie sans fil n'est pas utilisée dans le CDE et que l'entité a une politique qui interdit l'utilisation de la technologie sans fil dans son environnement. Cela est dû à la facilité avec laquelle un point d'accès sans fil peut être connecté à un réseau, à la difficulté de détecter sa présence et au risque accru présenté par les appareils sans fil non autorisés.

Avant la mise en œuvre de la technologie sans fil, une entité doit soigneusement évaluer le besoin de la technologie par rapport au risque. Envisagez de déployer la technologie sans fil uniquement pour la transmission de données non sensibles.

## Lorsque des Données de Titulaires de Carte et/ou des Données d'Authentification Sensibles sont Accidentallement Reçues Via un Canal Imprévu

Il peut arriver qu'une entité reçoive des données de titulaire de carte et/ou des données d'authentification sensibles non sollicitées via un canal de communication non sécurisé qui n'était pas destiné à recevoir des données sensibles. Dans ce cas, l'entité peut choisir de :

- Inclure le canal dans le périmètre de leur CDE et le sécuriser selon la norme PCI DSS

Ou

- Supprimer les données en toute sécurité et mettre en œuvre des mesures pour empêcher que le canal ne soit utilisé à l'avenir pour l'envoi de ces données.

## Données Chiffrées des Titulaires de Carte et Impact sur le Périmètre du Standard PCI DSS

Le chiffrement des données des titulaires de carte avec une cryptographie robuste est une méthode acceptable pour rendre les données illisibles conformément à l'exigence 3.5 du standard PCI DSS. Cependant, le chiffrement seul est généralement insuffisant pour rendre les données des titulaires de cartes hors de périmètre du standard PCI DSS et n'élimine pas le besoin du standard PCI DSS dans cet environnement. L'environnement de l'entité est toujours dans le champ d'application du standard PCI DSS en raison de la présence de données des titulaires de cartes. Par exemple, pour un environnement de cartes de commerçants, il existe un accès physique aux cartes de paiement pour effectuer une transaction et il peut également y avoir des rapports ou des reçus papier portant les données du titulaire de la carte. De même, dans les environnements sans cartes de commerçants, tels que la vente par correspondance/commande téléphonique et le commerce électronique, les détails de la carte de paiement sont fournis via des canaux qui doivent être évalués et protégés conformément au standard PCI DSS.

Les éléments suivants se trouvent chacun dans le périmètre du standard PCI DSS :

- Les systèmes effectuant le chiffrement et/ou le déchiffrement des données des titulaires de cartes, et les systèmes effectuant des fonctions de gestion des clés,
- Les données chiffrées des titulaires de cartes qui ne sont pas isolées des processus de chiffrement et déchiffrement et de la gestion des clés,
- Les données chiffrées des titulaires de cartes présentes sur un système ou un support contenant également la clé de déchiffrement,
- Les données chiffrées des titulaires de cartes présentes dans le même environnement que la clé de déchiffrement,
- Les données de titulaires de cartes chiffrées accessibles à une entité qui a également accès à la clé de déchiffrement.

**Remarque :** Une solution de chiffrement de bout en bout (P2PE) répertoriée PCI peut réduire considérablement le nombre d'exigences du standard PCI DSS applicables à l'environnement de données des titulaires de cartes d'un commerçant. Cependant, elle n'élimine pas complètement l'applicabilité du standard PCI DSS dans l'environnement du commerçant.

## Données Chiffrées des Titulaires de Cartes et Impact sur le Périmètre du Standard PCI DSS pour les Prestataires de Services Tiers

Lorsqu'un prestataire de services tiers (TPSP) reçoit et/ou stocke uniquement des données chiffrées par une autre entité, et lorsqu'il n'a pas la capacité de déchiffrer les données, le TPSP peut être en mesure de considérer les données chiffrées comme hors du périmètre si certaines conditions sont réunies. En effet, la responsabilité des données incombe généralement à l'entité, ou aux entités, avec la possibilité de déchiffrer les données ou d'avoir une incidence sur la sécurité des données chiffrées. Déterminer quelle partie est responsable des mesures de sécurité spécifiques du standard PCI DSS dépendra de plusieurs facteurs, notamment qui a accès aux clés de déchiffrement, le rôle joué par chaque partie et l'accord entre les parties. Les responsabilités doivent être clairement définies et documentées afin de garantir que le TPSP et l'entité fournissant les données chiffrées comprennent quelle entité est responsable de quelles mesures de sécurité de sécurité.

À titre d'exemple, un TPSP fournissant des services de stockage reçoit et stocke les données chiffrées des titulaires de cartes, fournies par les clients à des fins de sauvegarde. Ce TPSP n'a pas accès aux clés de chiffrement ou de déchiffrement, et n'effectue aucune gestion des clés pour ses clients. Le TPSP peut exclure de telles données chiffrées lors de la détermination du périmètre de sa standard PCI DSS. Cependant, le TPSP conserve la responsabilité de contrôler l'accès au stockage des données chiffrées dans le cadre de ses contrats de service avec ses clients.

La responsabilité de s'assurer que les données chiffrées et les clés cryptographiques sont protégées conformément aux exigences applicables du standard PCI DSS est souvent partagée entre les entités. Dans l'exemple ci-dessus, le consommateur détermine quels membres de son personnel sont autorisés à accéder au support de stockage, et l'installation de stockage est responsable de la gestion des mesures de sécurité d'accès physiques et/ou logiques afin de garantir que seules les personnes autorisées par le consommateur ont accès aux supports de stockage. Les exigences spécifiques du standard PCI DSS applicables à un TPSP dépendront des services fournis et de l'accord entre les deux parties. Dans l'exemple d'un TPSP fournissant des services de stockage, les mesures de sécurité d'accès physiques et logiques fournis par le TPSP devront être évalués au moins une fois par an. Cette évaluation pourrait être effectuée dans le cadre de

l'évaluation du standard PCI DSS du commerçant ou, alternativement, l'évaluation pourrait être effectuée et les mesures de sécurité validée par le TPSP avec les preuves appropriées fournies au commerçant. Pour plus d'informations sur les « preuves appropriées », consultez [Options pour les TPSP de valider la conformité au standard PCI DSS pour les services des TPSP qui répondent aux exigences du standard PCI DSS des clients](#).

Autre exemple, un TPSP qui ne reçoit que des données chiffrées de titulaires de cartes à des fins de routage vers d'autres entités, et qui n'a pas accès aux données ou aux clés cryptographiques, peut n'avoir aucune responsabilité PCI DSS pour ces données chiffrées. Dans ce scénario, lorsque le TPSP ne fournit aucun service de sécurité ou contrôle d'accès, il peut être considéré comme un réseau public ou non fiable, et il incomberait à l'entité ou aux entités qui envoient ou reçoivent des données de carte via le réseau pour s'assurer que les mesures de sécurité du standard PCI DSS sont appliquées afin de protéger les données transmises.

## Utilisation de Prestataires de Services Tiers

Une entité (appelée « consommateur » dans cette section) peut choisir d'utiliser un prestataire de services tiers (TPSP) pour stocker, traiter ou transmettre des données de carte ou pour gérer les composants systèmes concernés au nom du consommateur. L'utilisation d'un TPSP peut avoir une incidence sur la sécurité du CDE d'un consommateur.

**Remarque :** *L'utilisation d'un TPSP conforme au standard PCI DSS ne rend pas un consommateur conforme au standard PCI DSS et n'élimine pas la responsabilité du consommateur quant à sa propre conformité au standard PCI DSS. Même si un consommateur utilise un TPSP, ledit consommateur reste responsable de la confirmation de sa propre conformité, comme le demandent les entreprises qui gèrent les programmes de conformité (par exemple, les réseaux internationaux et les acquéreurs). Les clients doivent contacter ces entreprises pour toute exigence.*

## Utilisation des Prestataires de Services Internet et Impact sur les Clients Répondant à L'exigence 12.8 du Standard PCI DSS

Il existe de nombreux scénarios différents dans lesquels un consommateur peut utiliser un ou plusieurs TPSP pour des fonctions au sein de, ou liées au CDE du consommateur. Dans tous les scénarios où un TPSP est utilisé, le consommateur doit gérer et superviser toutes ses relations avec le TPSP et surveiller le statut de conformité au standard PCI DSS de ses TPSP conformément à l'exigence 12.8, y compris les TPSP qui :

- Ont accès au CDE du consommateur,
- Gèrent les composants système dans le périmètre au nom du consommateur, et/ou
- Peuvent avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles du consommateur.

La gestion des relations avec le TPSP conformément à l'exigence 12.8 comprend l'exercice d'une diligence raisonnable, la mise en place d'accords appropriés, l'identification des exigences qui s'appliquent au consommateur et celles qui s'appliquent au TPSP, et le suivi de l'état de conformité des TPSP au moins une fois par an.

L'exigence 12.8 ne précise pas que les TPSP du consommateur doivent être conformes au standard PCI DSS, mais uniquement que le consommateur surveille l'état de sa conformité comme spécifié dans l'exigence. Par conséquent, les TPSP n'ont pas besoin d'être conformes au standard PCI DSS pour que leur consommateur réponde à l'exigence 12.8.

### ***Impact de L'utilisation de TPSP pour des Services qui Répondent aux Exigences du Standard PCI DSS des Clients***

Lorsque le TPSP fournit un service qui répond à une ou plusieurs exigences du standard PCI DSS au nom du consommateur ou lorsque ce service peut avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles du consommateur, alors ces exigences sont dans le périmètre de l'évaluation du consommateur et la conformité de ce service aura un impact sur la conformité au standard PCI DSS du consommateur. Le TPSP doit démontrer qu'il satisfait aux exigences applicables du standard PCI DSS pour que ces exigences soient en place pour ses clients. Par exemple, si une entité engage un TPSP pour gérer ses mesures de sécurité de sécurité réseau et que le TPSP ne fournit pas la preuve qu'il répond aux exigences applicables de l'exigence 1 du standard PCI DSS, alors ces exigences ne sont pas en place pour l'évaluation du consommateur. Autre exemple, les TPSP qui stockent des sauvegardes des données des titulaires de cartes au nom des clients devraient satisfaire aux exigences applicables liées aux mesures de sécurité d'accès, à la sécurité physique, etc., afin que leurs clients prennent en compte ces exigences en place pour leurs évaluations.

### ***Importance de Comprendre les Responsabilités entre les Clients des TPSP et les TPSP***

Lorsqu'un fournisseur de services de transfert de services fournit un service qui répond à une ou plusieurs exigences PCI DSS au nom du client ou lorsque ce service peut avoir un impact sur la sécurité des données du titulaire de carte et/ou des données d'authentification sensibles du client, il est important que les clients et les TPSP identifient clairement et comprennent les éléments suivants :

- Les services et composants du système inclus dans le périmètre de l'évaluation du standard PCI DSS du TPSP,
- Les exigences et sous-exigences spécifiques du standard PCI DSS couvertes par l'évaluation du standard PCI DSS du TPSP,
- Toutes les exigences qu'il incombe aux clients du TPSP d'inclure dans leurs propres évaluations du standard PCI DSS, et
- Toute exigence du standard PCI DSS dont la responsabilité est partagée entre le TPSP et ses clients.

Par exemple, un prestataire de services cloud doit clairement définir les adresses IP qui sont analysées dans le cadre de son processus trimestriel d'analyse des vulnérabilités, et les adresses IP qu'il incombe à ses clients d'analyser.

Conformément à l'exigence 12.9.2, les TPSP sont tenus de répondre aux demandes d'informations de leurs clients concernant l'état de conformité au standard PCI DSS du TPSP lié aux services fournis aux clients, et concernant les exigences du standard PCI DSS qui relèvent de la responsabilité du TPSP, lesquelles sont de la responsabilité du consommateur, et toutes les responsabilités partagées entre le

consommateur et le TPSP. Reportez-vous au document *Supplément d'information : Assurance de la sécurité par un tiers* pour un exemple de modèle de matrice de responsabilité qui peut être utilisé pour documenter et clarifier la façon dont les responsabilités sont partagées entre les TPSP et les clients.

*Toutes les relations avec les TPSP n'exigent pas que les TPSP fournissent aux clients une documentation sur la manière dont les responsabilités sont partagées entre les TPSP et les clients. Le TPSP n'est obligé de partager cette documentation que si ledit TPSP satisfait une ou plusieurs exigences PCI DSS au nom du client, si la responsabilité de satisfaire une exigence PCI DSS est partagée entre le TPSP et son client, ou si le service du TPSP peut avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles. Alors qu'un TPSP peut ne pas être obligé de fournir cette documentation à ses clients car il n'existe aucune responsabilité partagée, le TPSP doit toujours assister ses clients en leur fournissant aux clients les informations relatives à leur statut de conformité PCI DSS, afin que les clients puissent gérer et surveiller leurs TPSP conformément à l'Exigence 12.8 du PCI DSS.*

## **Options pour les TPSP de Valider la Conformité au Standard PCI DSS pour les Services des TPSP qui Répondent aux Exigences du Standard PCI DSS des Clients**

Les TPSP sont tenus de démontrer leur conformité au standard PCI DSS, comme demandé par les entreprises qui gèrent les programmes de conformité (par exemple, les réseaux internationaux et les acquéreurs). Les TPSP doivent contacter ces entreprises pour toute exigence.

Lorsqu'un TPSP fournit des services destinés à satisfaire aux, ou à faciliter le respect des exigences du standard PCI DSS d'un consommateur ou qui peuvent avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles d'un consommateur, ces exigences entrent dans le périmètre de l'audit du standard PCI DSS du consommateur. Dans ce scénario, les TPSP disposent de deux options pour valider la conformité :

- **Évaluation annuelle** : Le TPSP est soumis à une ou plusieurs évaluations annuelles du standard PCI DSS et fournit à ses clients des preuves démontrant que le TPSP répond aux exigences applicables du standard PCI DSS ; ou
- **Plusieurs évaluations à la demande** : Si un TPSP ne subit pas d'évaluation annuelle du standard PCI DSS, il doit subir des évaluations à la demande de ses clients et/ou participer à chacune des évaluations du standard PCI DSS de ses clients, les résultats de chaque examen étant fournis au ou aux clients respectifs.

Si le TPSP subit son propre audit du standard PCI DSS, il est censé fournir des preuves suffisantes à ses clients afin de vérifier que le périmètre de l'évaluation du standard PCI DSS du TPSP a couvert les services applicables au consommateur, et les exigences PCI DSS pertinentes ont été examinées et qu'il a été confirmé qu'elles sont en place. Si le fournisseur dispose d'une Attestation de Conformité (AOC) au standard PCI DSS, il est prévu que le TPSP fournis l'AOC aux clients à leur demande. Le consommateur peut également demander les sections pertinentes du Rapport sur la conformité (ROC) du TPSP. Le ROC peut être caviardé afin de protéger toute information confidentielle.

Si le TPSP n'audite pas sa propre standard PCI DSS et n'a donc pas d'AOC, le TPSP est censé fournir des preuves spécifiques liées aux exigences applicables du standard PCI DSS, de sorte que le consommateur (ou son auditeur) soit en mesure de confirmer que le TPSP satisfait aux exigences de sa standard PCI DSS.

## **La présence sur une Liste de Réseaux Internationaux de Prestataires de Services Conformes au Standard PCI DSS**

Pour un consommateur qui suit l'état de conformité d'un TPSP conformément à l'exigence 12.8, la présence du TPSP sur la liste d'une marque de paiement de prestataires de services conformes au standard PCI DSS **peut être une preuve suffisante** de l'état de conformité du TPSP s'il ressort clairement de la liste que les services applicables au consommateur ont été couverts par l'évaluation du standard PCI DSS du TPSP. Si cela n'est pas clair sur la liste, le consommateur doit obtenir une autre confirmation écrite qui traite de l'état de conformité au standard PCI DSS du TPSP.

Pour un consommateur qui recherche des preuves de conformité au standard PCI DSS pour les exigences auxquelles un TPSP satisfait au nom d'un consommateur, ou lorsque le service fourni peut avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles du consommateur, la présence du TPSP sur la liste d'une marque de paiement de prestataires de services conformes au standard PCI DSS **n'est pas une preuve suffisante** que les exigences applicables du standard PCI DSS pour ce TPSP ont été incluses dans l'évaluation. Si le TPSP dispose d'une AOC au standard PCI DSS, il est censé le fournir aux clients à leur demande.

## 5 Bonnes Pratiques pour la mise en œuvre du Standard PCI DSS dans les Processus des Affaires Courantes (Business-as-Usual ou « BAU »)

Une entité qui met en œuvre des processus BAU dans le cadre de sa stratégie de sécurité globale prend des mesures afin de garantir que les mesures de sécurité de sécurité mises en œuvre pour sécuriser les données et un environnement continuent d'être correctement mis en œuvre et fonctionnant correctement en tant que cours normal des affaires.

Certaines exigences du standard PCI DSS sont destinées à agir comme des processus BAU en surveillant les mesures de sécurité de sécurité afin de garantir leur efficacité en permanence. Cette supervision par l'entité contribue à fournir une assurance raisonnable que la conformité de son environnement est préservée entre les évaluations du standard PCI DSS. Bien qu'il existe actuellement des exigences BAU définies dans le standard, une entité doit adopter des processus BAU supplémentaires spécifiques à son entreprise et à son environnement, le cas échéant. Les processus BAU sont un moyen de vérifier que les mesures de sécurité automatisés et manuels fonctionnent comme prévu. Qu'une exigence du standard PCI DSS soit automatisée ou manuelle, il est important que les processus BAU détectent les alertes et signalent les anomalies afin que les personnes en charge traitent la situation en temps opportun.

Des exemples de la façon dont le standard PCI DSS doit être intégré aux activités BAU comportent les actions suivantes, sans toutefois s'y limiter :

- Attribuer la responsabilité globale et la responsabilité de la conformité au standard PCI DSS, à un individu ou à une équipe. Cela peut inclure une charte définie par la Direction Générale pour un programme de conformité spécifique à un standard PCI DSS et une communication destinée à la direction générale.
- Développer des indicateurs de performance afin de mesurer l'efficacité des initiatives relatives à la sécurité et la surveillance continue des mesures de sécurité de sécurité, y compris ceux sur lesquels on s'appuie fortement, tels que les mesures de sécurité de sécurité réseau, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les mécanismes de détection de changement, les solutions contre les logiciels malveillants et les mesures de sécurité d'accès, afin de garantir qu'ils fonctionnent efficacement et comme prévu.
- Examiner les données enregistrées plus fréquemment afin d'obtenir des informations sur les tendances ou les comportements qui peuvent ne pas être évidents avec uniquement le suivi.
- Veiller à ce que toutes les défaillances des mesures de sécurité de sécurité soient détectées et traitées dans les plus brefs délais. Les processus pour répondre aux défaillances du contrôle de sécurité doivent inclure les éléments suivants :
  - La restauration de la mesure de sécurité.
  - Identifier la cause de l'échec.
  - Identifier et résoudre tous les problèmes de sécurité survenus lors de l'échec de la mesure de sécurité.
  - La mise en œuvre des mesures de mitigation, telles que des processus ou techniques de mesures de sécurité, afin d'éviter que la cause de la défaillance ne se reproduise.

- Reprendre le monitoring des mesures de sécurité, éventuellement avec une surveillance renforcée pendant une période de temps, afin de vérifier que la mesure fonctionne efficacement.
- Examiner les modifications qui pourraient introduire des risques de sécurité pour l'environnement PCI DSS (par exemple, ajout de nouveaux systèmes, modifications des configurations système ou réseau) avant d'effectuer la mise en production, et inclure les éléments suivants :
  - Une évaluation des risques pour déterminer l'impact potentiel sur le périmètre de le standard PCI DSS (par exemple, une nouvelle règle de mesures de sécurité réseau qui autorise la connectivité entre un système au sein du CDE et un autre système pourrait amener d'autres systèmes ou des réseaux dans le périmètre du standard PCI DSS).
  - L'identification des exigences du standard PCI DSS qui s'appliquent aux systèmes et réseaux affectés par les modifications (par exemple, si un nouveau système est couvert par le standard PCI DSS, il devra être configuré conformément aux standards de configuration du système, y compris les mécanismes de détection des modifications, les logiciels contre les programmes malveillants, les correctifs et la journalisation des audits. Ces nouveaux systèmes et réseaux devraient être ajoutés à l'inventaire des composants système dans le périmètre et au calendrier trimestriel d'analyse des vulnérabilités).
  - Mettre à jour le périmètre PCI DSS et mettre en œuvre des mesures de sécurité de sécurité, le cas échéant.
  - Mettre à jour la documentation pour qu'elle reflète les changements mis en œuvre.
- Examiner l'impact sur le périmètre et les exigences PCI DSS en cas de modification de la structure organisationnelle (par exemple, une fusion ou une acquisition d'entreprise).
- Examiner périodiquement les connexions externes et l'accès des tiers.
- Pour les entités qui font appel à des tiers pour le développement de logiciels, confirmer périodiquement que ces activités de développement de logiciels continuent de se conformer aux exigences de développement de logiciels de l'exigence 6.
- Effectuer des examens périodiques pour confirmer que les exigences du standard PCI DSS continuent d'être en place et que le personnel suit les processus établis. Les examens périodiques doivent couvrir toutes les installations et tous les emplacements, y compris les points de vente et les centres de données, qu'ils soient autogérés ou que les services d'un TPSP sont utilisés. Par exemple, des examens périodiques peuvent être utilisés pour confirmer que les standards de configuration ont été appliqués aux systèmes applicables, les comptes et les mots de passe du prestataire par défaut sont supprimés ou désactivés, les correctifs et les solutions contre les logiciels malveillants sont à jour, les journaux d'audit sont en cours d'examen, 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, sauf indication contraire dans le standard PCI DSS.

Ces examens peuvent également être utilisés pour vérifier que les preuves requises pour une évaluation du standard PCI DSS sont conservées. Par exemple, des preuves de journaux d'audit, de rapports d'analyse de vulnérabilité et d'examens des ensembles de règles de mesures de sécurité du réseau sont nécessaires pour aider l'entité à se préparer pour sa prochaine évaluation du standard PCI DSS.

- La mise en place d'une communication avec toutes les parties concernées, à la fois externes et internes, au sujet des menaces nouvellement identifiées et des changements apportés à la structure de l'entreprise. Les supports de communication doivent aider les destinataires à comprendre l'impact des menaces, les mesures pour les atténuer et les points de contact pour de plus amples informations ou pour un recours hiérarchique.
- L'examen des technologies matérielles et logicielles au moins une fois tous les 12 mois afin de confirmer qu'elles continuent d'être prises en charge par le fournisseur et qu'elles peuvent répondre aux exigences de sécurité de l'entité, y compris celles du standard PCI DSS. Si les technologies ne sont plus prises en charge par le fournisseur ou ne peuvent plus satisfaire aux besoins de sécurité de l'entité, l'entité doit préparer un plan de remise en état, y compris, si nécessaire, le remplacement de la technologie.

**Remarque :** Certaines bonnes pratiques de cette section sont également incorporées en tant qu'exigences du standard PCI DSS pour certaines entités. Par exemple, celles subissant une évaluation complète du standard PCI DSS, les prestataires de services validant les exigences supplémentaires « prestataires de services uniquement » et les entités désignées qui doivent valider conformément à l'annexe A3 : Validation complémentaire des entités désignées.

Chaque entité doit envisager de mettre en œuvre ces bonnes pratiques dans son environnement, même si l'entité n'est pas obligée de les valider (par exemple, les commerçants faisant l'objet d'une auto-évaluation).

Reportez-vous au document *Bonnes pratiques pour maintenir la conformité du standard PCI DSS* dans la bibliothèque de documents sur le site Web PCI SSC afin d'obtenir des conseils supplémentaires.

## 6 Pour les Auditeurs : Échantillonnage pour les Évaluations du Standard PCI DSS

L'échantillonnage est une option pour les auditeurs effectuant des évaluations du standard PCI DSS afin de faciliter le processus d'évaluation lorsqu'il y a un grand nombre d'éléments dans une population testée.

Bien qu'il soit acceptable pour un auditeur d'échantillonner à partir d'éléments similaires dans une population testée dans le cadre de son examen de la conformité du standard PCI DSS d'une entité, il n'est pas acceptable qu'une entité applique les exigences du standard PCI DSS à uniquement un échantillon de son environnement (par exemple, les exigences relatives aux analyses trimestrielles des vulnérabilités s'appliquent à tous les composants du système). De même, il n'est pas acceptable qu'un auditeur n'examine qu'un échantillon des exigences du standard PCI DSS pour la conformité.

Bien que l'échantillonnage permette aux auditeurs de tester moins de 100 % d'une population donnée, les auditeurs doivent toujours s'efforcer d'obtenir l'examen le plus complet possible. Les auditeurs sont encouragés à utiliser des processus automatisés ou d'autres mécanismes si la population complète, quelle que soit sa taille, peut être testée rapidement et efficacement avec une incidence minimale sur les ressources de l'entité en cours d'évaluation. Lorsque des processus automatisés ne sont pas disponibles pour tester une population à 100 %, l'échantillonnage est une approche également acceptable.

Après avoir examiné le périmètre global, la complexité et la cohérence de l'environnement évalué, ainsi que la nature (automatisée ou manuelle) des processus utilisés par une entité afin de satisfaire à une exigence, l'auditeur peut sélectionner de manière indépendante des échantillons représentatifs des populations examinées afin d'évaluer la conformité de l'entité aux exigences du standard PCI DSS. Les échantillons doivent être une sélection représentative de toutes les variantes de la population et doivent être suffisamment nombreux pour qu'ils puissent fournir à l'auditeur l'assurance que les mesures de sécurité sont mises en œuvre comme prévu dans l'ensemble de la population. Lorsqu'il teste la performance périodique d'une exigence (par exemple, toutes les semaines, tous les trois mois ou périodiquement), l'auditeur doit tenter de sélectionner un échantillon qui représente toute la période couverte par l'évaluation afin qu'il puisse juger raisonnablement que l'exigence a été satisfaite tout au long de la période d'évaluation. Tester le même échantillon d'éléments année après année pourrait impliquer que des nouveaux éléments appartenant à de l'environnement PCI ne soient pas inclus dans les éléments non échantillonés. Les auditeurs doivent revalider la justification de l'échantillonnage pour chaque évaluation et tenir compte des ensembles d'échantillons précédents. Différents échantillons doivent être sélectionnés pour chaque évaluation.

La sélection adéquate de l'échantillonnage dépend de ce qui est pris en compte lors de l'examen des composants de l'échantillon. Par exemple, déterminer la présence de logiciel "anti- malware " sur des serveurs connus pour être vulnérables à ceux-ci peut conduire à déterminer la population comme étant tous les serveurs de l'environnement ou tous les serveurs de l'environnement qui exécutent un système d'exploitation donné, ou tous les serveurs qui ne sont pas des ordinateurs centraux, etc. La sélection d'un échantillon approprié comprendrait alors des représentants de TOUS les membres de la population identifiée, y compris tous les serveurs exécutant le système d'exploitation identifié et toutes les versions, ainsi que les serveurs dans la population qui sont utilisés pour différentes fonctions (par exemple, serveurs Web, serveurs d'applications et serveurs de bases de données).

Dans le cas où un élément spécifique de configuration est envisagé, la population peut être divisée de manière adéquate et des groupes d'échantillons distincts identifiés. Par exemple, un échantillon de tous les serveurs peut ne pas être approprié lors de l'examen d'un paramètre de configuration d'un système d'exploitation, où différents systèmes d'exploitation sont présents dans l'environnement. Dans ce cas, des

exemples de chaque type de système d'exploitation seraient appropriés pour identifier que la configuration a été correctement définie pour chaque système d'exploitation. Chaque échantillon doit inclure des serveurs représentatifs de chaque type de système d'exploitation, y compris la version, ainsi que des fonctions représentatives.

D'autres exemples d'échantillonnage comportent des sélections de personnel avec des rôles similaires ou variés, en fonction de l'exigence évaluée ; par exemple, un échantillon d'administrateurs par rapport à un échantillon de tous les employés.

L'auditeur est tenu d'exercer son jugement professionnel dans la planification, la performance et l'évaluation de l'échantillon afin d'étayer sa conclusion quant à savoir si et comment l'entité a satisfait à une exigence. L'objectif de l'auditeur dans l'échantillonnage est d'obtenir suffisamment de preuves pour avoir un fondement raisonnable pour son opinion. Lors d'une sélection indépendante des échantillons, les auditeurs doivent tenir compte des éléments suivants :

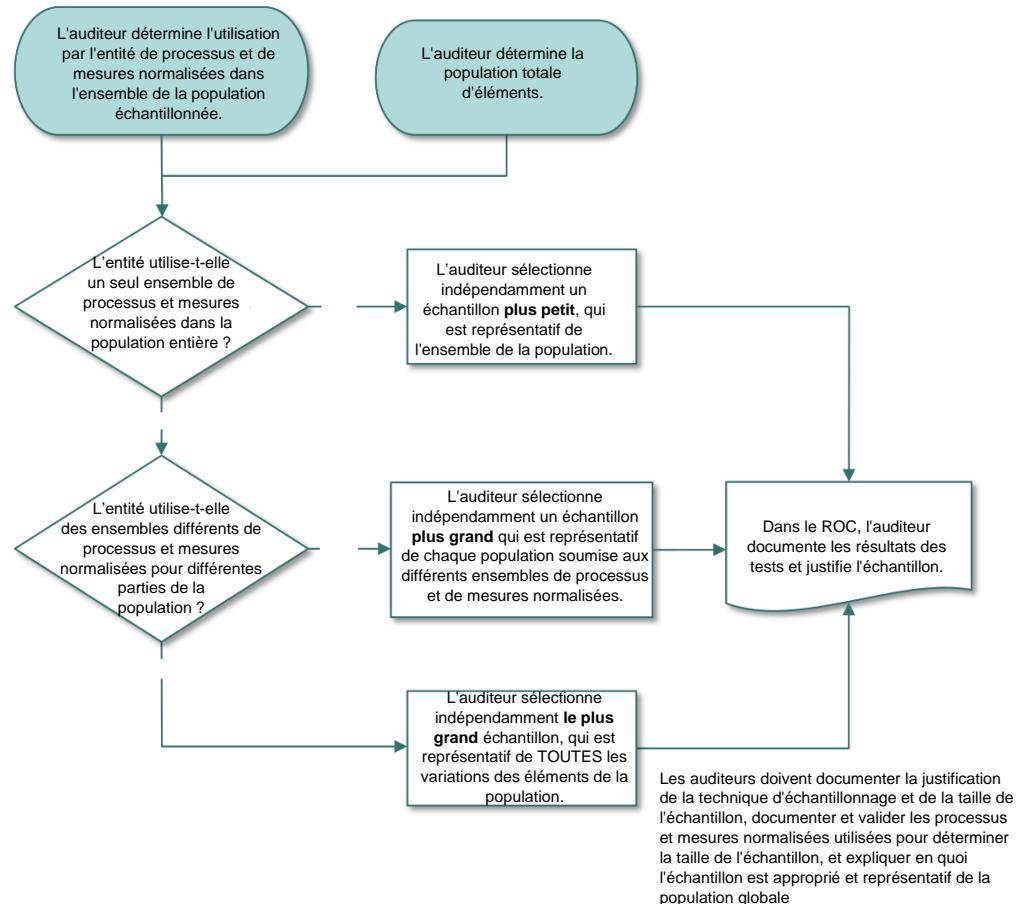
- L'auditeur doit sélectionner l'échantillon dans la population complète sans aucune influence de l'entité évaluée.
- Si l'entité a mis en place des processus et des mesures de sécurité normalisés qui garantissent la cohérence et qui sont appliqués à chaque élément de la population, l'échantillon ne peut être plus restreint que si l'entité n'avait pas de processus/mesures de sécurité normalisés en place. L'échantillon doit être suffisamment grand pour fournir à l'auditeur une assurance raisonnable que les éléments de la population adhèrent aux processus normalisés qui sont appliqués à chaque élément de la population. L'auditeur doit vérifier que les mesures de sécurité normalisée sont mises en œuvre et fonctionnent de manière efficace.
- Si l'entité a mis en place plusieurs types de processus normalisés (par exemple, pour différents types d'installations commerciales/composants système), l'échantillon doit inclure des éléments soumis à chaque type de processus. Par exemple, les populations pourraient être divisées en sous-populations en fonction de caractéristiques susceptibles d'avoir une incidence sur la cohérence des exigences évaluées, telles que l'utilisation de différents processus ou outils. Des échantillons seraient ensuite sélectionnés dans chaque sous-population.
- Si l'entité n'a pas mis en place de processus/mesures de sécurité PCI DSS normalisés et que chaque élément de la population est géré par des processus non normalisés, l'échantillon doit être plus grand pour que l'auditeur soit assuré que les exigences du standard PCI DSS sont correctement appliquées à chaque élément dans la population.
- Les échantillons de composants système doivent inclure tous les types et combinaisons utilisés. Lorsqu'une entité a plus d'un CDE, les échantillons doivent inclure des populations dans tous les composants système dans la portée. Par exemple, lorsque des applications sont échantillonnées, l'échantillon doit inclure toutes les versions et les plates-formes pour chaque type d'application.
- La taille des échantillons doit toujours être supérieure à un, à moins qu'il n'y ait qu'un seul élément dans la population donnée, ou qu'une mesure automatisée soit utilisé lorsque l'auditeur a confirmé que la mesure fonctionne comme programmé pour chaque population d'échantillon évaluée.
- Si l'auditeur s'appuie sur des processus et des mesures de sécurité normalisés pour sélectionner un échantillon, mais découvre ensuite au cours des tests que des processus et des mesures de sécurité normalisés ne sont pas en place ou ne fonctionnent pas efficacement, l'auditeur doit alors augmenter la taille de l'échantillon pour tenter d'obtenir l'assurance que les exigences du standard PCI DSS sont respectées.

Pour chaque instance où l'échantillonnage est utilisé, l'auditeur doit :

- Documenter la justification de la technique d'échantillonnage et de la taille de l'échantillon.
- Valider et documenter les processus et mesures de sécurité normalisés utilisés pour déterminer la taille de l'échantillon.
- Expliquer en quoi l'échantillon est approprié et représentatif de la population globale.

La figure 3 montre les considérations pour déterminer la taille de l'échantillon.

**Figure 3. Considérations Relatives à L'échantillonnage PCI DSS**



**Remarque :** Dans le standard PCI DSS v4.0, les références spécifiques à l'échantillonnage ont été supprimées de toutes les procédures de test. Ces références ont été supprimées car le fait de mentionner l'échantillonnage uniquement dans certaines procédures de test peut avoir impliqué que l'échantillonnage était obligatoire pour ces procédures de test (ce qui n'était pas le cas) ou que l'échantillonnage n'était autorisé que là où il était spécifiquement mentionné. Les auditeurs doivent sélectionner des échantillons lorsque cela convient à la population testée et, conformément à ce qui précède, prendre ces décisions après avoir examiné le périmètre et la complexité globales d'un environnement.

## 7 Description des Délais Utilisés dans les Exigences PCI DSS

Certaines exigences du standard PCI DSS ont été établies avec des délais spécifiques pour les activités qui doivent être effectuées de manière cohérente via un processus régulièrement programmé et reproductible. L'intention est que l'activité soit effectuée à un intervalle aussi proche que possible de cette période sans toutefois la dépasser. L'entité a le pouvoir discrétionnaire d'effectuer une activité plus souvent que spécifié (par exemple, effectuer une activité mensuellement lorsque l'exigence du standard PCI DSS spécifie qu'elle doit être effectuée tous les trois mois).

Le tableau 4 présente la fréquence des différentes périodes utilisées dans les exigences du standard PCI DSS.

**Tableau 4. Délais des Exigences du Standard PCI DSS**

Délais dans les Exigences du Standard PCI DSS	Descriptions et Exemples
Tous les jours	Tous les jours de l'année (pas uniquement les jours ouvrables).
Toutes les semaines	Au moins une fois tous les sept jours.
Tous les mois	Au moins une fois tous les 30 à 31 jours, ou le $n^{\text{ème}}$ jour du mois.
Tous les trois mois (« chaque trimestre »)	Au moins une fois tous les 90 à 92 jours, ou le $n^{\text{ème}}$ jour de chaque troisième mois.
Tous les six mois	Au moins une fois tous les 180 à 184 jours, ou le $n^{\text{ème}}$ jour de chaque sixième mois.
Tous les 12 mois (« annuellement »)	Au moins une fois tous les 365 (ou 366 pour les années bissextiles) jours ou à la même date chaque année.
Périodiquement	La fréquence d'occurrence est à la discréSSION de l'entité et est documentée et étayée par l'analyse de risques de l'entité. L'entité doit démontrer que la fréquence est appropriée pour que l'activité soit efficace et pour répondre à l'intention de l'exigence.
Immédiatement	Sans délai. En temps réel ou quasi réel.
Ponctuellement	Dès que raisonnablement possible.

Délais dans les Exigences du Standard PCI DSS	Descriptions et Exemples
Changement significatif	<p>Il existe plusieurs exigences qui spécifient les activités à entreprendre lors d'un changement significatif dans l'environnement d'une entité. Alors que ce qui constitue un changement significatif dépend fortement de la configuration d'un environnement donné, chacune des activités suivantes, au minimum, a des incidences potentielles sur la sécurité du CDE, et doit être prise en considération et évaluée afin de déterminer si un changement est un changement significatif pour une entreprise dans le contexte des exigences connexes du standard PCI SSD :</p> <ul style="list-style-type: none"> <li>• Nouveau matériel, logiciel ou équipement réseau ajouté au CDE.</li> <li>• Tout remplacement ou mises à niveau majeures du matériel et/ou des logiciels du CDE.</li> <li>• Tout changement dans le flux ou le stockage des données de carte.</li> <li>• Toute modification de la limite du CDE et/ou du périmètre de l'évaluation du standard PCI DSS.</li> <li>• Toute modification au périmètre à l'infrastructure de soutien sous-jacente du CDE (y compris, sans toutefois s'y limiter, les modifications apportées aux services d'annuaire, aux serveurs de temps, à la journalisation et à la surveillance).</li> <li>• Toute modification au périmètre aux fournisseurs/prestataires de services tiers (ou aux services fournis) qui appuient le CDE ou répondent aux exigences du standard PCI DSS au nom de l'entité.</li> </ul>

Pour les autres exigences du standard PCI DSS, lorsque le standard ne définit pas de fréquence minimale pour les activités récurrentes, mais permet plutôt de respecter l'exigence « périodiquement », l'entité doit définir la fréquence appropriée de son activité. La fréquence définie par l'entité doit être étayée par la politique de sécurité de l'entité et l'analyse de risques réalisée conformément à l'exigence 12.3.1 du standard PCI DSS. L'entité doit également être en mesure de démontrer que la fréquence qu'elle a définie est appropriée pour que l'activité soit efficace et pour répondre à l'intention de l'exigence.

Dans les deux cas, lorsque le standard PCI DSS spécifie une fréquence obligatoire et lorsque le standard PCI DSS autorise des performances « périodiques », l'entité doit avoir documenté et mis en œuvre des processus afin de garantir que les activités sont exécutées dans un délai raisonnable, y compris au moins les éléments suivants :

- L'entité est rapidement notifiée chaque fois qu'une activité n'est pas effectuée selon son calendrier défini,
- L'entité détermine les événements qui ont conduit à rater une activité programmée,
- L'entité exécute l'activité dès que possible après qu'elle a été ratée et, soit elle reprend le calendrier, soit elle établit un nouveau calendrier,
- L'entité produit une documentation qui montre que les éléments ci-dessus se sont produits.

Lorsqu'une entité a mis en place les processus cités ci-dessus afin de détecter et traiter quand une activité programmée est ratée, une approche raisonnable est autorisée, ce qui signifie que si une activité doit être effectuée au moins une fois tous les trois mois, l'entité n'est pas automatiquement non conforme si l'activité est effectuée en retard lorsque le processus documenté et mis en œuvre de l'entité (voir ci-dessus)

a été suivi. Cependant, quand aucun processus de ce type n'est en place et/ou que l'activité n'a pas été exécutée conformément au calendrier en raison d'une omission, d'une mauvaise gestion ou d'un manque de surveillance, l'entité n'a pas satisfait à l'exigence. Dans de tels cas, l'exigence ne sera en place que lorsque l'entité 1) documente (ou reconfirme) le processus ci-dessus afin de s'assurer que l'activité prévue se déroule à temps, 2) rétablit le calendrier et 3) fournit la preuve que l'entité a effectué l'activité prévue au moins une fois conformément à son calendrier.

**Remarque :** *Lorsqu'une entité est évaluée pour la première fois pour une exigence PCI DSS avec un calendrier défini, cela est considéré comme une évaluation PCI DSS initiale de cette exigence. Cela signifie que l'entreprise n'a jamais subi une évaluation préalable pour cette exigence, lorsque l'évaluation a abouti à la soumission d'un document de validation de conformité (par exemple, un OAC, SAQ ou ROC)*

*Pour une évaluation initiale pour une exigence ayant un calendrier défini, il n'est pas nécessaire que l'activité ait été entreprise pour chacun de ces calendriers pendant l'année écoulée, si l'auditeur vérifie que :*

- *L'activité a été réalisée conformément à l'exigence applicable dans le délai le plus récent (par exemple, la période de trois ou six mois la plus récente), et*
- *L'entité a des politiques et des procédures documentées pour continuer à exercer l'activité dans le délai défini.*

*Pour les années qui suivent à l'évaluation initiale, l'activité doit avoir été réalisée au moins une fois au cours de chaque délai obligatoire. Par exemple, une activité obligatoire tous les trois mois doit avoir été réalisée au moins quatre fois au cours de l'année précédente à un intervalle ne dépassant pas 90 à 92 jours.*

## 8 Approches pour la mise en œuvre et la Validation du Standard PCI DSS

Pour soutenir la flexibilité dans la façon dont les objectifs de sécurité sont atteints, il existe deux approches pour la mise en œuvre et la validation du standard PCI DSS. Les entités doivent identifier l'approche la mieux adaptée à la mise en œuvre de leur sécurité et utiliser cette approche pour valider les mesures de sécurité.

<b>L'approche Définie</b>	<p>Suit la méthode classique de mise en œuvre et de validation du standard PCI DSS et utilise les exigences et les procédures de test définies dans le standard. Dans l'approche définie, l'entité met en œuvre des mesures de sécurité afin de répondre aux exigences énoncées, et l'auditeur suit les Procédures de Test de L'approche Définie afin de vérifier que les exigences ont été satisfaites.</p> <p>L'approche définie prend en charge les entités avec des mesures en place qui répondent aux exigences du standard PCI DSS, comme indiqué. Cette approche peut également convenir aux entités qui souhaitent davantage de conseils sur la manière d'atteindre les objectifs de sécurité, ainsi qu'aux entités novices en matière de sécurité des informations ou du standard PCI DSS.</p> <p><b>Mesures Compensatoires</b></p> <p>Dans le cadre de l'approche définie, les entités qui ne peuvent pas répondre explicitement à une exigence du standard PCI DSS, tel qu'indiqué, en raison d'une contrainte technique ou commerciale légitime et documentée, peuvent mettre en œuvre d'autres <i>mesures compensatoires</i>, qui atténueraient suffisamment le risque associé au fait de ne pas satisfaire à l'exigence. Sur une base annuelle, toutes les mesures compensatoires doivent être documentées par l'entité, examinées et validées par l'auditeur et incluses dans la soumission du rapport sur la conformité.</p>	<p><b>Remarque :</b> Pour plus de détails, consultez <i>l'Annexe B : Mesures compensatoires</i> et <i>l'Annexe C : Feuille de travail sur les mesures compensatoires</i>.</p>
<b>Approche Personnalisée</b>	<p>Se focalise sur l'objectif de chaque exigence du standard PCI DSS (se applicable), permettant aux entités de mettre en œuvre des mesures de sécurité afin de répondre à l'objectif de l'approche personnalisée indiqué par l'exigence d'une manière qui ne respecte pas strictement l'exigence définie. Étant donné que chaque implémentation personnalisée sera différente, il n'y a pas de procédures de test définies ; l'auditeur est tenu de dériver des procédures de test qui sont appropriées à l'implémentation spécifique afin de valider que les mesures de sécurité mis en œuvre répondent à l'objectif énoncé.</p> <p>L'approche personnalisée prend en charge l'innovation dans les pratiques de sécurité, permettant aux entités une plus grande flexibilité afin de montrer comment leurs mesures de sécurité de sécurité actuels répondent aux objectifs du standard PCI DSS. Cette approche est destinée aux entités qui jouissent d'une maturité en termes de gestion des risques, et qui démontrent une approche robuste de gestion des risques en matière de sécurité, y compris, sans toutefois s'y limiter, un service dédié à la gestion des</p>	<p><b>Remarque :</b> Pour plus de détails, consulter <i>l'Annexe D : Approche personnalisée</i> et <i>PCI DSS v4.x : Exemples de modèles pour prendre en charge l'Approche Personnalisée</i> sur le site Web du PCI SSC.</p>

risques ou une approche de gestion des risques à l'échelle de l'entreprise.

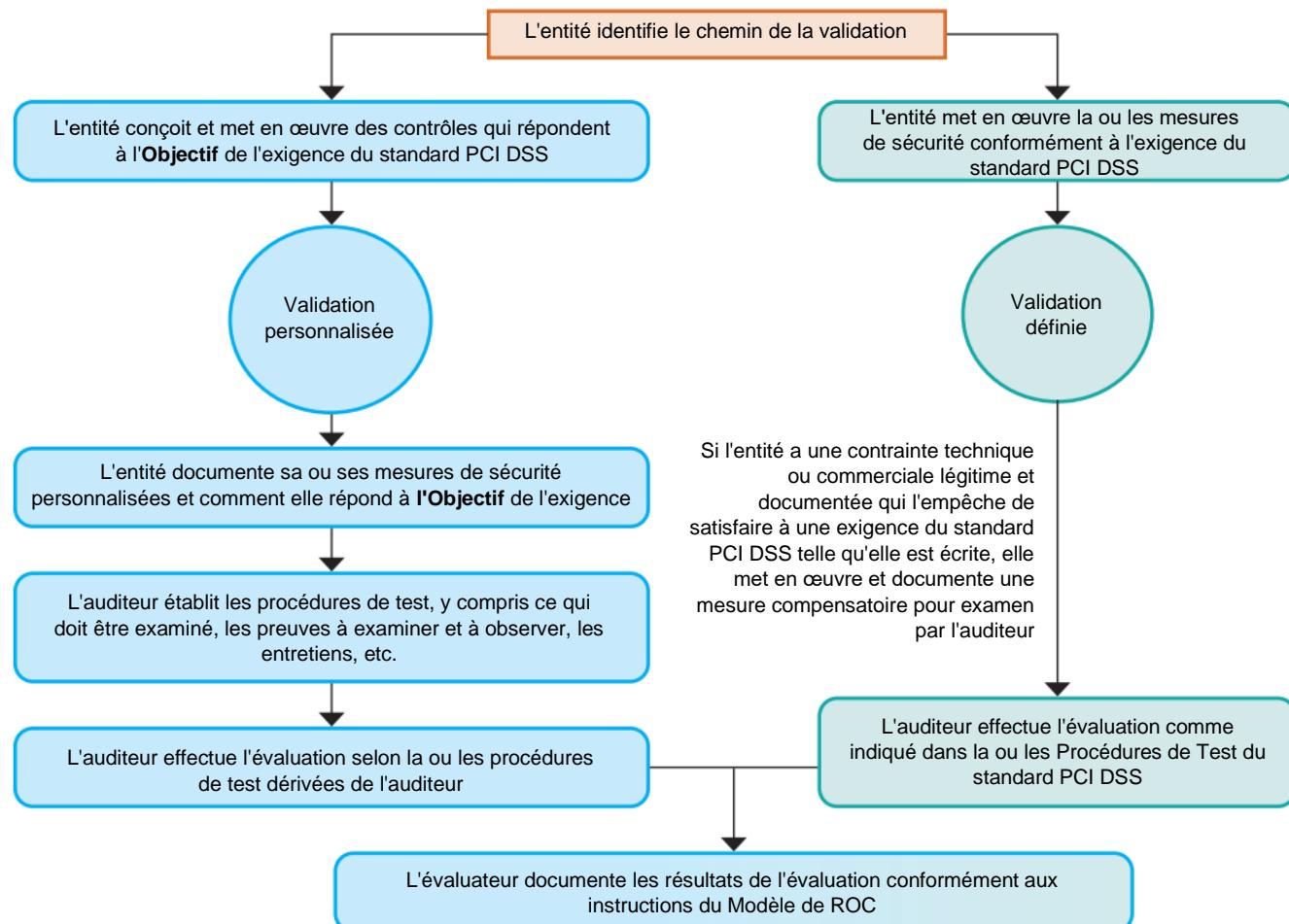
Les mesures de sécurité mis en œuvre et validés via l'approche personnalisée devraient atteindre ou dépasser la sécurité fournie par l'exigence de l'approche définie. Le niveau de documentation et d'effort requis pour valider les mises en œuvre personnalisées sera également supérieur à celui de l'approche définie.

La plupart des exigences du standard PCI DSS peuvent être satisfaites en utilisant l'approche définie ou personnalisée. Cependant, plusieurs exigences ne prescrivent aucun objectif d'approche personnalisée déclaré ; l'approche personnalisée n'est pas une option pour ces exigences.

Les entités peuvent utiliser à la fois les approches définies et personnalisées dans leur environnement. Cela signifie qu'une entité pourrait utiliser l'approche définie pour satisfaire à certaines exigences et utiliser l'approche personnalisée afin de satisfaire à d'autres exigences. Cela signifie également qu'une entité pourrait utiliser l'approche définie pour satisfaire à une exigence PCI DSS donnée pour un composant système ou dans un environnement, et utiliser l'approche personnalisée pour satisfaire à cette même exigence du standard PCI DSS pour un composant système différent ou dans un environnement différent. De cette façon, une évaluation du standard PCI DSS pourrait inclure des procédures de test à la fois définies et personnalisées.

La figure 4 montre les deux options de validation pour le standard PCI DSS v4.x.

**Figure 4. Approches de Validation du Standard PCI DSS**



## 9 Protéger les Informations Relatives à L'état de Sécurité d'une Entité

Les processus pour obtenir et maintenir un environnement conforme au standard PCI DSS génèrent de nombreux artefacts qu'une entité peut considérer comme sensibles et peut souhaiter protéger en tant que tels, notamment des éléments suivants :

- Le rapport sur la conformité ou le questionnaire d'auto-évaluation (l'attestation de conformité associée n'est pas considérée comme sensible et les prestataires de services tiers (TPSP) sont censés partager leur AOC avec les clients).
- Diagrammes de réseau et diagrammes de flux de données de carte, et configurations et règles de sécurité.
- Standards relatifs à la configuration du système.
- Méthodes et protocoles de cryptographie et de gestion des clés.

Les entités doivent examiner tous les artefacts liés aux mesures de sécurité PCI DSS ou à l'évaluation, et les protéger conformément aux politiques de sécurité de l'entité pour ce type d'informations.

Les TPSP sont tenus (exigence 12.9 du standard PCI DSS) de prendre en charge leurs clients dans les domaines suivants :

- Les informations nécessaires aux clients pour surveiller l'état de conformité PCI DSS des TPSP (afin de permettre au consommateur de se conformer à l'exigence 12.8), et
- Des preuves que le TPSP satisfait aux exigences PCI DSS applicables lorsque les services du TPSP sont destinés à répondre au, ou à faciliter le respect des exigences PCI DSS d'un consommateur, ou lorsque ces services peuvent avoir une incidence sur la sécurité données de titulaires de carte ou des données d'authentification sensibles d'un consommateur.

Cette section n'affecte ni n'annule l'obligation d'un TPSP de soutenir et de fournir des informations à ses clients conformément à l'exigence 12.9.

Pour plus de détails sur les attentes des TPSP et les relations entre les TPSP et les clients, voir [Utilisation de Prestataires de Services Tiers](#).

### ***Protection des Informations Confidentielles et Sensibles par des Entreprises D'évaluation de Sécurité Qualifiées***

Chaque entreprise d'audit de sécurité qualifié (QSA) signe un accord avec le PCI SSC selon lequel elle adhérera aux exigences de qualification pour les QSA. La section *Protection des informations confidentielles et sensibles* de ce document comporte les éléments suivants :

« L'entreprise QSA doit avoir et suivre un processus documenté pour la protection des informations confidentielles et sensibles. Cela doit inclure des garanties physiques, électroniques et procédurales adéquates conformes aux pratiques acceptées par l'industrie afin de protéger les informations confidentielles et sensibles contre toute menace ou accès non autorisé pendant le stockage, le traitement et/ou la communication de ces informations.

L'entreprise QSA doit préserver le caractère privé et confidentiel des informations obtenues dans le cadre de l'exercice de ses fonctions et obligations en tant qu'entreprise QSA, à moins que (et dans la mesure où) la divulgation ne soit requise par une autorité juridique. »

## 10 Méthodes de Test pour les Exigences du Standard PCI DSS

Les méthodes de test identifiées dans les Procédures de test pour chaque exigence décrivent les activités sensées être effectuées par l'auditeur afin de déterminer si l'entité a satisfait à l'exigence. L'intention derrière chaque méthode de test est décrite comme suit :

- **Examen** : L'auditeur évalue de manière critique les justificatifs des données disponibles. Les exemples courants incluent les documents (électroniques ou physiques), les captures d'écran, les fichiers de configuration, les journaux d'audit et les fichiers de données.
- **Observer** : L'auditeur observe une action ou voit quelque chose dans l'environnement. Des exemples de sujets d'observation incluent le personnel effectuant une tâche ou un processus, les composants du système exécutant une fonction ou répondant à une entrée, les conditions environnementales et les mesures de sécurité physiques.
- **Entretien** : L'auditeur s'entretient avec le personnel individuel. Les objectifs de l'entretien peuvent inclure la confirmation de l'exécution d'une activité, des descriptions de la manière dont une activité est exécutée et si le personnel a des connaissances ou une compréhension particulière.

Les méthodes de test sont destinées à permettre à l'entité évaluée de démontrer comment elle a satisfait à une exigence. Elles fournissent également à l'entité évaluée et à l'auditeur une compréhension commune des activités d'évaluation à effectuer. Les éléments spécifiques à examiner ou à observer et le personnel à interroger doivent être adaptés à la fois à l'exigence évaluée et à la mise en œuvre particulière de chaque entité. Lors de la documentation des résultats de l'audit, l'auditeur identifie les activités de test réalisées et le résultat de chaque activité.

## 11 Instructions et Contenu du Rapport de Conformité

Les instructions et le contenu du rapport de conformité (ROC) sont fournis dans le *Modèle de rapport de conformité au standard PCI DSS (ROC)*.

Le modèle de rapport de conformité PCI DSS (ROC) doit être utilisé comme modèle pour créer un rapport de conformité au standard PCI DSS.

Le fait qu'une entité soit tenue de se conformer ou de valider sa conformité au standard PCI DSS reste à la discréction des entreprises qui gèrent les programmes de conformité (telles que les réseaux internationaux et les acquéreurs). Les entités doivent contacter ces entreprises afin de déterminer les exigences et les instructions de rapports.

## 12 Processus D'évaluation du Standard PCI DSS

Le processus d'évaluation du standard PCI DSS comprend les étapes de haut niveau suivantes :<sup>5</sup>

1. Confirmer le périmètre de l'évaluation du standard PCI DSS
2. Effectuer l'évaluation PCI DSS de l'environnement.
3. Remplir le rapport applicable pour l'évaluation conformément aux directives et instructions du standard PCI DSS.
4. Remplir l'attestation de conformité dans son intégralité pour les prestataires de services ou les commerçants, selon le cas. Les attestations officielles de conformité ne sont disponibles que sur le site Web du standard PCI SSC.
5. Soumettre la documentation applicable du standard PCI SSC et l'attestation de conformité, ainsi que toute autre documentation demandée, telle que les rapports d'analyse ASV, aux entreprises requérantes (à savoir celles qui gèrent les programmes de conformité telles que les réseaux internationaux et les acquéreurs (pour les commerçants) ou autres requérants (pour les prestataires de services)).
6. Si nécessaire, effectuer des mesures correctives afin de répondre aux exigences qui ne sont pas en place et fournir un rapport mis à jour.

**Remarque :** Les exigences du standard PCI DSS ne sont pas considérées comme étant en place si les mesures de sécurité ne sont pas encore mises en œuvre ou sont programmés pour la mise en œuvre à une date ultérieure. Une fois que tous les éléments ouverts ou non en place ont été traités par l'entité, l'auditeur procédera à une réévaluation afin de valider que les mesures correctives ont été réalisées et que toutes les exigences sont désormais satisfaites. Reportez-vous aux ressources suivantes (disponibles sur le site Web du standard PCI SSC) pour documenter l'évaluation du standard PCI DSS :

- Pour obtenir des instructions sur la manière de remplir des rapports sur la conformité (ROC), reportez-vous au modèle de rapport sur la conformité (ROC) du standard PCI DSS.
- Pour obtenir des instructions sur la manière de remplir les questionnaires d'auto-évaluation (SAQ), reportez-vous aux instructions et directives relatives aux SAQ du standard PCI DSS.
- Pour obtenir des instructions sur la soumission des rapports de validation de conformité au standard PCI DSS, reportez-vous à l'attestation de conformité du standard PCI DSS.

<sup>5</sup> Le processus d'évaluation du standard PCI DSS, ainsi que les rôles et les responsabilités pour la réalisation de chaque étape, varient en fonction du type d'évaluation et des programmes de conformité, qui sont gérés par les réseaux internationaux et les acquéreurs.

## 13 Autres Références

Le tableau 5 répertorie les organismes de standardisation externes référencés dans les exigences du standard PCI DSS ou les directives associées. Ces entreprises externes et leurs références sont fournies à titre indicatif et ne remplacent ni n'étendent aucune exigence du standard PCI DSS.

**Tableau 5. Entreprises Externes Référencées dans les Exigences du Standard PCI DSS**

Référence	Nom Complet
ANSI	American National Standards Institute (Institut national américain de normalisation)
CIS	Center for Internet Security (Centre pour la sécurité Internet)
CSA	Cloud Security Alliance (Alliance pour la sécurité du cloud)
ENISA	European Union Agency for Cybersecurity (Agence de l'Union européenne pour la cybersécurité) (précédemment connue sous le nom de European Network and Information Security Agency (Agence européenne chargée de la sécurité des réseaux et de l'information))
FIDO Alliance	La FIDO Alliance (Alliance FIDO)
ISO	International Organization for Standardization (Organisation internationale de normalisation)
NCSC	The UK National Cyber Security Centre (Le Centre national de cybersécurité du Royaume-Uni)
NIST	National Institute of Standards and Technology (Institut national des standards et de la technologie)
OWASP	Open Web Application Security Project (Projet de sécurité des applications Web ouvertes)
SAFECode	Software Assurance Forum for Excellence in Code (Forum de la Software Assurance pour l'excellence dans le code)

## 14 Versions du Standard PCI DSS

À la date de publication de ce document, le standard PCI DSS v4.0.1 est la version en vigueur du standard.

Des questions concernant l'utilisation de versions antérieures doivent être adressées à ces entreprises qui gèrent les programmes de conformité (tels que les marques de paiement et les acquéreurs).

Le tableau 6 résume les versions du standard PCI DSS et leurs dates pertinentes.<sup>6</sup>

**Tableau 6. Versions du Standard PCI DSS**

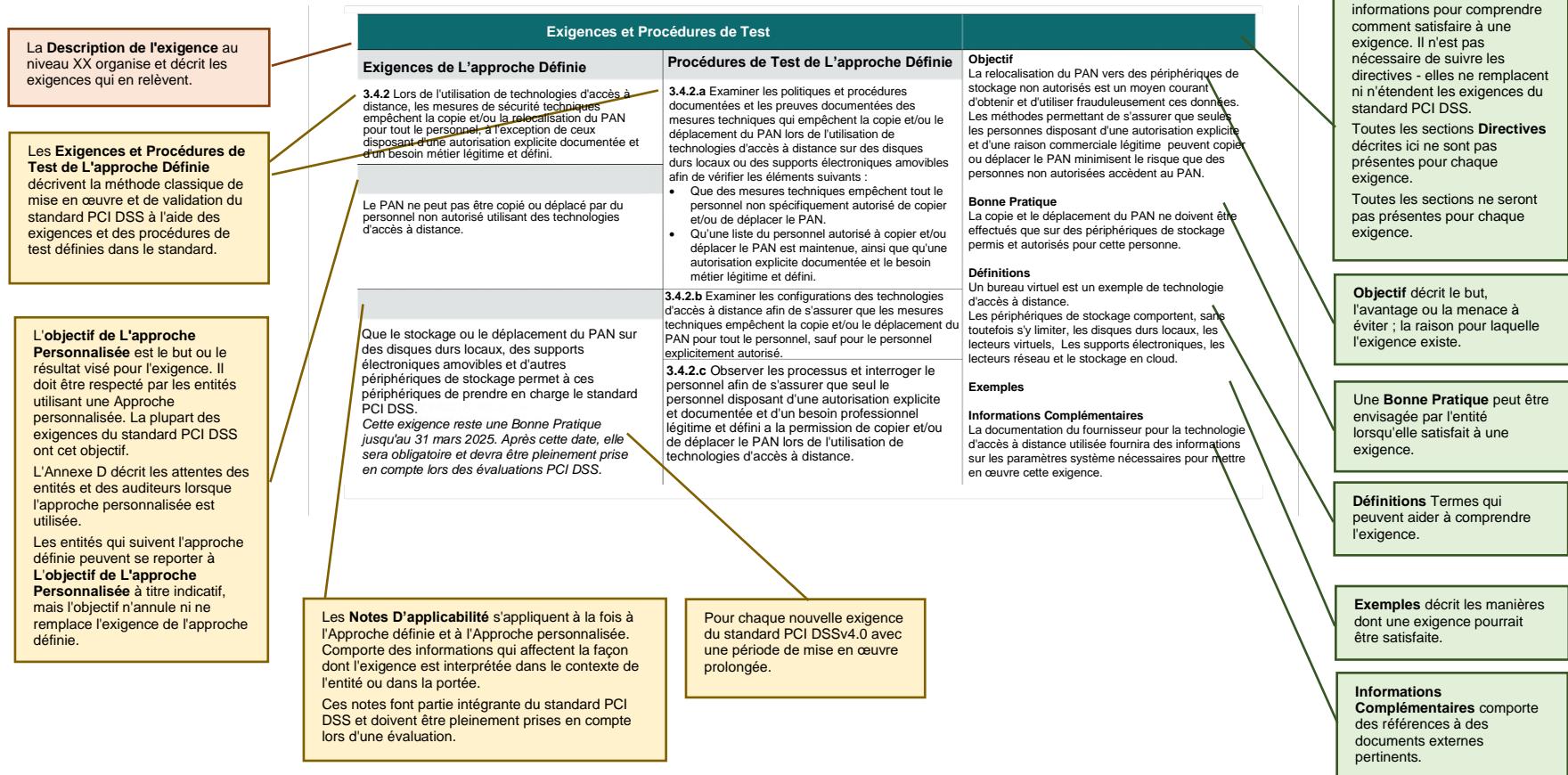
Version	Publiée	Retirée
PCI DSS v4.0.1 (le présent document)	Juin 2024	À déterminer
PCI DSS v4.0	Mars 2022	31 décembre 2024
PCI DSS v3.2.1	Mai 2018	31 mars 2024
PCI DSS v3.2	Avril 2016	31 décembre 2018

<sup>6</sup> Sous réserve de modifications lors de la sortie d'une nouvelle version du standard PCI DSS.

## 15 Exigences Détaillées du Standard PCI DSS et Procédures de Test

La figure 5 décrit les en-têtes et le contenu des colonnes pour les exigences du standard PCI DSS.

Figure 5. Comprendre les Parties des Exigences



## ***Exigences Supplémentaires pour les Prestataires de Services Uniquement***

Certaines exigences ne s'appliquent que lorsque l'entité évaluée est un prestataire de services. Celles-ci sont identifiées dans l'exigence comme « *Exigence supplémentaire pour les prestataires de services uniquement* » et s'appliquent en plus de toutes les autres exigences applicables. Lorsque l'entité évaluée est à la fois un commerçant et un prestataire de services, les exigences notées « *Exigence supplémentaire pour les prestataires de services uniquement* » s'appliquent à la partie relative au prestataire de services de l'activité de l'entité. Les exigences identifiées par « *Exigence supplémentaire pour les prestataires de services uniquement* » sont également recommandées en tant que meilleures pratiques à prendre en compte par toutes les entités.

## ***Annexes avec des Exigences Supplémentaires du Standard PCI DSS pour Différents Types D'entités***

En plus des 12 exigences principales, l'annexe A du standard PCI DSS contient des exigences PCI DSS supplémentaires concernant différents types d'entités. Les sections de l'Annexe A comprennent :

- Annexe A1 : Autres exigences du standard PCI DSS pour les prestataires de services mutualisés.
- Annexe A2 : Autres exigences du standard PCI DSS pour les entités utilisant SSL/précoce TLS pour les connexions de terminaux POS POI avec carte.
- Annexe A3 : Validation complémentaire des entités désignées (DESV).

## Créer et Maintenir un Réseau et des Systèmes Sécurisés

### ***Exigence 1 : Installer et Maintenir des Mesures de Sécurité du Réseau***

#### Sections

- 1.1** Les processus et mécanismes d'installation et de maintenance des mesures de sécurité de sécurité du réseau sont définis et compris.
- 1.2** Les mesures de sécurité de sécurité réseau (NSC) sont configurés et maintenus.
- 1.3** L'accès au réseau vers et depuis l'environnement de données du titulaire de carte est restreint.
- 1.4** Les connexions réseau entre les réseaux de confiance et les réseaux non fiables sont contrôlées.
- 1.5** Les risques pour le CDE provenant d'appareils informatiques capables de se connecter à la fois à des réseaux non fiables et au CDE sont atténués.

## Aperçu

Les mesures de sécurité de sécurité réseau (NSC), tels que les pare-feu et autres technologies de sécurité réseau, sont des points d'application de la politique réseau qui contrôlent généralement le trafic réseau entre deux ou plusieurs segments de réseau logiques ou physiques (ou sous-réseaux) en fonction de *politiques* ou de *règles* prédéfinies.

Les NSC examinent tout le trafic réseau entrant (entrée) et sortant (sortie) d'un segment et décident, en fonction des politiques définies, si le trafic réseau est autorisé à passer ou s'il doit être rejeté. En règle générale, les NSC sont placés entre des environnements avec des besoins de sécurité ou des niveaux de confiance différents, mais dans certains environnements, les NSC contrôlent le trafic vers des appareils individuels indépendamment des limites de confiance. L'application des politiques se produit généralement à la couche 3 du modèle OSI, mais les données présentes dans les couches supérieures sont également fréquemment utilisées pour déterminer les décisions politiques.

Traditionnellement, cette fonction était assurée par des pare-feu physiques ; cependant, cette fonctionnalité peut désormais être fournie par des appareils virtuels, des mesures de sécurité d'accès cloud, des systèmes de virtualisation/conteneurs et d'autres technologies réseau basées sur des logiciels.

Les NSC sont utilisés pour contrôler le trafic au sein des réseaux propres d'une entité ; par exemple, entre des zones hautement sensibles et des zones moins sensibles, et également pour protéger les ressources de l'entité contre l'exposition à des réseaux non fiables.

L'environnement de données des titulaires de cartes (CDE) est un exemple de zone plus sensible au sein du réseau d'une entité. Souvent, des chemins apparemment insignifiants vers et depuis des réseaux non fiables peuvent fournir des chemins non protégés vers des systèmes sensibles. Les NSC fournissent un mécanisme de protection clé pour tout réseau informatique.

Les exemples courants de réseaux non fiables incluent Internet, les connexions dédiées telles que les canaux de communication interentreprises, les réseaux sans fil, les réseaux d'opérateurs (tels que les réseaux cellulaires), les réseaux de tiers et d'autres sources que l'entité n'est pas en mesure de contrôler. En outre, les réseaux non fiables incluent également les réseaux d'entreprise qui sont considérés comme hors périmètre pour PCI DSS, car ils ne sont pas évalués et doivent donc être traités comme non fiables car l'existence de mesures de sécurité de sécurité n'a pas été vérifiée. Alors qu'une entité peut considérer qu'un réseau interne est digne de confiance du point de vue de l'infrastructure, si un réseau est hors périmètre pour PCI DSS, ce réseau doit être considéré comme non fiable pour le standard PCI DSS.

Se reporter à *l'Annexe G* pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>1.1 Les processus et mécanismes d'installation et de maintenance des mesures de sécurité du réseau sont définis et compris.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 1 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attentes, les mesures de sécurité et la surveillance des activités relatives à l'exigence 1 sont définis, compris et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 1 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b> L'exigence 1.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 1. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'Exigence 1, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour ces raisons, penser à mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique.</p> <p><b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 1 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités des activités de l'exigence 1 sont documentées et attribuées.</p> <p><b>1.1.2.b</b> Interroger le personnel responsable de l'exécution des activités de l'Exigence 1 afin de vérifier que les rôles et les responsabilités sont attribués comme documentés et sont compris.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 1 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redouble, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>1.2 Les mesures de sécurité de sécurité réseau (NSC) sont configurés et maintenus.</b>	
<b>Exigences de L'approche Définie</b> <p><b>1.2.1</b> Les standards de configuration pour les ensembles de règles NSC sont :</p> <ul style="list-style-type: none"> <li>• Définies.</li> <li>• Mise en œuvre.</li> <li>• Maintenues.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.2.1.a</b> Examiner les standards de configuration des ensembles de règles NSC afin de vérifier que les standards sont conformes à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.2.1.b</b> Examiner les paramètres de configuration des ensembles de règles NSC afin de vérifier que les ensembles de règles sont mis en œuvre conformément aux standards de configuration.</p>
<b>Objectif de L'approche Personnalisée</b> <p>La façon dont les NSC sont configurés et fonctionnent est définie et appliquée de manière cohérente.</p>	<b>Objectif</b> <p>La mise en œuvre de ces standards de configuration entraîne la configuration et la gestion du NSC pour exécuter correctement sa fonction de sécurité (souvent appelée ensemble de règles).</p> <p><b>Bonne Pratique</b></p> <p>Ces standards définissent souvent les exigences pour les protocoles acceptables, les ports dont l'utilisation est autorisée et les exigences de configuration spécifiques qui sont acceptables. Les standards de configuration peuvent également décrire ce que l'entité considère comme inacceptable ou non autorisé au sein de son réseau.</p> <p><b>Définitions</b></p> <p>Les NSC sont des composants clés d'une architecture réseau. Le plus souvent, les NSC sont utilisés aux limites du CDE afin de contrôler le trafic réseau entrant et sortant du CDE. Les standards de configuration décrivent les exigences minimales d'une entité pour la configuration de ses NSC.</p> <p><b>Exemples</b></p> <p>Des exemples de NSC couverts par ces standards de configuration comprennent, sans toutefois s'y limiter, les pare-feu, les routeurs configurés avec des listes de contrôle d'accès et les réseaux virtuels cloud.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>1.2.2</b> Toutes les modifications apportées aux connexions réseau et aux configurations des NSC sont approuvées et gérées conformément au processus de contrôle des modifications défini dans l'exigence 6.5.1.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.2.2.a</b> Examiner les procédures documentées pour vérifier que les modifications apportées aux connexions réseau et aux configurations des NSC sont incluses dans le processus formel de contrôle des modifications conformément à l'exigence 6.5.1.</p> <p><b>1.2.2.b</b> Examiner les paramètres de configuration réseau afin d'identifier les modifications apportées aux connexions réseau. Interroger le personnel en charge et examiner les enregistrements de contrôle des modifications afin de vérifier que les modifications identifiées des connexions réseau ont été approuvées et gérées conformément à l'exigence 6.5.1.</p> <p><b>1.2.2.c</b> Examiner les paramètres de configuration réseau afin d'identifier les modifications apportées aux configurations des NSC. Interroger le personnel en charge et examiner les enregistrements de contrôle des modifications afin de vérifier que les modifications identifiées apportées aux configurations des NSC ont été approuvées et gérées conformément à l'exigence 6.5.1.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les modifications apportées aux connexions réseau et aux NSC ne peuvent pas entraîner une mauvaise configuration, une mise en œuvre de services non sécurisés ou des connexions réseau non autorisées.</p>	<b>Objectif</b> Suivre un processus structuré de contrôle des changements pour tous les changements aux NSC réduit le risque qu'un changement pourrait introduire une vulnérabilité de sécurité. <b>Bonne Pratique</b> Les modifications doivent être approuvées par des personnes ayant l'autorité et les connaissances appropriées pour comprendre l'impact des modifications. La vérification doit fournir une assurance raisonnable que les modifications n'ont eu aucun impact négatif sur la sécurité du réseau et que le changement fonctionne comme prévu. Pour éviter d'avoir à résoudre les problèmes de sécurité introduits par un changement, toutes les modifications doivent être approuvées avant d'être mises en œuvre et vérifiées après la mise en œuvre du changement. Une fois les modifications approuvées et vérifiées, la documentation du réseau doit être mise à jour pour inclure lesdites modifications afin d'éviter les incohérences entre la documentation du réseau et la configuration réelle.
<b>Notes D'applicabilité</b> <p>Les modifications apportées aux connexions réseau comprennent l'ajout, la suppression ou la modification d'une connexion.</p> <p>Les modifications apportées aux configurations NSC comprennent celles liées au composant lui-même ainsi que celles affectant la manière dont il exécute sa fonction de sécurité.</p>	

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>1.2.3</b> Un ou des schémas de réseau précis sont maintenus, montrant toutes les connexions entre le CDE et les autres réseaux, y compris les réseaux sans fil.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.2.3.a</b> Examiner le ou les schémas et observer les configurations de réseau afin de vérifier qu'un ou des schémas de réseau précis existent conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.2.3.b</b> Examiner la documentation et interroger le personnel responsable afin de vérifier que le ou les schémas de réseau sont précis et mis à jour en cas de modification de l'environnement.</p>	<b>Objectif</b> Le maintien d'un ou de plusieurs schémas de réseau précis et à jour évite que les connexions et les périphériques réseau ne soient négligés et laissés involontairement non sécurisés et vulnérables à la compromission. Un ou des schémas de réseau correctement maintenus aident une entreprise à vérifier son périmètre PCI DSS en identifiant les systèmes se connectant vers et depuis le CDE.
<b>Objectif de L'approche Personnalisée</b> Une représentation des limites entre le CDE, tous les réseaux de confiance et tous les réseaux non fiables est maintenue et disponible.		<b>Bonne Pratique</b> Toutes les connexions vers et depuis le CDE doivent être identifiées, y compris les systèmes fournissant des services de sécurité, de gestion ou de maintenance aux composants système du CDE. Les entités doivent envisager d'inclure les éléments suivants dans leurs schémas de réseau : <ul style="list-style-type: none"> <li>Tous les emplacements, y compris les emplacements de vente au détail, les centres de données, les emplacements d'entreprise, les fournisseurs de cloud, etc.</li> <li>Un étiquetage clair de tous les segments du réseau.</li> <li>Tous les mesures de sécurité fournissant une segmentation, y compris des identifiants uniques pour chaque mesure (par exemple, le nom de la mesure, la marque, le modèle et la version).</li> <li>Tous les composants systèmes concernés, y compris les NSC, les pare-feux d'applications Web, les solutions anti-programmes malveillants, les solutions de gestion des modifications, les systèmes IDS/IPS, les systèmes d'agrégation de journaux, les terminaux de paiement, les applications de paiement, les HSM, etc.</li> </ul> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Un ou des schémas de réseau actuels ou une autre solution technique ou topologique qui identifie les connexions réseau et les périphériques peuvent être utilisés pour satisfaire à cette exigence.</p>	<ul style="list-style-type: none"> <li>• Un étiquetage clair de toutes les zones classées hors périmètre PCI DSS sur le schéma via une case ombrée ou un autre mécanisme.</li> <li>• La date de la dernière mise à jour et les noms des personnes qui ont effectué et approuvé les mises à jour.</li> <li>• Une légende ou une clé pour expliquer le schéma.</li> </ul> <p>Les schémas doivent être mis à jour par un personnel autorisé afin de s'assurer que lesdits schémas continuent de fournir une description précise du réseau.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.2.4</b> Un ou des diagrammes de flux de données précis sont maintenus et répondent aux critères suivants :</p> <ul style="list-style-type: none"> <li>• Affiche tous les flux de données de carte à travers tous les systèmes et les réseaux.</li> <li>• Mis à jour au besoin lors de modifications apportées à l'environnement.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.2.4.a</b> Examiner le ou les diagrammes de flux de données et interroger le personnel afin de vérifier que le ou les diagrammes affichent tous les flux de données de carte conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.2.4.b</b> Examiner la documentation et interroger le personnel responsable afin de vérifier que le ou les diagrammes de flux de données sont précis et mis à jour en cas de modification de l'environnement.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Une représentation de toutes les transmissions de données de carte entre les composants système et à travers les segments de réseau est maintenue et disponible.</p>	<p><b>Objectif</b></p> <p>Un diagramme de flux de données à jour et facilement disponible aide une entreprise à comprendre et à suivre le périmètre de son environnement en montrant la façon dont les données de carte circulent sur les réseaux et entre les systèmes et les appareils individuels.</p> <p>Le maintien à jour d'un ou de plusieurs diagrammes de flux de données évite que les données de carte ne soient ignorées et laissées involontairement non sécurisées.</p> <p><b>Bonne Pratique</b></p> <p>Le diagramme de flux de données doit inclure tous les points de connexion où les données de carte sont reçues et envoyées hors du réseau, y compris les connexions aux réseaux publics ouverts, les flux de traitement des applications, le stockage, les transmissions entre les systèmes et les réseaux, ainsi que les sauvegardes de fichiers.</p> <p>Le diagramme de flux de données est censé s'ajouter au diagramme de réseau et devrait concorder avec ce dernier et le compléter. Comme Bonne Pratique, les entités peuvent envisager d'inclure les éléments suivants dans leurs diagrammes de flux de données :</p> <ul style="list-style-type: none"> <li>• Tous les flux de traitement des données de carte, y compris l'autorisation, la télécollecte/ la remise de la compensation, le règlement, les impayés et les remboursements.</li> <li>• Tous les canaux d'acceptation distincts, y compris avec carte, sans carte et le commerce électronique.</li> <li>• Tous les types de réception ou de transmission de données, y compris celles impliquant des supports papier.</li> </ul> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Un ou des diagrammes de flux de données ou une autre solution technique ou topologique qui identifie les flux de données de carte à travers les systèmes et les réseaux peuvent être utilisés pour répondre à la présente exigence.</p>	<ul style="list-style-type: none"> <li>Le flux de données de carte depuis le point où elles entrent dans l'environnement jusqu'à leur destination finale.</li> <li>Où les données de carte sont transmises et traitées, où elles sont stockées et si le stockage est à court ou à long terme.</li> <li>La source de toutes les données de carte reçues (par exemple, clients, tiers, etc.) et toutes les entités avec lesquelles les données de carte sont partagées.</li> <li>La date de la dernière mise à jour et les noms des personnes qui ont effectué et approuvé les mises à jour.</li> </ul>
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.2.5</b> Tous les services, protocoles et ports autorisés sont identifiés, approuvés et ont un besoin métier défini.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.2.5.a</b> Examiner la documentation afin de vérifier qu'il existe une liste de tous les services, protocoles et ports autorisés, y compris la justification métier et l'approbation de chacun desdits services.</p> <p><b>1.2.5.b</b> Examiner les paramètres de configuration des NSC afin de vérifier que seuls les services, protocoles et ports approuvés sont utilisés.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un trafic réseau non autorisé (services, protocoles ou paquets destinés à des ports spécifiques) ne peut pas entrer ou sortir du réseau.</p>	<p><b>Objectif</b> Des compromissions surviennent souvent en raison de services (par exemple, telnet et FTP), de protocoles et de ports inutilisés ou non sécurisés, car ceux-ci peuvent entraîner l'ouverture de points d'accès inutiles dans le CDE. Par ailleurs, les services, protocoles et ports activés mais non utilisés sont souvent négligés et laissés non sécurisés et non corrigés. En identifiant les services, protocoles et ports nécessaires à l'activité, les entités peuvent garantir que tous les autres services, protocoles et ports sont désactivés ou éliminés.</p> <p><b>Bonne Pratique</b> Le risque de sécurité associé à chaque service, protocole et port autorisé doit être compris. Les approbations doivent être accordées par un personnel indépendant de ceux qui gèrent la configuration. Le personnel d'approbation doit posséder les connaissances et la responsabilité nécessaires pour prendre des décisions d'approbation.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>1.2.6</b> Les fonctionnalités de sécurité sont définies et mises en œuvre pour tous les services, protocoles et ports utilisés et considérés comme non sécurisés, de sorte que le risque soit atténué.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.2.6.a</b> Examiner la documentation qui identifie tous les services, protocoles et ports non sécurisés utilisés afin de vérifier que pour chacun, des dispositifs de sécurité sont définis pour atténuer le risque.</p> <p><b>1.2.6.b</b> Examiner les paramètres de configuration des NSC afin de vérifier que les dispositifs de sécurité définies sont mis en œuvre pour chaque service, protocole et port identifié comme non sécurisé.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les risques spécifiques associés à l'utilisation de services, de protocoles et de ports non sécurisés sont compris, évalués et atténués de manière adéquate.</p>	<b>Objectif</b> Les compromissions profitent des configurations réseau non sécurisées. <b>Bonne Pratique</b> Si des services, protocoles ou ports non sécurisés sont nécessaires à l'activité de l'entreprise, le risque posé par ces services, protocoles et ports doit être clairement compris et accepté par l'entreprise, l'utilisation du service, du protocole ou du port doit être justifiée, et les dispositifs de sécurité qui atténuent le risque d'utilisation de ces services, protocoles et ports doivent être définies et mises en œuvre par l'entité. <b>Informations Complémentaires</b> Pour des directives sur les services, protocoles ou ports considérés comme non sécurisés, se référer aux standards et conseils du secteur (par exemple, de NIST, ENISA, OWASP).

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>1.2.7</b> Les configurations des NSC sont revues au moins une fois tous les six mois pour confirmer qu'elles sont pertinentes et efficaces.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.2.7.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour l'examen des configurations des NSC au moins une fois tous les six mois.</p> <p><b>1.2.7.b</b> Examiner la documentation relative aux configurations pour les NSC et interroger le personnel responsable afin de vérifier que les revues ont lieu au moins une fois tous les six mois.</p> <p><b>1.2.7.c</b> Examiner les configurations des NSC afin de vérifier que les configurations identifiées comme n'étant plus appuyées par une justification métier sont supprimées ou mises à jour.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les configurations NSC qui autorisent ou limitent l'accès aux réseaux de confiance sont vérifiées périodiquement afin de s'assurer que seules les connexions autorisées par une justification métier actuelle sont autorisées.</p>	<b>Objectif</b> Un tel examen donne à l'entreprise la possibilité de nettoyer toutes les règles et configurations inutiles, obsolètes ou incorrectes qui pourraient être utilisées par une personne non autorisée. En outre, il garantit que toutes les règles et configurations n'autorisent que les services, protocoles et ports autorisés qui correspondent aux justifications métier documentées. <b>Bonne Pratique</b> Cette revue, qui peut être mise en œuvre grâce à de méthodes manuelles, automatisées ou basées sur le système, est destinée à confirmer que les paramètres qui gèrent les règles de trafic, ce qui est autorisé dans et hors du réseau, correspondent aux configurations approuvées. La revue doit fournir la confirmation que tout accès autorisé a une raison métier justifiée. Toute déviation ou incertitude concernant une règle ou une configuration doit être signalée pour résolution. Bien que cette exigence spécifie que cette revue a lieu au moins une fois tous les six mois, les entreprises avec un volume élevé de changements de leurs configurations réseau peuvent envisager d'effectuer des revues plus fréquemment afin de s'assurer que les configurations continuent de répondre aux besoins métier.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.2.8</b> Les fichiers de configuration des NSC sont comme suit :</p> <ul style="list-style-type: none"> <li>• Sécurisés contre les accès non autorisés.</li> <li>• Maintenus cohérents avec les configurations de réseau actives.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.2.8</b> Examiner les fichiers de configuration des NSC afin de vérifier qu'ils sont conformes à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les NSC ne peuvent pas être définis ou modifiés en utilisant des objets de configuration non fiables (y compris des fichiers).</p>	<p><b>Objectif</b> Afin de prévenir l'application de configurations non autorisées au réseau, les fichiers stockés avec des configurations réseau doivent être tenus à jour et protégés contre les modifications non autorisées.</p> <p>Le maintien des informations de configuration à jour et sécurisées garantit que les paramètres corrects pour les NSC sont appliqués chaque fois que la configuration est exécutée.</p>
<p><b>Notes D'applicabilité</b></p> <p>Tout fichier ou paramètre utilisé pour configurer ou synchroniser les NSC est considéré « fichier de configuration ». Cela inclut les fichiers, les mesures de sécurité automatisée et les mesures de sécurité basée sur le système, les scripts, les paramètres, l'infrastructure en tant que code ou d'autres paramètres qui sont sauvegardés, archivés ou stockés à distance.</p>	<p><b>Exemples</b> Si la configuration sécurisée d'un routeur est stockée dans une mémoire non volatile, lorsque ce routeur est réinitialisé ou redémarré, ces mesures de sécurité doivent garantir que sa configuration sécurisée a été rétablie.</p>

Exigences et Procédures de Test	Directives
<b>1.3 L'accès au réseau vers et depuis l'environnement de données du titulaire de carte est restreint.</b>	
<b>Exigences de L'approche Définie</b> <p><b>1.3.1</b> Le trafic entrant vers le CDE est limité comme suit :</p> <ul style="list-style-type: none"> <li>• Seul le trafic qui est nécessaire.</li> <li>• Tout autre trafic est spécifiquement refusé.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.3.1.a</b> Examiner les standards de configuration des NSC afin de vérifier qu'elles définissent la restriction du trafic entrant vers le CDE conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.3.1.b</b> Examiner les configurations des NSC afin de vérifier que le trafic entrant vers le CDE est limité conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le trafic non autorisé ne peut pas entrer dans le CDE.</p>	<b>Objectif</b> Cette exigence vise à empêcher les individus malveillants d'accéder au réseau de l'entité via des adresses IP non autorisées ou d'utiliser des services, des protocoles ou des ports d'une manière non autorisée. <b>Bonne Pratique</b> Tout le trafic entrant vers le CDE, quelle que soit sa provenance, doit être évalué pour s'assurer qu'il respecte les règles établies et autorisées. Les connexions doivent être inspectées pour s'assurer que le trafic est limité aux seules communications autorisées, par exemple, en limitant les adresses et les ports source/destination et en bloquant le contenu. <b>Exemples</b> La mise en œuvre d'une règle qui refuse tout trafic entrant et sortant qui n'est pas spécifiquement nécessaire (par exemple, en utilisant une instruction explicite « tout refuser » ou implicite après autorisation) permet d'éviter des failles accidentelles qui permettraient un trafic involontaire et potentiellement dangereux.

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>1.3.2</b> Le trafic sortant du CDE est limité comme suit :</p> <ul style="list-style-type: none"> <li>• Seul le trafic qui est nécessaire.</li> <li>• Tout autre trafic est spécifiquement refusé.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.3.2.a</b> Examiner les standards de configuration des NSC afin de vérifier qu'elles définissent la restriction du trafic sortant du CDE conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.3.2.b</b> Examiner les configurations des NSC afin de vérifier que le trafic sortant du CDE est limité conformément à tous les éléments spécifiés dans cette exigence.</p>	<b>Objectif</b> Cette exigence vise à empêcher les individus malveillants et les composants système compromis au sein du réseau de l'entité de communiquer avec un hôte externe non fiable. <b>Bonne Pratique</b> Tout le trafic sortant du CDE, quelle que soit sa destination, doit être évalué pour s'assurer qu'il respecte les règles établies et autorisées. Les connexions doivent être inspectées pour limiter le trafic aux seules communications autorisées, par exemple, en limitant les adresses et les ports source/destination et en bloquant le contenu. <b>Exemples</b> La mise en œuvre d'une règle qui refuse tout trafic entrant et sortant qui n'est pas spécifiquement nécessaire (par exemple, en utilisant une instruction explicite « tout refuser » ou implicite après autorisation) permet d'éviter des failles accidentelles qui permettraient un trafic involontaire et potentiellement dangereux.
<b>Objectif de L'approche Personnalisée</b> Le trafic non autorisé ne peut pas sortir du CDE.		
<b>Exigences de L'approche Définie</b> <p><b>1.3.3</b> Les NSC sont installés entre tous les réseaux sans fil et le CDE, que le réseau sans fil soit ou non un CDE, de sorte que :</p> <ul style="list-style-type: none"> <li>• Tout le trafic sans fil allant des réseaux sans fil vers le CDE est refusé par défaut.</li> <li>• Seul le trafic sans fil avec des besoins métier autorisés est autorisé à accéder au CDE.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.3.3</b> Examiner les paramètres de configuration et les schémas réseau afin de vérifier que les NSC sont mis en œuvre entre tous les réseaux sans fil et le CDE, conformément à tous les éléments spécifiés dans cette exigence.</p>	<b>Objectif</b> La mise en œuvre et l'exploitation connues (ou inconnues) de la technologie sans fil au sein d'un réseau sont une porte d'entrée courante utilisée par les individus malveillants pour accéder au réseau et aux données de carte. Si un appareil ou un réseau sans fil est installé à l'insu de l'entité, un individu malveillant pourrait facilement et « invisiblement » accéder au réseau. Si les NSC ne limitent pas l'accès des réseaux sans fil au CDE, les individus malveillants qui obtiennent un accès non autorisé au réseau sans fil peuvent facilement se connecter au CDE et compromettre les informations de compte.
<b>Objectif de L'approche Personnalisée</b> Le trafic non autorisé ne peut pas traverser les frontières du réseau entre les réseaux sans fil et les environnements câblés dans le CDE.		

Exigences et Procédures de Test	Directives
<b>1.4 Les connexions réseau entre les réseaux de confiance et les réseaux non fiables sont contrôlées.</b>	
<b>Exigences de L'approche Définie</b> <p><b>1.4.1</b> Les NSC sont mis en œuvre entre les réseaux approuvés et les réseaux non fiables.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.4.1.a</b> Examiner les standards de configuration et les schémas réseau afin de vérifier que les NSC sont définis entre les réseaux approuvés et les réseaux non fiables.</p> <p><b>1.4.1.b</b> Examiner les configurations réseau afin de vérifier que les NSC sont en place entre les réseaux de confiance et les réseaux non fiables, conformément aux standards de configuration et aux schémas de réseau documentés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le trafic non autorisé ne peut pas traverser les frontières du réseau entre les réseaux de confiance et ceux non fiables.</p>	<b>Objectif</b> La mise en œuvre de NSC à chaque connexion entrante et sortant de réseaux de confiance permet à l'entité de surveiller et de contrôler l'accès, et minimise les chances qu'un individu malveillant obtienne l'accès au réseau interne via une connexion non protégée. <b>Exemples</b> Une entité pourrait mettre en œuvre une DMZ, qui est une partie du réseau qui gère les connexions entre un réseau non fiable (pour des exemples de réseaux non fiables, se reporter à l'exigence 1 - Aperçu) et les services qu'une organisation doit mettre à la disposition du public, tels qu'un serveur Web. Veuillez noter que si la DMZ d'une entité traite ou transmet des données de carte (par exemple, un site Web de commerce électronique), elle est également considérée comme un CDE.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.4.2</b> Le trafic entrant des réseaux non fiables vers les réseaux de confiance est limité :</p> <ul style="list-style-type: none"> <li>• Aux communications avec des composants systèmes autorisés à fournir des services, des protocoles et des ports accessibles au public.</li> <li>• Aux réponses avec état aux communications initiées par les composants système dans un réseau de confiance.</li> <li>• Tout autre trafic est refusé.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.4.2</b> Examiner la documentation du fournisseur et les configurations des NSC afin de vérifier que le trafic entrant des réseaux non fiables vers les réseaux de confiance est limité conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Seul le trafic autorisé ou qui est une réponse à un composant système dans le réseau de confiance peut entrer dans un réseau de confiance à partir d'un réseau non fiable.</p>	<p><b>Objectif</b> S'assurer que l'accès public à un composant système est spécifiquement autorisé réduit le risque que les composants système soient inutilement exposés à des réseaux non fiables.</p> <p><b>Bonne Pratique</b> Les composants système qui fournissent des services accessibles au public, tels que les serveurs de messagerie, Web et DNS, sont les plus vulnérables aux menaces provenant de réseaux non fiables.</p>
<p><b>Notes D'applicabilité</b></p> <p>Le but de cette exigence est de traiter des sessions de communication entre les réseaux de confiance et les réseaux non fiables, plutôt que les spécificités des protocoles.</p> <p>Cette exigence ne limite pas l'utilisation du protocole UDP ou d'autres protocoles réseau en mode non connecté si l'état est maintenu par le NSC.</p>	<p>L'idéal est que ces systèmes soient placés dans un réseau de confiance dédié, qui soit accessible au public (par exemple, une DMZ) mais qui est séparé à l'aide de NSC des systèmes internes plus sensibles, ce qui contribue à protéger le reste du réseau au cas où ces systèmes accessibles de l'extérieur seraient compromis. Cette fonctionnalité est destinée à empêcher les personnes malveillantes d'accéder au réseau interne de l'organisation à partir d'Internet, ou d'utiliser des services, des protocoles ou des ports de manière non autorisée.</p> <p>Lorsque cette fonctionnalité est fournie en tant que caractéristique intégrée d'un NSC, l'entité doit s'assurer que ses configurations n'entraînent pas la désactivation ou le contournement de la fonctionnalité.</p> <p><b>Définitions</b> Le maintien de « l'état » (ou le statut) de chaque connexion dans un réseau signifie que le NSC « sait » si une réponse apparente à une connexion précédente est une réponse valide et autorisée (puisque le NSC conserve le statut de chaque connexion) ou s'il s'agit d'un trafic malveillant essayant de tromper le NSC pour qu'il autorise la connexion.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>1.4.3</b> Des mesures d'anti usurpation sont mises en œuvre afin de détecter et empêcher les adresses IP sources falsifiées d'entrer dans le réseau de confiance.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les paquets avec des adresses IP source falsifiées ne peuvent pas entrer dans un réseau de confiance.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>1.4.3</b> Examiner la documentation et les configurations du fournisseur pour les NSC afin de vérifier que des mesures d'anti usurpation sont mises en œuvre pour détecter et empêcher les adresses IP sources falsifiées d'entrer dans le réseau de confiance.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>1.4.4</b> Les composants système qui stockent les données des titulaires de cartes ne sont pas directement accessibles à partir de réseaux non fiables.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.4.4.a</b> Examiner le diagramme de flux de données et le schéma réseau afin de vérifier que la documentation justifie que les composants du système stockant les données des titulaires de cartes ne sont pas directement accessibles à partir des réseaux non fiables.</p> <p><b>1.4.4.b</b> Examiner les configurations des NSC afin de vérifier que les mesures de sécurité sont mises en œuvre de telle sorte que les composants du système stockant les données des titulaires de carte ne soient pas directement accessibles à partir de réseaux non fiables.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les données de titulaires de cartes stockées ne sont pas accessibles à partir de réseaux non fiables.</p>	<b>Objectif</b> <p>Les données de titulaires de cartes qui sont directement accessibles depuis un réseau non fiable, par exemple, parce qu'elles sont stockées sur un système au sein de la DMZ ou dans un service de base de données cloud, sont plus faciles d'accès par un attaquant externe car il y a moins de couches défensives à pénétrer. Il est possible d'empêcher le trafic réseau non autorisé d'atteindre le composant du système en utilisant des NSC afin de garantir que les composants système qui stockent les données des titulaires de cartes (tels qu'une base de données ou un fichier) ne soient directement accessibles qu'à partir de réseaux de confiance.</p>
<b>Notes D'applicabilité</b> <p>Cette exigence n'est pas destinée à être appliquée au stockage des données de carte dans la mémoire volatile, mais à être appliquée lorsque la mémoire est traitée comme un stockage persistant (par exemple, un disque virtuel). Les données de carte peuvent être stockées dans la mémoire volatile uniquement le temps nécessaire pour prendre en charge le processus métier associé (par exemple, jusqu'à la fin de la transaction par carte de paiement associée).</p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>1.4.5</b> La divulgation des adresses IP internes et des informations de routage est limitée aux seules parties autorisées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>1.4.5.a</b> Examiner les configurations des NSC afin de vérifier que la divulgation des adresses IP internes et des informations de routage est limitée aux seules parties autorisées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les informations du réseau interne sont protégées contre toute divulgation non autorisée.</p>	<b>Objectif</b> Limiter la divulgation des adresses IP internes, privées et locales est nécessaire afin d'empêcher un pirate d'avoir la connaissance de ces adresses IP et de les utiliser pour accéder au réseau. <b>Bonne Pratique</b> Les méthodes utilisées pour satisfaire à l'intention de cette exigence peuvent varier, selon la technologie de réseau spécifique utilisée. Par exemple, les mesures de sécurité utilisée pour répondre à cette exigence peuvent être différents pour les réseaux IPv4 et les réseaux IPv6. <b>Exemples</b> Les méthodes pour masquer l'adressage IP peuvent inclure, sans toutefois s'y limiter : <ul style="list-style-type: none"> <li>Traduction d'adresses réseau (NAT) IPv4.</li> <li>Placer les composants système derrière les serveurs proxy ou les NSC.</li> <li>Suppression ou filtrage des annonces d'itinéraire pour les réseaux internes qui utilisent un adressage enregistré.</li> <li>Utilisation interne du standard RFC 1918 (IPv4) ou utilisation de l'extension de confidentialité IPv6 (RFC 4941) lors du lancement de sessions sortantes vers Internet.</li> </ul>

Exigences et Procédures de Test	Directives
<b>1.5 Les risques pour le CDE provenant d'appareils informatiques capables de se connecter à la fois à des réseaux non fiables et au CDE sont atténués.</b>	

Exigences de L'approche Définie	Procédures de Test de L'approche Définie	Objectif
<p><b>1.5.1</b> Des mesures de sécurité sont mis en œuvre sur tous les appareils informatiques, y compris les appareils appartenant à l'entreprise et aux employés, qui se connectent à la fois aux réseaux non fiables (y compris Internet) et au CDE, de la manière suivante :</p> <ul style="list-style-type: none"> <li>Des paramètres de configuration spécifiques sont définis afin d'empêcher l'introduction de menaces dans le réseau de l'entité.</li> <li>Les mesures de sécurité sont activées et en cours d'exécution.</li> <li>Les mesures de sécurité ne sont pas modifiables par les utilisateurs des appareils informatiques, à moins qu'ils ne soient spécifiquement documentés et autorisés par la direction au cas par cas pour une période limitée.</li> </ul>	<p><b>1.5.1.a</b> Examiner les politiques et les standards de configuration et interroger le personnel afin de vérifier que les mesures de sécurité de sécurité pour les appareils informatiques qui se connectent à la fois aux réseaux non fiables et au CDE, sont mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>1.5.1.b</b> Examiner les paramètres de configuration sur les appareils informatiques qui se connectent à la fois aux réseaux non fiables et au CDE afin de vérifier que les paramètres sont mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>	<p>Les appareils informatiques autorisés à se connecter à Internet de l'extérieur de l'environnement de l'entreprise (par exemple, ordinateurs de bureau, ordinateurs portables, tablettes, smartphones et autres appareils informatiques mobiles utilisés par les employés) sont plus vulnérables aux menaces Internet. L'utilisation de mesures de sécurité de sécurité tels que des mesures de sécurité basés sur l'hôte (par exemple, un logiciel de pare-feu personnel ou des solutions de protection des terminaux), des mesures de sécurité de sécurité basés sur le réseau (par exemple, des pare-feu, une inspection heuristique basée sur le réseau et une simulation de logiciels malveillants) ou du matériel, aide à protéger les appareils contre les attaques sur Internet, qui pourraient utiliser l'appareil pour accéder aux systèmes et aux données de l'entreprise lorsque l'appareil se reconnecte au réseau.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les appareils qui se connectent à des environnements non fiables et se connectent également au CDE ne peuvent pas introduire de menaces au CDE de l'entité.</p>		<p><b>Bonne Pratique</b></p> <p>Les paramètres de configuration spécifiques sont déterminés par l'entité et doivent être conformes à ses politiques et procédures de sécurité réseau. Lorsqu'il existe un besoin légitime de désactiver temporairement les mesures de sécurité de sécurité sur un appareil appartenant à l'entreprise ou à un employé qui se connecte à la fois à un réseau non fiable et au CDE, par exemple pour soutenir une activité de maintenance spécifique ou une enquête sur un problème technique, la raison pour prendre une telle mesure est comprise et approuvée par un représentant approprié de la direction.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Ces mesures de sécurité de sécurité ne peuvent être temporairement désactivés que s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si ces mesures de sécurité de sécurité doivent être désactivés dans un but précis, cette décision doit être formellement autorisée. Des mesures de sécurité supplémentaires peuvent également devoir être mises en œuvre pour la période pendant laquelle ces mesures de sécurité de sécurité ne sont pas actifs.</p> <p>Cette exigence s'applique aux appareils informatiques appartenant aux employés et à l'entreprise. Les systèmes qui ne peuvent pas être gérés par la politique de l'entreprise introduisent des faiblesses et offrent des opportunités que des individus malveillants peuvent exploiter.</p>	<p>Toute désactivation ou modification de ces mesures de sécurité de sécurité, y compris sur les propres appareils des administrateurs, est effectuée par du personnel autorisé.</p> <p>Il est reconnu que les administrateurs ont des priviléges qui peuvent leur permettre de désactiver les mesures de sécurité de sécurité sur leurs propres ordinateurs, mais des mécanismes d'alerte doivent être mis en place lorsque ces mesures de sécurité sont désactivées et un suivi est effectué pour s'assurer que les processus ont été suivis.</p> <p><b>Exemples</b></p> <p>Les pratiques incluent l'interdiction de la tunnelisation fractionnée des VPN pour les appareils mobiles appartenant aux employés ou à l'entreprise, et l'exigence que ces appareils démarrent dans un VPN.</p>

## ***Exigence 2 : Appliquer des Configurations Sécurisées à tous les Composants Système***

### **Sections**

- 2.1** Les processus et mécanismes d'application de configurations sécurisées à tous les composants système sont définis et compris.
- 2.2** Les composants système sont configurés et gérés en toute sécurité.
- 2.3** Les environnements sans fil sont configurés et gérés en toute sécurité.

### **Aperçu**

Les personnes malveillantes, à la fois externes et internes à une entité, utilisent souvent des mots de passe par défaut et d'autres paramètres par défaut du fournisseur afin de compromettre les systèmes. Ces mots de passe et paramètres sont bien connus et sont facilement déterminés via des informations publiques.

L'application de configurations sécurisées aux composants système réduit les moyens dont dispose un attaquant pour compromettre le système. La modification des mots de passe par défaut, la suppression des logiciels, fonctions et comptes inutiles et la désactivation ou la suppression de services inutiles contribuent tous à réduire le périmètre d'attaque potentielle.

Se reporter à l'[Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>2.1 Les processus et mécanismes d'application de configurations sécurisées à tous les composants système sont définis et compris.</b>	
<b>Exigences de L'approche Définie</b> <p><b>2.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 2 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 2 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les attentes, les mesures de sécurité et la surveillance des activités relatives à l'exigence 2 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<b>Objectif</b> L'exigence 2.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 2. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'Exigence 2, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées. <b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, penser à mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique. <b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>2.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 2 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>2.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 2 sont documentées et attribuées.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 2 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts.</p> <p>Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>2.2 Les composants système sont configurés et gérés en toute sécurité.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>2.2.1</b> Les standards de configuration sont élaborées, mises en œuvre et maintenues pour :</p> <ul style="list-style-type: none"> <li>• Couvrir tous les composants système.</li> <li>• Corriger toutes les vulnérabilités de sécurité connues.</li> <li>• Se conformer aux standards relatifs à la sécurité renforcée des systèmes agréés par l'industrie ou aux recommandations pour une sécurité renforcée des fournisseurs.</li> <li>• Se tenir informé des nouvelles vulnérabilités identifiées, comme défini dans l'exigence 6.3.1.</li> <li>• Être appliquées lorsque de nouveaux systèmes sont configurés et vérifiés comme étant en place avant ou immédiatement après la connexion d'un composant système à un environnement de production.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>2.2.1.a</b> Examiner les standards de configuration du système afin de vérifier qu'elles définissent des processus qui incluent tous les éléments spécifiés dans cette exigence.</p> <p><b>2.2.1.b</b> Examiner les politiques et les procédures et interroger le personnel afin de vérifier que les standards de configuration du système sont mises à jour à mesure que de nouveaux problèmes de vulnérabilité sont identifiés, comme défini dans l'exigence 6.3.1.</p> <p><b>2.2.1.c</b> Examiner les paramètres de configuration et interroger le personnel afin de vérifier que les standards de configuration du système sont appliqués lorsque de nouveaux systèmes sont configurés et vérifiés comme étant en place avant ou immédiatement après la connexion d'un composant système à un environnement de production.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Tous les composants système sont configurés de manière sécurisée et uniforme et conformément aux standards de sécurité renforcée, agréées par l'industrie ou aux recommandations des fournisseurs.</p>	<p><b>Objectif</b></p> <p>Il existe des faiblesses connues touchant de nombreux systèmes d'exploitation, bases de données, périphériques réseau, logiciels, applications, images conteneurs et autres périphériques utilisés par une entité ou dans l'environnement d'une entité. Il existe également des moyens connus de configurer ces composants système afin de corriger les failles de sécurité. La correction des vulnérabilités de sécurité réduit les opportunités disponibles pour un attaquant.</p> <p>En élaborant des standards, les entités s'assurent que leurs composants système seront configurés de manière uniforme et sécurisée, et répondent à la protection des appareils pour lesquels une sécurité renforcée complète peut être plus difficile.</p> <p><b>Bonne Pratique</b></p> <p>Se tenir au courant des directives actuelles de l'industrie aidera l'entité à maintenir des configurations sécurisées.</p> <p>Les mesures de sécurité spécifiques à appliquer à un système varieront et devraient être adaptés au type et à la fonction du système.</p> <p>De nombreuses entreprises de sécurité ont établi des directives et des recommandations visant une sécurité renforcée des systèmes, qui indiquent comment corriger les failles courantes et connues.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p><b>Informations Complémentaires</b></p> <p>Les sources de conseils sur les standards de configuration incluent, sans toutefois s'y limiter : Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance et les fournisseurs de produits.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>2.2.2</b> Les comptes par défaut du fournisseur sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>• Si le ou les comptes par défaut du fournisseur sont utilisés, le mot de passe par défaut est modifié conformément à l'exigence 8.3.6.</li> <li>• Si le ou les comptes par défaut du fournisseur ne sont pas utilisés, le compte est supprimé ou désactivé.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>2.2.2.a</b> Examiner les standards de configuration du système afin de vérifier qu'elles incluent la gestion des comptes par défaut des fournisseurs conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>2.2.2.b</b> Examiner la documentation du fournisseur et observer un administrateur système se connecter à l'aide des comptes par défaut du fournisseur pour vérifier que les comptes sont mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>2.2.2.c</b> Examiner les fichiers de configuration et interroger le personnel afin de vérifier que tous les comptes par défaut du fournisseur qui ne seront pas utilisés sont supprimés ou désactivés.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les composants système ne sont pas accessibles par des mots de passe par défaut.</p>	<p><b>Objectif</b> Les personnes malveillantes utilisent souvent les noms de compte et les mots de passe par défaut des fournisseurs afin de compromettre les systèmes d'exploitation, les applications et les systèmes sur lesquels ils sont installés. Étant donné que ces paramètres par défaut sont souvent publiés et bien connus, leur modification rendra les systèmes moins vulnérables aux attaques.</p> <p><b>Bonne Pratique</b> Tous les comptes par défaut des fournisseurs doivent être identifiés, et leur objectif et leur utilisation compris. Il est important d'établir des mesures de sécurité pour les comptes d'application et système, y compris ceux utilisés pour déployer et maintenir les services cloud afin qu'ils n'utilisent pas de mots de passe par défaut et ne soient pas utilisables par des personnes non autorisées.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cela s'applique à TOUS les comptes et mots de passe par défaut des fournisseurs, y compris, sans toutefois s'y limiter, ceux utilisés avec des valeurs par défaut par les systèmes d'exploitation, les logiciels qui fournissent des services de sécurité, les comptes d'application et système, les terminaux de point de vente (POS), les applications de paiement et le Protocole simplifié de gestion de réseau (SNMP).</p> <p>Cette exigence s'applique également lorsqu'un composant système n'est pas installé dans l'environnement d'une entité ; par exemple, des logiciels et des applications qui font partie du CDE et qui sont accessibles via un service d'abonnement cloud.</p>	<p>Lorsqu'un compte par défaut n'est pas destiné à être utilisé, changer le mot de passe par défaut en un mot de passe unique qui répond à l'exigence 8.3.6 du standard PCI DSS, supprimer tout accès au compte par défaut, puis désactiver le compte, empêchera une personne malveillante d'activer le compte et l'accès avec le mot de passe par défaut.</p> <p>L'utilisation d'un réseau intermédiaire isolé pour installer et configurer de nouveaux systèmes est recommandée et peut également être utilisée afin de confirmer que les informations d'identification par défaut n'ont pas été introduites dans les environnements de production.</p> <p><b>Exemples</b> Les valeurs par défaut à prendre en compte comportent les identifiants utilisateur, les mots de passe et d'autres informations d'authentification couramment utilisées par les fournisseurs dans leurs produits.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>2.2.3</b> Les fonctions principales nécessitant différents niveaux de sécurité sont gérées de la manière suivante :</p> <ul style="list-style-type: none"> <li>• Une seule fonction principale existe sur un composant système,</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• Les fonctions principales avec des niveaux de sécurité différents qui existent sur le même composant système sont isolées les unes des autres,</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• Les fonctions principales avec des niveaux de sécurité différents sur le même composant système sont toutes sécurisées au niveau exigé par la fonction ayant le besoin de sécurité le plus élevé.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>2.2.3.a</b> Examiner les standards de configuration du système afin de vérifier qu'elles incluent la gestion des fonctions principales nécessitant différents niveaux de sécurité, tel que spécifié dans cette exigence.</p> <p><b>2.2.3.b</b> Examiner les configurations du système afin de vérifier que les fonctions principales nécessitant différents niveaux de sécurité sont gérées selon l'une des façons spécifiées dans cette exigence.</p> <p><b>2.2.3.c</b> Lorsque des technologies de virtualisation sont utilisées, examiner les configurations système afin de vérifier que les fonctions système nécessitant différents niveaux de sécurité sont gérées de l'une des manières suivantes :</p> <ul style="list-style-type: none"> <li>• Des fonctions ayant des besoins de sécurité différents ne coexistent pas sur le même composant système.</li> <li>• Les fonctions avec des besoins de sécurité différents qui existent sur le même composant système sont isolées les unes des autres.</li> <li>• Les fonctions avec des besoins de sécurité différents sur le même composant système sont toutes sécurisées au niveau exigé par la fonction ayant le besoin de sécurité le plus élevé.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les fonctions principales avec des besoins de sécurité inférieurs ne peuvent pas avoir une incidence sur la sécurité des fonctions principales avec des besoins de sécurité plus élevés sur le même composant système.</p>	<p><b>Objectif</b></p> <p>Les systèmes contenant une combinaison de services, de protocoles et de démons pour leur fonction principale auront un profil de sécurité approprié pour permettre à cette fonction d'être efficace. Par exemple, les systèmes qui doivent être directement connectés à Internet auraient un profil particulier, tels qu'un serveur DNS, un serveur Web ou un serveur de commerce électronique. A l'inverse, d'autres composants du système peuvent exécuter une fonction principale comprenant un ensemble différent de services, de protocoles et de démons qui exécute des fonctions qu'une entité ne souhaite pas exposer sur Internet. Cette exigence vise à garantir que différentes fonctions n'ont aucun impact sur les profils de sécurité d'autres services d'une manière qui pourrait les amener à fonctionner à un niveau de sécurité supérieur ou inférieur.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p><b>Bonne Pratique</b></p> <p>Il serait idéal que chaque fonction soit placée sur différents composants système. Ceci peut être réalisé en mettant en œuvre une fonction principale unique sur chaque composant système. Une autre option consiste à isoler les fonctions principales sur le même composant système qui ont différents niveaux de sécurité ; par exemple, en isolant les serveurs Web (qui doivent être directement connectés à Internet) des serveurs d'applications et de bases de données.</p> <p>Si un composant système contient des fonctions principales qui nécessitent des niveaux de sécurité différents, une troisième option consiste à mettre en œuvre des mesures de sécurité supplémentaires afin de garantir que le niveau de sécurité résultant de la ou des fonctions principales ayant des besoins de sécurité plus élevés n'est pas réduit par la présence des fonctions principales de niveau de sécurité inférieure. Par ailleurs, les fonctions ayant un niveau de sécurité inférieur doivent être isolées et/ou sécurisées afin de s'assurer qu'elles ne peuvent pas accéder ou nuire aux ressources d'une autre fonction du système, et n'introduisent pas de failles de sécurité pour d'autres fonctions sur le même serveur.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Les fonctions de niveaux de sécurité différents peuvent être isolées par des mesures de sécurité physiques ou logiques. Par exemple, un système de base de données ne doit pas également héberger des services Web, à moins d'utiliser des mesures de sécurité tels que des technologies de virtualisation pour isoler et contenir les fonctions dans des sous-systèmes distincts. Un autre exemple consiste à utiliser des instances virtuelles ou à fournir un accès mémoire dédié par fonction système.</p> <p>Lorsque des technologies de virtualisation sont utilisées, les niveaux de sécurité doivent être identifiés et gérés pour chaque composant virtuel. Ci-dessous des exemples de considérations pour les environnements virtualisés :</p> <ul style="list-style-type: none"> <li>• La fonction de chaque instance d'application, de conteneur ou de serveur virtuel.</li> <li>• Comment les machines virtuelles (VM) ou les conteneurs sont stockés et sécurisés.</li> </ul>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>2.2.4</b> Seuls les services, protocoles, démons et fonctions nécessaires sont activés et toutes les fonctionnalités inutiles sont supprimées ou désactivées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.2.4.a</b> Examiner les standards de configuration du système afin de vérifier que les services, les protocoles, les démons et les fonctions nécessaires sont identifiés et documentés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les composants système ne peuvent pas être compromis en exploitant les fonctionnalités inutiles présentes dans le composant système.</p>	<p><b>2.2.4.b</b> Examiner les configurations des composants système afin de vérifier les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Toutes les fonctionnalités inutiles sont supprimées ou désactivées.</li> <li>• Seules les fonctionnalités requises, comme celles documentées dans les standards de configuration, sont activées.</li> </ul> <p><b>Objectif</b> Des services et des fonctions inutiles peuvent offrir des opportunités supplémentaires aux personnes malveillantes d'accéder à un système. En supprimant ou en désactivant tous les services, protocoles, démons et fonctions inutiles, les entreprises peuvent se focaliser sur la sécurisation des fonctions requises et réduire le risque que des fonctions inconnues ou inutiles soient exploitées.</p> <p><b>Bonne Pratique</b> Il existe de nombreux protocoles qui pourraient être activés par défaut et qui sont couramment utilisés par des personnes malveillantes pour compromettre un réseau. La désactivation ou la suppression de tous les services, fonctions et protocoles qui ne sont pas utilisés minimise le périmètre d'attaque potentielle, par exemple en supprimant ou en désactivant un serveur FTP ou Web inutilisé.</p> <p><b>Exemples</b> Les fonctionnalités inutiles peuvent inclure, sans toutefois s'y limiter, des scripts, des pilotes, des fonctionnalités, des sous-systèmes, des systèmes de fichiers, des interfaces (USB et Bluetooth) et des serveurs Web inutiles.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>2.2.5</b> Si des services, protocoles ou démons non sécurisés sont présents :</p> <ul style="list-style-type: none"> <li>La justification métier est documentée.</li> <li>Des fonctionnalités de sécurité supplémentaires sont documentées et mises en œuvre afin de réduire le risque d'utilisation de services, de protocoles ou de démons non sécurisés.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.2.5.a</b> Si des services, protocoles ou démons non sécurisés sont présents, examiner les standards de configuration du système et interroger le personnel afin de vérifier qu'ils sont gérés et mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>2.2.5.b</b> Si des services, des protocoles ou des démons non sécurisés sont présents, examiner les paramètres de configuration afin de vérifier que des fonctionnalités de sécurité supplémentaires sont mises en œuvre pour réduire le risque d'utiliser des services, des démons et des protocoles non sécurisés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les composants système ne peuvent pas être compromis en exploitant des services, des protocoles ou des démons non sécurisés.</p>	<b>Objectif</b> La garantie que tous les services, protocoles et démons non sécurisés sont correctement sécurisés avec des fonctionnalités de sécurité adéquates rend plus difficile pour les personnes malveillantes d'exploiter les points habituels de compromission au sein d'un réseau. <b>Bonne Pratique</b> L'activation des fonctionnalités de sécurité avant le déploiement de nouveaux composants système empêchera l'introduction de configurations non sécurisées dans l'environnement. Des solutions de certains fournisseurs peuvent fournir des fonctions de sécurité supplémentaires afin d'aider à sécuriser un processus non sécurisé. <b>Informations Complémentaires</b> Pour des directives sur les services, les protocoles ou les démons considérés comme non sécurisés, se reporter aux standards et aux conseils du secteur (par exemple, tels que publiés par NIST, ENISA et OWASP).

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>2.2.6</b> Les paramètres de sécurité du système sont configurés afin d'éviter toute utilisation abusive.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.2.6.a</b> Examiner les standards de configuration du système afin de vérifier qu'elles contiennent la configuration des paramètres de sécurité du système pour éviter toute utilisation abusive.</p> <p><b>2.2.6.b</b> Interroger les administrateurs système et/ou les responsables de la sécurité afin de vérifier qu'ils connaissent les paramètres de sécurité courants pour les composants système.</p> <p><b>2.2.6.c</b> Examiner les composants du système afin de vérifier que les paramètres de sécurité courants sont définis de manière adéquate et conformément aux standards de configuration du système.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les composants système ne peuvent pas être compromis en raison d'une configuration incorrecte des paramètres de sécurité.</p>	<b>Objectif</b> La configuration correcte des paramètres de sécurité fournis dans les composants système tire parti des capacités du composant système à déjouer les attaques malveillantes. <b>Bonne Pratique</b> Les standards de configuration du système et les processus associés doivent traiter spécifiquement des réglages et paramètres de sécurité qui ont des implications de sécurité connues pour chaque type de système utilisé. Pour que les systèmes soient configurés en toute sécurité, le personnel responsable de la configuration et/ou de l'administration des systèmes doit connaître les paramètres et les réglages de sécurité spécifiques qui s'appliquent au système. Les considérations doivent également inclure des réglages sécurisés pour les paramètres utilisés afin d'accéder aux portails cloud. <b>Informations Complémentaires</b> Se reporter à la documentation du fournisseur et aux références de l'industrie notées dans l'exigence 2.2.1 afin d'obtenir des informations sur les paramètres de sécurité applicables pour chaque type de système.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>2.2.7</b> Tous les accès d'administration non-console sont chiffrés à l'aide d'une cryptographie robuste.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.2.7.a</b> Examiner les standards de configuration du système afin de vérifier qu'elles incluent le chiffrement de tous les accès administratifs non-console à l'aide d'une cryptographie robuste.</p> <p><b>2.2.7.b</b> Observer un administrateur se connecter aux composants du système et examiner les configurations du système afin de vérifier que l'accès administratif non-console est géré conformément à la présente exigence.</p> <p><b>2.2.7.c</b> Examiner les paramètres des composants du système et des services d'authentification afin de vérifier que les services de connexion à distance non sécurisés ne sont pas disponibles pour l'accès administratif non-console.</p> <p><b>2.2.7.d</b> Examiner la documentation du fournisseur et interroger le personnel afin de vérifier qu'une cryptographie robuste pour la technologie utilisée est mise en œuvre conformément aux meilleures pratiques de l'industrie et/ou aux recommandations du fournisseur.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les données permettant la connexion à des fins d'administration « en clair » ne peuvent être lues ou interceptées à partir d'aucune transmission réseau.</p>	<b>Objectif</b> Si l'administration non-console (y compris à distance) n'utilise pas de communications chiffrées, les données permettant la connexion à des fins d'administration (tels que les identifiants et les mots de passe) peuvent être révélés à une personne malveillante. Une personne malveillante pourrait utiliser ces informations pour accéder au réseau, devenir administrateur et voler des données. <b>Bonne Pratique</b> Quel que soit le protocole de sécurité utilisé, il doit être configuré pour n'utiliser que des versions et des configurations sécurisées afin d'empêcher l'utilisation d'une connexion non sécurisée ; par exemple en utilisant uniquement des certificats de confiance, en ne prenant en charge que le chiffrement robuste et en ne prenant pas en charge le recours à des protocoles ou des méthodes plus faibles et non sécurisés. <b>Exemples</b> Les protocoles « en clair » (tels que HTTP, telnet, etc.) ne chiffrent pas le trafic ou les détails de connexion, ce qui permet à une personne malveillante d'intercepter facilement ces informations. L'accès non-console peut être facilité par des technologies qui offrent un accès alternatif aux systèmes, y compris, sans toutefois s'y limiter, l'accès hors bande (OOB), lights-out management (LOM), Intelligent Platform Management Interface (IPMI), et les commutateurs écran-clavier-souris (KVM) avec capacités à distance. Celles-ci, ainsi que d'autres technologies et méthodes d'accès non-console, doivent être sécurisées par une cryptographie robuste. <b>Informations Complémentaires</b> Se reporter aux standards de l'industrie et aux meilleures pratiques telles que <i>NIST SP 800-52</i> et <i>SP 800-57</i> .
<b>Notes D'applicabilité</b> <p>Cela inclut l'accès administratif via des interfaces basées sur un navigateur et des interfaces de programmation d'applications (API).</p>	

Exigences et Procédures de Test	Directives
<b>2.3 Les environnements sans fil sont configurés et gérés en toute sécurité.</b>	
<b>Exigences de L'approche Définie</b> <p><b>2.3.1</b> Pour les environnements sans fil connectés au CDE ou transmettant des données de carte, toutes les valeurs par défaut du fournisseur sans fil sont modifiées lors de l'installation ou sont confirmées comme étant sécurisées, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Clés cryptographiques sans fil par défaut.</li> <li>• Mots de passe par défaut des points d'accès sans fil.</li> <li>• Valeurs SNMP par défaut.</li> <li>• Toute autre valeur par défaut du fournisseur sans fil liée à la sécurité.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>2.3.1.a</b> Examiner les politiques et les procédures et interroger le personnel responsable afin de vérifier que les processus sont définis pour les valeurs par défaut du fournisseur sans fil afin de les modifier lors de l'installation ou de confirmer qu'ils sont sécurisés conformément à tous les éléments de la présente exigence.</p> <p><b>2.3.1.b</b> Examiner la documentation du fournisseur et observer un administrateur système se connecter aux périphériques sans fil afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• Les valeurs SNMP par défaut ne sont pas utilisées.</li> <li>• Les mots de passe/phrases secrètes par défaut sur les points d'accès ne sont pas utilisés.</li> </ul> <p><b>2.3.1.c</b> Examiner la documentation du fournisseur et les paramètres de configuration sans fil afin de vérifier que les autres paramètres par défaut du fournisseur sans fil liés à la sécurité ont été modifiés, le cas échéant.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les réseaux sans fil ne sont pas accessibles à l'aide des mots de passe par défaut ou des configurations par défaut du fournisseur.</p>	<b>Objectif</b> Si les réseaux sans fil ne sont pas mis en œuvre avec des configurations de sécurité suffisantes (y compris la modification des paramètres par défaut), des renifleurs sans fil peuvent espionner le trafic, capturer facilement des données et des mots de passe, et accéder au, et attaquer facilement le réseau. <b>Bonne Pratique</b> Les mots de passe sans fil doivent être construits de manière à résister aux attaques par force brute hors ligne.
<b>Notes D'applicabilité</b> <p>Cela inclut, sans toutefois s'y limiter, les clés cryptographiques sans fil par défaut, les mots de passe par défaut sur les points d'accès sans fil, les valeurs SNMP par défaut et toute autre valeur par défaut du fournisseur sans fil liée à la sécurité.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>2.3.2</b> Pour les environnements sans fil connectés au CDE ou transmettant des données de carte, les clés cryptographiques sans fil sont modifiées comme suit :</p> <ul style="list-style-type: none"> <li>• Chaque fois que le personnel connaissant la clé quitte l'entreprise ou le rôle pour lequel la connaissance de la clé était nécessaire.</li> <li>• Chaque fois qu'une clé est soupçonnée ou avérée être compromise.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>2.3.2</b> Interroger le personnel responsable et examiner la documentation de gestion des clés afin de vérifier que les clés cryptographiques sans fil sont modifiées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>La connaissance des clés cryptographiques sans fil ne permet pas un accès non autorisé aux réseaux sans fil.</p>	<p><b>Objectif</b></p> <p>Le changement des clés cryptographiques sans fil chaque fois qu'une personne connaissant la clé quitte l'organisation ou passe à un rôle qui n'exige plus la connaissance de la clé, permet de limiter la connaissance des clés à ceux de l'entreprise avec besoin de les connaître.</p> <p>De plus, le changement des clés cryptographiques sans fil chaque fois qu'une clé est soupçonnée ou avérée être compromise rend un réseau sans fil plus résistant à la compromission.</p> <p><b>Bonne Pratique</b></p> <p>Cet objectif peut être atteint de plusieurs manières, y compris des changements périodiques des clés, le changement de clés via un processus défini « joiners-movers-leavers » (JML), la mise en œuvre de mesures de sécurité techniques supplémentaires et l'absence de clés pré-partagées fixes.</p> <p>De plus, toutes les clés avérées ou soupçonnées être compromises doivent être gérées conformément au plan de réponse aux incidents de l'entité à l'exigence 12.10.1.</p>

## Protéger les Données de Carte

### Exigence 3 : Protéger les Données de Carte Stockées

#### Sections

- 3.1 Les processus et mécanismes de protection des données de carte stockées sont définis et compris.
- 3.2 Le stockage des données de carte est réduit au minimum.
- 3.3 Les données d'authentification sensibles (SAD) ne sont pas stockées après autorisation.
- 3.4 L'accès à l'affichage du PAN complet et la possibilité de copier les PAN sont limités.
- 3.5 Le numéro de compte primaire (PAN) est sécurisé partout où il est stocké.
- 3.6 Les clés cryptographiques utilisées pour protéger les données de carte stockées sont sécurisées.
- 3.7 Lorsque la cryptographie est utilisée pour protéger les données de carte stockées, des processus et procédures de gestion des clés couvrant tous les aspects du cycle de vie des clés sont définis et mis en œuvre.

#### Aperçu

Les méthodes de protection telles que la cryptographie, la troncature, le masquage et le hachage sont des composants essentiels de la protection des données de carte. Si un intrus contourne d'autres mesures de sécurité de sécurité et accède aux données de carte chiffrées, les données sont illisibles sans les clés cryptographiques appropriées et sont inutilisables pour cet intrus. D'autres méthodes efficaces de protection des données stockées doivent également être envisagées comme opportunités potentielles d'atténuation des risques. Par exemple, les méthodes pour minimiser les risques consistent à ne pas stocker les données de carte sauf si cela est nécessaire, à tronquer les données du titulaire de carte si un PAN complet n'est pas nécessaire et à n'envoyer aucun PAN non protégé à l'aide de technologies de messagerie d'utilisateur final telles que le courrier électronique et la messagerie instantanée.

Si les données de carte sont présentes dans la mémoire non persistante (par exemple, RAM, mémoire volatile), le chiffrement des PAN n'est pas requis. Cependant, des mesures de sécurité appropriées doivent être en place afin de garantir que la mémoire maintient un état non persistant. Les données doivent être supprimées de la mémoire volatile une fois que l'objectif métier (par exemple, la transaction associée) est terminé. Dans le cas où le stockage de données devient persistant, toutes les exigences applicables du standard PCI DSS s'appliqueront, y compris le chiffrement des données stockées.

L'exigence 3 s'applique à la protection des données de carte stockées, sauf indication contraire dans une exigence individuelle.

Se reporter à [l'Annexe G](#) pour les définitions de « cryptographie robuste » et d'autres termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>3.1 Les processus et mécanismes de protection des données de carte stockées sont définis et compris.</b>	
<b>Exigences de L'approche Définie</b> <p><b>3.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 3 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 3 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les attentes, les mesures de sécurité et la surveillance des activités relatives à l'exigence 3 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<b>Objectif</b> L'exigence 3.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 3. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 3, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées. <b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique. <b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 3 sont documentés, attribués et compris.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 3 sont documentées et attribuées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 3 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>3.1.2.b</b> Interroger le personnel chargé d'exécuter les activités de l'exigence 3 afin de vérifier que les rôles et les responsabilités sont assignés comme documentés et qu'ils sont compris.</p> <p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives	
<b>3.2 Le stockage des données de carte est réduit au minimum.</b>		
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.2.1</b> Le stockage des données de carte est réduit au minimum grâce à la mise en œuvre de politiques, procédures et processus de conservation et d'élimination des données qui incluent au moins les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Couverture de tous les emplacements des données de carte stockées.</li> <li>• Couverture de toutes les données d'authentification sensibles (SAD) stockées avant la fin de l'autorisation. <i>Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</i></li> <li>• Limiter la quantité de stockage des données et la durée de conservation à ce qui est requis pour les exigences légales ou réglementaires et/ou métier.</li> <li>• Des exigences de rétention spécifiques pour les données de carte stockées qui définissent la durée de la période de conservation et incluent une justification métier documentée.</li> <li>• Des processus de suppression sécurisée ou pour rendre les données de carte irrécupérables lorsqu'elles ne sont plus nécessaires conformément à la politique de conservation.</li> <li>• Un processus pour vérifier, au moins une fois tous les trois mois, que les données de carte stockées dépassant la période de conservation définie ont été supprimées en toute sécurité ou rendues irrécupérables.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.2.1.a</b> Examiner les politiques, procédures et processus de conservation et d'élimination des données, et interroger le personnel afin de vérifier que les processus sont définis pour inclure tous les éléments spécifiés dans cette exigence.</p> <p><b>3.2.1.b</b> Examiner les fichiers et les enregistrements système sur les composants système dans lesquels les données de carte sont stockées afin de vérifier que la quantité de stockage des données et la durée de conservation ne dépassent pas les exigences définies dans la stratégie de conservation des données.</p> <p><b>3.2.1.c</b> Observer les mécanismes utilisés pour rendre les données de carte irrécupérables afin de vérifier que les données ne peuvent pas être récupérées.</p>	<p><b>Objectif</b></p> <p>Une politique formelle de conservation des données identifie les données qui doivent être conservées, la durée de leur conservation et le ou les emplacements où ces données résident afin qu'elles puissent être détruites ou supprimées en toute sécurité dès qu'elles ne sont plus nécessaires. Les seules données de carte qui peuvent être stockées 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.</p> <p>Le stockage des données SAD avant l'achèvement du processus d'autorisation est également inclus dans la politique de conservation et d'élimination des données afin que le stockage de ces données sensibles soit réduit au minimum et conservé uniquement pendant la durée définie.</p> <p><b>Bonne Pratique</b></p> <p>Lors de l'identification des emplacements des données de carte stockées, tenir compte de tous les processus et du personnel ayant accès aux données, car les données pourraient avoir été déplacées et stockées dans des emplacements différents de ceux définis à l'origine. Les emplacements de stockage qui sont souvent négligés incluent les systèmes de sauvegarde et d'archivage, les périphériques amovibles de stockage de données, les supports papier et les enregistrements audio.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les données du compte ne sont conservées que lorsque cela est nécessaire et pour le moins de temps nécessaire, et sont supprimées en toute sécurité ou rendues irrécupérables lorsqu'elles ne sont plus nécessaires.</p>	<p>Pour définir des exigences de conservation adéquates, une entité doit d'abord comprendre ses propres besoins métier ainsi que toutes les obligations légales ou réglementaires qui s'appliquent à son secteur ou au type de données conservées.</p> <p>La mise en œuvre d'un processus automatisé pour garantir que les données sont supprimées automatiquement et en toute sécurité, conformément à la limite de conservation définie, peut aider à garantir que les données du compte ne sont pas conservées au-delà de ce qui est nécessaire à des fins métiers, légales ou réglementaires.</p> <p>Les méthodes d'élimination des données lorsqu'elles dépassent la période de conservation comprennent la suppression sécurisée pour terminer la suppression des données ou pour les rendre irrécupérables et incapables d'être reconstruites. L'identification et l'élimination sécurisée des données stockées qui ont dépassé leur période de conservation spécifiée évitent la conservation inutile des données qui ne sont plus nécessaires. Ce processus peut être automatisé, manuel ou une combinaison des deux.</p> <p>La fonction de suppression dans la plupart des systèmes d'exploitation n'est pas une « suppression sécurisée » car elle permet de récupérer les données supprimées. Par conséquent, une fonction de suppression sécurisée dédiée ou une application doit être utilisée pour rendre les données irrécupérables.</p> <p><i>Il ne faut pas oublier que si vous n'en avez pas besoin, ne les stockez pas !</i></p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Lorsque les données de carte sont stockées par un TPSP (par exemple, dans un environnement cloud), les entités sont tenues de collaborer avec leurs prestataires de services afin de comprendre comment le TPSP satisfait à cette exigence pour l'entité. Les considérations incluent de s'assurer que toutes les instances géographiques d'un élément de données sont supprimées en toute sécurité.</p> <p><i>La point ci-dessus (concernant la couverture des SAD stockées avant l'achèvement de l'autorisation) est une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera requise dans le cadre de l'exigence 3.2.1 et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	<p><b>Exemples</b></p> <p>Une procédure automatisée et programmatique pourrait être exécutée afin de localiser et supprimer des données, ou un examen manuel des emplacements de stockage des données pourrait être effectué. Quelle que soit la méthode utilisée, c'est une bonne idée de surveiller le processus afin de s'assurer qu'il est achevé avec succès et que les résultats sont enregistrés et validés comme étant terminés. La mise en œuvre de méthodes de suppression sécurisées garantit que les données ne peuvent pas être récupérées lorsqu'elles ne sont plus nécessaires.</p> <p><b>Informations Complémentaires</b></p> <p>See <i>NIST SP 800-88 Rev. 1, Directives pour l'effacement des supports de stockage</i>.</p>

Exigences et Procédures de Test	Directives
<b>3.3 Les données d'authentification sensibles (SAD) ne sont pas stockées après autorisation.</b>	
<b>Exigences de L'approche Définie</b> <p><b>3.3.1</b> Les SAD ne sont pas stockés après autorisation, même si elles sont chiffrées. Toutes les données d'authentification sensibles reçues sont rendues irrécupérables à la fin du processus d'autorisation.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.3.1.a</b> Si des SAD sont reçues, examiner les politiques, procédures et configurations systèmes documentés afin de vérifier que les données ne sont pas stockés après autorisation.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>3.3.1.b</b> Si des SAD sont reçues, examiner les procédures documentées et observer les processus de suppression sécurisée des données afin de vérifier que les données sont rendues irrécupérables à la fin du processus d'autorisation.</p>
<b>Notes D'applicabilité</b> <p>Les émetteurs et les entreprises qui prennent en charge les services d'émission, lorsqu'il existe un besoin commercial légitime documenté de stocker les SAD ne sont pas tenus de satisfaire à cette exigence. Un besoin commercial légitime est un besoin qui est nécessaire pour l'exécution de la fonction fournie par et pour l'émetteur.</p> <p>Se reporter à l'exigence 3.3.3 pour des exigences supplémentaires élaborées spécifiquement pour ces entités.</p> <p>Les données d'authentification sensibles incluent les données citées dans les exigences 3.3.1.1 à 3.3.1.3.</p>	<b>Objectif</b> <p>Les SAD sont très précieuses pour les personnes malveillantes car elles leur permettent de générer des cartes de paiement contrefaites et de créer des transactions frauduleuses. Par conséquent, le stockage des SAD à l'issue de l'achèvement du processus d'autorisation est interdit.</p> <p><b>Bonne Pratique</b></p> <p>Il peut être acceptable pour une entité de stocker les SAD en mémoire non-permanente pendant une courte durée une fois l'autorisation terminée, si les conditions suivantes sont satisfaites :</p> <ul style="list-style-type: none"> <li>• Il y a un besoin commercial légitime d'accéder aux SAD en mémoire une fois l'autorisation terminée.</li> <li>• Les SAD sont uniquement stockées en mémoire non-permanente (par exemple, RAM, mémoire volatile).</li> <li>• Des mesures sont en place pour s'assurer que la mémoire conserve un état non-permanent.</li> <li>• Les SAD sont supprimées dès que le but commercial est atteint.</li> </ul> <p>Il n'est pas permis de stocker les SAD en mémoire permanente</p> <p><b>Définitions</b></p> <p>Lorsqu'un commerçant reçoit une réponse à la demande d'autorisation (par exemple, une approbation ou un refus).</p> <p>Se reporter à l'Annexe G pour la définition de « l'autorisation. »</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.3.1.1</b> Le contenu complet d'une piste n'est pas stocké à la fin du processus d'autorisation.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p> <p><b>Notes D'applicabilité</b></p> <p>Dans le cours normal des activités, les éléments de données suivants de la piste peuvent devoir être conservés :</p> <ul style="list-style-type: none"> <li>• Le Nom du titulaire de carte.</li> <li>• Le Numéro de compte primaire (PAN).</li> <li>• La Date d'expiration.</li> <li>• Le Code de service.</li> </ul> <p>Pour minimiser les risques, ne stocker en toute sécurité que ces éléments de données nécessaires à l'activité.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.3.1.1</b> Examiner les sources de données afin de vérifier que le contenu complet d'une piste n'est pas stocké à la fin du processus d'autorisation.</p> <p><b>Objectif</b></p> <p>Si le contenu complet d'une piste (de la piste magnétique au dos d'une carte si elle est présente, des données équivalentes contenues sur un point ou ailleurs) est stocké, des personnes malveillantes qui obtiennent ces données peuvent les utiliser pour reproduire des cartes de paiement et effectuer des transactions frauduleuses.</p> <p><b>Définitions</b></p> <p>Les données complètes d'une piste sont également appelées données de piste complète, de piste, de piste 1, de piste 2 et de piste magnétique. Chaque piste contient un certain nombre d'éléments de données, et cette exigence spécifie uniquement ceux qui peuvent être conservés après l'autorisation.</p> <p><b>Exemples</b></p> <p>Les sources de données à examiner pour s'assurer que le contenu complet d'une piste n'est pas conservé à la fin du processus d'autorisation comprennent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Les données de transaction entrantes.</li> <li>• Tous les journaux (par exemple, transaction, historique, débogage, erreur).</li> <li>• Les fichiers d'historique.</li> <li>• Les fichiers de trace.</li> <li>• Les schémas de base de données.</li> <li>• Les contenus de bases de données et les emplacements de stockage sur site (on-premise) et dans le cloud.</li> <li>• Tout fichier existant de type dump mémoire / crash dump.</li> </ul>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.3.1.2</b> Le code de vérification de la carte n'est pas stocké à la fin du processus d'autorisation.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.3.1.2</b> Examiner les sources de données afin de vérifier que le code de vérification de la carte n'est pas stocké à la fin du processus d'autorisation.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<b>Objectif</b> Si les données du code de vérification de la carte sont volées, des personnes malveillantes peuvent exécuter des transactions frauduleuses sur Internet et par correspondance ou via commande téléphonique (MO/TO). Le fait de ne pas stocker ces données réduit la probabilité qu'elles soient compromises.
<b>Notes D'applicabilité</b> <p>Le code de vérification de la carte est le numéro à trois ou quatre chiffres imprimés au recto ou au verso d'une carte de paiement utilisée pour vérifier les transactions sans carte présente.</p>	<b>Exemples</b> Si les codes de vérification des cartes sont stockés sur un support papier avant la fin de l'autorisation, une méthode d'effacement ou de recouvrement des codes devrait empêcher leur lecture une fois l'autorisation expirée. Des exemples de méthodes pour rendre les codes illisibles incluent la suppression du code avec des ciseaux et l'application d'un marqueur convenablement opaque et indélébile sur le code. Les sources de données à examiner pour s'assurer que le code de vérification de la carte n'est pas conservé à la fin du processus d'autorisation comprennent, sans toutefois s'y limiter : <ul style="list-style-type: none"> <li>• Les données de transaction entrantes.</li> <li>• Tous les journaux (par exemple, transaction, historique, débogage, erreur).</li> <li>• Les fichiers d'historique.</li> <li>• Les fichiers de trace.</li> <li>• Les schémas de base de données.</li> <li>• Les contenus de bases de données et les emplacements de stockage sur site (on-premise) et dans le cloud.</li> <li>• Tout fichier existant de type dump mémoire / crash dump.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.3.1.3</b> Le numéro d'identification personnel (PIN) et le bloc PIN ne sont pas stockés à la fin du processus d'autorisation.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p> <p><b>Notes D'applicabilité</b></p> <p>Les blocs PIN sont chiffrés au cours du déroulement naturel des processus de transaction ; cependant, même si une entité chiffre à nouveau le bloc PIN, il n'est toujours pas autorisé à être stocké après l'achèvement du processus d'autorisation.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.3.1.3</b> Examiner les sources de données afin de vérifier que les codes PIN et blocs PIN ne sont pas stockés à la fin du processus d'autorisation.</p> <p><b>Objectif</b></p> <p>Les codes PIN et les blocs PIN ne doivent être connus que du propriétaire de la carte ou de l'entité qui a émis la carte. Si ces données sont volées, des personnes malveillantes peuvent exécuter des transactions frauduleuses basées sur un code PIN (par exemple, des achats en magasin et des retraits aux guichets automatiques). Le fait de ne pas stocker ces données réduit la probabilité qu'elles soient compromises.</p> <p><b>Exemples</b></p> <p>Les sources de données à examiner pour s'assurer que les codes et les blocs PIN ne sont pas conservés à la fin du processus d'autorisation comprennent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Les données de transaction entrantes.</li> <li>• Tous les journaux (par exemple, transaction, historique, débogage, erreur).</li> <li>• Les fichiers d'historique.</li> <li>• Les fichiers de traçé.</li> <li>• Les schémas de base de données.</li> <li>• Les contenus de bases de données et les emplacements de stockage sur site (on-premise) et dans le cloud.</li> <li>• Tout fichier existant de type dump mémoire / crash dump.</li> </ul>

## Exigences et Procédures de Test

## Directives

### Exigences de L'approche Définie

**3.3.2** Les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation sont chiffrées à l'aide d'une cryptographie robuste.

### Objectif de L'approche Personnalisée

Cette exigence n'est pas admissible pour l'approche personnalisée.

### Notes D'applicabilité

Que les SAD soient permises d'être stockées avant l'autorisation est déterminée par les entreprises qui gèrent les programmes de conformité (par exemple, les réseaux internationaux et les acquéreurs). Contacter ces entreprises pour tout critère supplémentaire.

Cette exigence s'applique à tous les stockages de SAD, même si aucun PAN n'est présent dans l'environnement.

Se reporter à l'exigence 3.2.1 pour une exigence supplémentaire qui s'applique si les SAD sont stockées avant l'achèvement de l'autorisation.

Les émetteurs et les entreprises qui prennent en charge les services d'émission, lorsqu'il existe une justification commercial légitime d'émission pour stocker les SAD. Ne sont pas tenus de satisfaire à cette exigence. Un besoin commercial légitime est un besoin qui est nécessaire pour l'exécution de la fonction fournie par ou pour l'émetteur.

Se reporter à l'exigence 3.3.3 pour les exigences élaborées spécifiquement pour ces entités.

Cette exigence ne remplace pas la façon dont les blocs PIN doivent être gérés, ni ne signifie qu'un bloc PIN correctement chiffré doit être à nouveau chiffré.

(suite à la page suivante)

### Procédures de Test de L'approche Définie

**3.3.2** Examiner les magasins de données, les configurations système et/ou la documentation du fournisseur afin de vérifier que toutes les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation sont chiffrées à l'aide d'une cryptographie robuste.

### Objectif

Les SAD peuvent être utilisées par des personnes malveillantes afin d'augmenter la probabilité de réussir à générer des cartes de paiement contrefaites et de passer des transactions frauduleuses.

### Bonne Pratique

Les entités doivent envisager de chiffrer les SAD à l'aide d'une clé cryptographique différente de celle utilisée pour chiffrer le PAN. Notez que cela ne signifie pas que le PAN présent dans les SAD (dans le cadre des données de la piste) devrait être chiffré séparément.

### Définitions

Le processus d'autorisation est terminé lorsqu'un commerçant reçoit une réponse de transaction, (par exemple, une approbation ou un rejet).

Se reporter à l'Annexe G pour la définition d'« Autorisation. »

Exigences et Procédures de Test	Directives
<p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.3.3 Exigence supplémentaire pour les émetteurs et les entreprises qui prennent en charge les services d'émission et stockent des données d'authentification sensibles</b> : Tout stockage de données d'authentification sensibles est :</p> <ul style="list-style-type: none"> <li>• Limité à ce qui est nécessaire pour un besoin métier d'émission légitime, et est sécurisé.</li> <li>• Chiffré à l'aide d'une cryptographie robuste. Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.3.3.a Procédure de test supplémentaire pour les émetteurs et les entreprises qui prennent en charge les services d'émission et stockent des données d'authentification sensibles</b> : Examiner les politiques documentées et interroger le personnel afin de vérifier qu'il existe une justification métier documentée pour le stockage des données d'authentification sensibles.</p> <p><b>3.3.3.b Procédure de test supplémentaire pour les émetteurs et les entreprises qui prennent en charge les services d'émission et stockent des données d'authentification sensibles</b> : Examiner les magasins de données et les configurations système afin de vérifier que les données d'authentification sensibles sont stockées de manière sécurisée.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les données d'authentification sensibles ne sont conservées que si cela est nécessaire pour assurer les fonctions d'émission, et sont protégées contre tout accès non autorisé.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b> Les SAD peuvent être utilisées par des personnes malveillantes afin d'augmenter la probabilité de réussir à générer des cartes de paiement contrefaites et de réaliser des transactions frauduleuses.</p> <p><b>Bonne Pratique</b> Les entités doivent envisager de chiffrer les SAD à l'aide d'une clé cryptographique différente de celle utilisée pour chiffrer le PAN. Notez que cela ne signifie pas que le PAN présent dans les SAD (dans le cadre des données de la piste) devrait être chiffré séparément.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique uniquement aux émetteurs et aux entreprises qui prennent en charge les services d'émission et stockent des données d'authentification sensibles.</p> <p>Les entités qui émettent des cartes de paiement ou qui exécutent ou prennent en charge des services d'émission créent et contrôlent souvent des données d'authentification sensibles dans le cadre de la fonction d'émission. Il est permis aux entreprises qui exécutent, facilitent ou prennent en charge des services d'émission de stocker des données d'authentification sensibles UNIQUEMENT SI elles ont un besoin métier légitime de stocker ces données.</p> <p>Un besoin commercial légitime d'émission est un besoin qui est nécessaire à l'exécution de la fonction fournie par ou pour l'émetteur.</p> <p><i>La point ci-dessus (pour chiffrer les SAD stockées avec une cryptographie robuste) est une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire dans le cadre de l'exigence 3.3.3 et doit être pleinement prise en compte lors d'une évaluation PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>3.4 L'accès aux affichages du PAN complet et la possibilité de copier le PAN sont limités.</b>	
<b>Exigences de L'approche Définie</b> <p><b>3.4.1</b> Le PAN est masqué lorsqu'il est affiché (le BIN et les quatre derniers chiffres <b>sont le nombre maximum</b> de chiffres à afficher), de sorte que seul le personnel ayant un besoin métier légitime peut voir <b>plus que</b> le BIN et les quatre derniers chiffres du PAN.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.4.1.a</b> Examiner les politiques et procédures documentées pour masquer l'affichage des PAN afin de vérifier que :</p> <ul style="list-style-type: none"> <li>Une liste des rôles qui ont besoin d'accéder à plus que le BIN et les quatre derniers chiffres du PAN (y compris le PAN complet) est documentée, ainsi qu'un besoin métier légitime pour chaque rôle d'avoir un tel accès.</li> <li>Le PAN est masqué lorsqu'il est affiché de telle sorte que seul le personnel ayant un besoin métier légitime puisse voir plus que le BIN et les quatre derniers chiffres du PAN.</li> <li>Tous les rôles non spécifiquement autorisés à voir le PAN complet ne doivent voir que les PAN masqués.</li> </ul>
<b>Objectif de L'approche Personnalisée</b> <p>Les affichages du PAN sont limités au nombre minimum de chiffres nécessaires pour répondre à un besoin métier défini.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence ne remplace pas les exigences plus strictes en place pour l'affichage des données des titulaires de carte ; par exemple, les exigences légales ou de réseaux internationaux pour les reçus des points de vente (POS).</p> <p>Cette exigence concerne la protection du PAN lorsqu'il est affiché sur les écrans, les reçus papier, les impressions, etc., et ne doit pas être confondu avec l'exigence 3.5.1 pour la protection du PAN lorsqu'il est stocké, traité, ou transmis.</p>	<p><b>3.4.1.b</b> Examiner les configurations système afin de vérifier que le PAN complet n'est affiché que pour les rôles avec un besoin métier documenté, et que le PAN est masqué pour toutes les autres demandes.</p> <p><b>3.4.1.c</b> Examiner les affichages du PAN (par exemple, à l'écran, sur les reçus papier) afin de vérifier que les PAN sont masqués lorsqu'ils sont affichés, et que seuls ceux ayant un besoin métier légitime sont en mesure de voir plus que le BIN et/ou les quatre derniers chiffres du PAN.</p>
<b>Objectif</b> L'affichage du PAN complet sur des écrans d'ordinateur, sur des reçus de paiement par carte, sur des rapports papier, etc. peut entraîner l'obtention de ces données par des personnes non autorisées et leur utilisation frauduleuse. S'assurer que le PAN complet n'est affiché que pour ceux qui ont un besoin métier légitime minimise le risque que des personnes non autorisées accèdent aux données PAN.	
<b>Bonne Pratique</b> L'application de mesures de sécurité d'accès en fonction de rôles définis est un moyen de limiter l'accès à l'affichage du PAN complet aux seules personnes ayant un besoin métier défini.	
L'approche de masquage doit toujours afficher uniquement le nombre de chiffres nécessaires à l'exécution d'une fonction métier spécifique. Par exemple, si seuls les quatre derniers chiffres sont nécessaires pour exécuter une fonction métier, le PAN doit être masqué pour n'afficher que les quatre derniers chiffres. Autre exemple, si une fonction doit afficher le numéro d'identification bancaire (BIN) à des fins de routage, démasquer uniquement les chiffres du BIN pour cette fonction.	

(suite à la page suivante)

Exigences et Procédures de Test	Directives
	<p><b>Définitions</b> Le masquage n'est pas synonyme de troncature et ces termes ne peuvent pas être utilisés de manière interchangeable. Le masquage fait référence à la dissimulation de certains chiffres lors de l'affichage ou de l'impression, même lorsque l'intégralité du PAN est stockée sur un système. Il est différent de la troncature, dans laquelle les chiffres tronqués sont supprimés et ne peuvent pas être récupérés dans le système. Le PAN masqué peut être « démasqué », mais il n'y a pas de « dé-troncature » sans recréer le PAN à partir d'une autre source. Se référer à <a href="#">l'annexe G</a> pour les définitions de « masquage » et de « troncature ».</p> <p><b>Informations Complémentaires</b> Pour plus d'informations sur le masquage et la troncature, consultez la FAQ du PCI SSC sur ces sujets.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.4.2</b> Lors de l'utilisation de technologies d'accès à distance, les mesures de sécurité techniques empêchent la copie et/ou la relocalisation du PAN pour tout le personnel, à l'exception de ceux disposant d'une autorisation explicite documentée et d'un besoin métier légitime et défini.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.4.2.a</b> Examiner les politiques et procédures documentées et les preuves documentées des mesures de sécurité techniques qui empêchent la copie et/ou le déplacement du PAN lors de l'utilisation de technologies d'accès à distance sur des disques durs locaux ou des supports électroniques amovibles afin de vérifier les éléments suivants :</p> <ul style="list-style-type: none"> <li>Que des mesures de sécurité techniques empêchent tout personnel non spécifiquement autorisé de copier et/ou de déplacer le PAN.</li> <li>Qu'une liste du personnel autorisé à copier et/ou déplacer le PAN est maintenue, ainsi qu'une autorisation explicite documentée et que le besoin métier légitime est défini.</li> </ul>
<b>Objectif de L'approche Personnalisée</b> <p>Le PAN ne peut pas être copié ou déplacé par du personnel non autorisé utilisant des technologies d'accès à distance.</p>	<b>Objectif</b> La relocalisation du PAN vers des périphériques de stockage non autorisés est un moyen courant d'obtenir et d'utiliser frauduleusement ces données. Les méthodes permettant de s'assurer que seules les personnes disposant d'une autorisation explicite et d'une raison métier légitime peuvent copier ou déplacer le PAN, minimisent le risque que des personnes non autorisées accèdent au PAN. <b>Bonne Pratique</b> La copie et le déplacement du PAN ne doivent être effectués que sur des périphériques de stockage permis et autorisés pour cette personne. <b>Définitions</b> Un bureau virtuel est un exemple de technologie d'accès à distance. De telles technologies d'accès à distance comportent souvent des outils pour désactiver la fonction de copie et/ou de relocalisation. Les périphériques de stockage comportent, sans toutefois s'y limiter, les disques durs locaux, les lecteurs virtuels, les supports électroniques amovibles, les lecteurs réseau et le stockage en cloud.
<b>Notes D'applicabilité</b> <p>Le stockage ou le déplacement du PAN sur des disques durs locaux, des supports électroniques amovibles et d'autres périphériques de stockage fait entrer ces dispositifs dans le périmètre PCI DSS.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>3.4.2.b</b> Examiner les configurations des technologies d'accès à distance afin de s'assurer que les mesures de sécurité techniques empêchent la copie et/ou le déplacement du PAN pour tout le personnel, sauf pour le personnel explicitement autorisé.</p> <p><b>3.4.2.c</b> Observer les processus et interroger le personnel afin de s'assurer que seul le personnel disposant d'une autorisation explicite et documentée et d'un besoin métier légitime et défini a la permission de copier et/ou de déplacer le PAN lors de l'utilisation de technologies d'accès à distance.</p> <b>Informations Complémentaires</b> La documentation du fournisseur pour la technologie d'accès à distance utilisée fournira des informations sur les paramètres système nécessaires pour mettre en œuvre cette exigence.

Exigences et Procédures de Test	Directives
<b>3.5 Le numéro de compte primaire (PAN) est sécurisé partout où il est stocké.</b>	
<b>Exigences de L'approche Définie</b> <p><b>3.5.1</b> Le PAN est rendu illisible partout où il est stocké en utilisant l'une des approches suivantes :</p> <ul style="list-style-type: none"> <li>• Hachage à sens unique basé sur une cryptographie robuste de l'intégralité du PAN.</li> <li>• Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN). <ul style="list-style-type: none"> <li>– Si des versions hachées et tronquées du même PAN, ou des formats de troncature différents du même PAN, sont présentes dans un environnement, des mesures de sécurité supplémentaires sont en place afin que les différentes versions ne puissent pas être corrélées pour reconstruire le PAN d'origine.</li> </ul> </li> <li>• Token d'index.</li> <li>• Cryptographie robuste avec processus et procédures de gestion des clés associés.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.5.1.a</b> Examiner la documentation sur le système utilisé pour rendre le PAN illisible, y compris le fournisseur, le type de système/processus et les algorithmes cryptographiques (le cas échéant) afin de vérifier que le PAN est rendu illisible à l'aide de l'une des méthodes spécifiées dans cette exigence.</p> <p><b>3.5.1.b</b> Examiner les référentiels de données et les journaux d'audit, y compris les journaux des applications de paiement, afin de vérifier que le PAN est rendu illisible à l'aide de l'une des méthodes spécifiées dans cette exigence.</p> <p><b>3.5.1.c</b> Si des versions hachées et tronquées du même PAN sont présentes dans l'environnement, examiner les mesures de sécurité mis en œuvre afin de vérifier que les versions hachées et tronquées ne peuvent pas être corrélées aux fins de reconstruire le PAN d'origine.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les PAN en texte clair ne peuvent pas être lus ou reconstitués à partir du support de stockage.</p> <p>(suite à la page suivante)</p>	<b>Objectif</b> Rendre illisibles les PAN stockés est une mesure de défense en profondeur conçue pour protéger les données si une personne non autorisée accède aux données stockées en exploitant une vulnérabilité ou une mauvaise configuration du contrôle d'accès primaire d'une entité. <b>Bonne pratique</b> Il est relativement facile pour une personne malveillante de reconstruire les données du PAN d'origine si elle a accès aux versions à la fois tronquées et hachées d'un PAN. Les mesures de sécurité qui empêchent la corrélation de ces données aideront à garantir que le PAN d'origine reste illisible. La mise en place de hachages cryptographiques à clés avec des processus et procédures de gestion des clés conformément à l'Exigence 3.5.1.1 est une mesure supplémentaire valide pour prévenir la corrélation. <b>Informations Complémentaires</b> Pour plus d'informations sur les formats de troncature et la troncature en général, consulter la FAQ du PCI SSC sur le sujet. Les sources d'informations sur les jetons d'index comprennent : <ul style="list-style-type: none"> <li>• Directives de sécurité des produits de tokenisation du PCI SSC (<a href="https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf">https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf</a>)</li> <li>• ANSI X9.119-2-2017 : Services financiers de détail - Exigences relatives à la protection des données sensibles des cartes de paiement - Partie 2 : Mise en œuvre des systèmes de tokenisation post-autorisation</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique aux PAN stockés dans un stockage principal (bases de données ou fichiers plats tels que des feuilles de calcul en fichiers texte) ainsi que dans un stockage non principal (sauvegarde, journaux d'audit, journaux des exceptions ou de dépannage).</p> <p>Cette exigence n'exclut pas l'utilisation de fichiers temporaires contenant un PAN en texte clair lors du chiffrement et du déchiffrement du PAN.</p>	

## Exigences et Procédures de Test

## Directives

### Exigences de L'approche Définie

**3.5.1.1** Les hachages utilisés pour rendre le PAN illisible (selon le premier point de l'exigence 3.5.1) sont des hachages cryptographiques de l'ensemble du PAN, avec des processus et procédures de gestion des clés associés conformes aux exigences 3.6 et 3.7.

### Objectif de l'Approche Personnalisée

Le PAN en texte clair ne peut pas être déterminé à partir des hachages du PAN.

### Notes D'applicabilité

Toutes les Note d'Applicabilité pour l'exigence 3.5.1 s'applique également à cette exigence.

Les processus et procédures de gestion des clés (Exigences 3.6 et 3.7) ne s'appliquent pas aux composants système utilisés pour générer des hachages à clé individuels d'un PAN pour comparer avec un autre système si :

- Les composants système ont accès uniquement à une seule valeur de hachage à la fois (les valeurs de hachage ne sont pas stockées sur le système)

#### ET

- Il n'y a aucune autre donnée stockée sur le système sous forme de hachages.

*Cette exigence est considérée une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation PCI DSS. Cette exigence remplacera le point dans l'exigence 3.5.1 pour les hachages à sens unique une fois sa date d'échéance est atteinte.*

### Procédures de Test de L'approche Définie

**3.5.1.1.a** Examiner la documentation sur la méthode de hachage utilisée pour rendre le PAN illisible, y compris celle du fournisseur, le type de système/processus et les algorithmes cryptographiques (le cas échéant) afin de vérifier que la méthode de hachage aboutit à hachages cryptographiques de l'ensemble du PAN, avec les processus et procédures de gestion des clés associés.

**3.5.1.1.b** Examiner la documentation sur les procédures et processus de gestion des clés associés aux hachages cryptographiques à clé pour vérifier que les clés sont gérées conformément aux exigences 3.6 et 3.7.

**3.5.1.1.c** Examiner les dépôts de données afin de vérifier que le PAN est rendu illisible.

**3.5.1.1.d** Examiner les journaux d'audit, y compris les journaux d'applications de paiement, afin de vérifier que le PAN est rendu illisible.

### Objectif

Rendre illisible le PAN est une mesure de défense en profondeur conçue pour protéger les données si une personne non autorisée accède aux données stockées en exploitant une vulnérabilité ou une mauvaise configuration du contrôle d'accès primaire d'une entité.

Une fonction de hachage qui incorpore une clé secrète générée de façon aléatoire fournit une résistance aux attaques Brute Force et une intégrité à l'authentification secrète.

### Définitions

Se reporter à l'Annexe G pour la définition du « hachage cryptographique à clé » et pour des informations sur les algorithmes adéquats de hachage cryptographique à clé et autres ressources.

### Exemples

Les systèmes qui ont uniquement accès à une seule valeur de hachage à la fois, et qui ne stocke aucune autre donnée de compte sur le même système sous forme de hachage, ne sont pas tenus de satisfaire aux processus et procédures de gestion des clés (Exigences 3.6 et 3.7). Des exemples de tels systèmes comprennent les appareils de transactions d'origine qui génèrent un hachage du PAN pour utilisation sur un système backend, tels que les tourniquets de transit de paiement au portail. Cependant, dans une telle mise en œuvre, le système backend aura accès à plus d'une seule valeur de hachage à la fois, et, par conséquent, il doit satisfaire aux processus et procédures de gestion des clés de des Exigences 3.6 et 3.7.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.5.1.2</b> Si le chiffrement au niveau du disque ou au niveau de la partition (plutôt que le chiffrement de la base de données au niveau des fichiers, des colonnes ou des champs) est utilisé pour rendre le PAN illisible, il est mis en œuvre uniquement de la manière suivante :</p> <ul style="list-style-type: none"> <li>• Sur des supports électroniques amovibles <b>OU</b></li> <li>• S'il est utilisé sur des supports électroniques non amovibles, le PAN est également rendu illisible via un autre mécanisme qui satisfait à l'exigence 3.5.1.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.5.1.2.a</b> Examiner les processus de chiffrement afin de vérifier que, si le chiffrement au niveau du disque ou au niveau de la partition est utilisé pour rendre le PAN illisible, il est mis en œuvre uniquement de la manière suivante :</p> <ul style="list-style-type: none"> <li>• Sur des supports électroniques amovibles,</li> <li>• S'il est utilisé sur des supports électroniques non amovibles, examiner les processus de chiffrement utilisés afin de vérifier que le PAN est également rendu illisible via une autre méthode qui satisfait à l'exigence 3.5.1.</li> </ul> <p><b>3.5.1.2.b</b> Examiner les configurations et/ou la documentation du fournisseur et observer les processus de chiffrement afin de vérifier que le système est configuré conformément à la documentation du fournisseur de sorte que le disque ou la partition soit rendus illisible.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le PAN est uniquement déchiffré lorsqu'il y a un besoin commercial légitime d'accéder à ce PAN</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>En général, le chiffrement au niveau du disque et au niveau de la partition chiffre l'intégralité du disque ou de la partition à l'aide de la même clé, avec toutes les données automatiquement déchiffrées lorsque le système s'exécute ou lorsqu'un utilisateur autorisé le demande. Pour cette raison, le chiffrement au niveau du disque n'est pas approprié pour protéger le PAN stocké sur les ordinateurs de bureau, les ordinateurs portables, les serveurs, les baies de stockage ou tout autre système qui fournit un déchiffrement transparent lors de l'authentification de l'utilisateur.</p> <p><b>Informations Complémentaires</b></p> <p>Le cas échéant, le respect des directives de renforcement des fournisseurs et des meilleures pratiques de l'industrie peut aider à sécuriser le PAN sur ces périphériques.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à toutes les méthodes de chiffrement qui fournissent le PAN en texte clair automatiquement lorsqu'un système est exécuté, même si un utilisateur autorisé n'a pas spécifiquement demandé ces données.</p> <p>Bien que le chiffrement de disque ou de partition puisse toujours être présent sur ces types de périphériques, il ne peut pas être la seule méthode utilisée pour protéger le PAN stocké sur ces systèmes. Tout PAN stocké doit également être rendu illisible conformément à l'exigence 3.5.1 ; par exemple, via une troncature ou un mécanisme de chiffrement au niveau des données. Le chiffrement complet du disque aide à protéger les données en cas de perte physique d'un disque et, par conséquent, son utilisation n'est appropriée que pour les périphériques de stockage électroniques amovibles.</p> <p>Les supports faisant partie d'une architecture de centre de données (par exemple, les lecteurs remplaçables à chaud, les sauvegardes sur bande en masse) sont considérés comme des supports électroniques non amovibles auxquels l'exigence 3.5.1 s'applique.</p> <p>Les mises en œuvre du chiffrement de disques ou de partitions doivent également répondre à toutes les autres exigences PCI DSS de chiffrement et de gestion des clés.</p> <p>Pour les émetteurs et entreprises qui prennent en charge les services d'émission :</p> <p>Cette exigence ne s'applique pas aux PAN accédés pour un traitement de transactions en temps réel. Cependant, elle s'applique bel et bien aux PAN stockés à d'autres fins.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.5.1.3</b> Si le chiffrement au niveau du disque ou au niveau de la partition est utilisé (plutôt que le chiffrement au niveau de la base de données, des fichiers, des colonnes ou des champs) afin de rendre le PAN illisible, il est géré de la manière suivante :</p> <ul style="list-style-type: none"> <li>• L'accès logique est géré séparément et indépendamment de l'authentification du système d'exploitation natif et des mécanismes de contrôle d'accès.</li> <li>• Les clés cryptographiques ne sont pas associées aux comptes utilisateur.</li> <li>• Les facteurs d'authentification (mots de passe, phrases secrètes ou clés cryptographiques) qui permettent l'accès aux données non chiffrées sont stockés en toute sécurité.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.5.1.3.a</b> Si le chiffrement au niveau du disque ou au niveau de la partition est utilisé pour rendre le PAN illisible, examiner la configuration du système et observer le processus d'authentification afin de vérifier que l'accès logique est mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>3.5.1.3.b</b> Examiner les fichiers contenant les facteurs d'authentification (mots de passe, phrases secrètes ou clés cryptographiques) et interroger le personnel afin de vérifier que les facteurs d'authentification qui permettent l'accès aux données non chiffrées sont stockés en toute sécurité et sont indépendants des méthodes d'authentification et de contrôle d'accès du système d'exploitation natif.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les mises en œuvre du chiffrement de disque sont configurées pour exiger une authentification indépendante et des mesures de sécurité d'accès logique pour le déchiffrement.</p>	<b>Objectif</b> En général, le chiffrement au niveau du disque chiffre l'intégralité du disque ou de la partition à l'aide de la même clé, avec toutes les données automatiquement déchiffrées lorsque le système s'exécute ou lorsqu'un utilisateur autorisé le demande. De nombreuses solutions de chiffrement de disque interceptent les opérations de lecture/écriture du système d'exploitation et effectuent les transformations cryptographiques appropriées sans aucune action spéciale de la part de l'utilisateur autre que la fourniture d'un mot de passe ou d'une phrase secrète au démarrage du système ou au début d'une session. Cela ne fournit aucune protection contre une personne malveillante qui a déjà réussi à accéder à un compte d'utilisateur valide. <b>Bonne Pratique</b> Le chiffrement complet du disque aide à protéger les données en cas de perte physique d'un disque et, par conséquent, il est préférable de limiter son utilisation uniquement aux périphériques de stockage électroniques amovibles.
<b>Notes D'applicabilité</b> <p>Les mises en œuvre du chiffrement de disques ou de partitions doivent également répondre à toutes les autres exigences PCI DSS de chiffrement et de gestion des clés.</p>	

Exigences et Procédures de Test	Directives
<b>3.6 Les clés cryptographiques utilisées pour protéger les données de carte stockées sont sécurisées.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.6.1</b> Des procédures sont définies et mises en œuvre afin de protéger les clés cryptographiques utilisées pour protéger les données de carte stockées contre la divulgation et l'utilisation abusive, notamment :</p> <ul style="list-style-type: none"> <li>• L'accès aux clés est limité au plus petit nombre d'opérateurs nécessaire.</li> <li>• Les clés de chiffrement des clés sont au moins aussi robustes que les clés de chiffrement des données qu'elles protègent.</li> <li>• Les clés de chiffrement des clés sont stockées séparément des clés de chiffrement de données.</li> <li>• Les clés sont stockées en toute sécurité dans le moins d'emplacements et de formes possibles.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.6.1</b> Examiner les politiques et procédures de gestion des clés documentées afin de vérifier que les processus de protection des clés cryptographiques utilisées pour protéger les données de carte stockées contre la divulgation et l'utilisation abusive sont définies pour inclure tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les processus qui protègent les clés cryptographiques utilisées pour protéger les données de carte stockées contre la divulgation et l'utilisation abusive sont définis et mis en œuvre.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b> Les clés cryptographiques doivent être protégées de manière robuste, car ceux qui y accéderont pourront déchiffrer les données.</p> <p><b>Bonne Pratique</b> Il est recommandé de disposer d'un système centralisé de gestion de clés, basé sur les standards du secteur pour gérer les clés cryptographiques.</p> <p><b>Informations Complémentaires</b> Les procédures de gestion des clés de l'entité tireront parti des exigences du secteur. Les sources d'informations sur les cycles de vie de la gestion des clés cryptographiques comprennent :</p> <ul style="list-style-type: none"> <li>• <i>ISO 11568-1 Banque — Gestion des clés (commerce de détail) — Partie 1 : Principes</i> (en particulier le chapitre 10 et les parties 2 et 4 référencées)</li> <li>• <i>NIST SP 800-57 Partie 1, Révision 5 -- Recommandation pour la gestion des clés, Partie 1 : Généralités.</i></li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique aux clés utilisées pour protéger les données de carte stockées et aux clés de chiffrement utilisées pour protéger les clés de chiffrement des données.</p> <p>L'exigence de protéger les clés utilisées pour protéger les données de carte stockées contre la divulgation et l'utilisation abusive s'applique à la fois aux clés de chiffrement des données et aux clés de chiffrement des clés. Étant donné qu'une clé de chiffrement de clé peut accorder l'accès à de nombreuses clés de chiffrement de données, les clés de chiffrement de clés nécessitent des mesures de protection strictes.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.6.1.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Une description documentée de l'architecture cryptographique est maintenue, et qui comprend :</p> <ul style="list-style-type: none"> <li>• Les détails de tous les algorithmes, protocoles et clés utilisés pour la protection des données de carte stockées, y compris la robustesse de la clé et la date d'expiration.</li> <li>• Éviter l'utilisation des mêmes clés cryptographiques dans les environnements de production et de test. Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</li> <li>• Une description de l'utilisation des clés pour chaque clé.</li> <li>• L'inventaire de tous les modules de sécurité matérielle (HSM), systèmes de gestion de clés (KMS) et autres dispositifs cryptographiques sécurisés (SCD) utilisés pour la gestion des clés, y compris le type et l'emplacement des dispositifs, afin de satisfaire à l'Exigence 12.3.4.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Des détails précis de l'architecture cryptographique sont conservés et disponibles.</p> <p>(suite à la page suivante)</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.6.1.1 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Interroger le personnel en charge et examiner la documentation afin de vérifier qu'un document existe pour décrire l'architecture cryptographique qui comprend tous les éléments spécifiés dans cette exigence.</p>
	<p><b>Objectif</b></p> <p>La tenue à jour de la documentation de l'architecture cryptographique permet à une entité de comprendre les algorithmes, les protocoles et les clés cryptographiques utilisés pour protéger les données de carte stockées, ainsi que les dispositifs qui génèrent, utilisent et protègent les clés. Cela permet à une entité de suivre le rythme de l'évolution des menaces pesant sur son architecture et de planifier des mises à jour au fur et à mesure que le niveau d'assurance fourni par les différents algorithmes et la robustesse des clés change. Le maintien d'une telle documentation permet également à une entité de détecter des clés ou des dispositifs de gestion de clés perdus ou manquants et d'identifier les ajouts non autorisés à son architecture cryptographique. L'utilisation des mêmes clés cryptographiques dans les environnements de production et de test introduit un risque d'exposition de la clé si l'environnement de test n'est pas au même niveau de sécurité que l'environnement de production.</p> <p><b>Bonne Pratique</b></p> <p>Disposer d'un mécanisme de signalement automatisé peut aider à la maintenance des attributs cryptographiques.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Dans les implémentations de HSM en cloud, la responsabilité de l'architecture cryptographique conformément à cette exigence sera partagée entre le fournisseur du service cloud et le consommateur de cloud.</p> <p><i>La point ci-dessus (pour inclure, dans l'architecture cryptographique, que l'utilisation des mêmes clés cryptographiques en production et en test est évitée) est une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire dans le cadre de l'exigence 3.6.1.1 et doit être pleinement prise en compte lors d'une évaluation PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.6.1.2</b> Les clés secrètes et privées utilisées pour protéger les données de carte stockées sont conservées sous l'une (ou plusieurs) des formes suivantes à tout moment :</p> <ul style="list-style-type: none"> <li>• Chiffrées avec une clé de chiffrement de clé qui est au moins aussi robuste que la clé de chiffrement des données, et qui est stockée séparément de la clé de chiffrement des données.</li> <li>• Dans un dispositif cryptographique sécurisé (SCD), tel qu'un module de sécurité matérielle (HSM) ou un dispositif de point d'interaction approuvé PTS.</li> <li>• Sous forme d'au moins deux composants de clé ou de partages de clé de pleine longueur, conformément à une méthode acceptée par l'industrie.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.6.1.2.a</b> Examiner les procédures documentées afin de vérifier qu'il est défini que les clés cryptographiques utilisées pour chiffrer/déchiffrer les données de carte stockées ne doivent exister que sous une (ou plusieurs) des formes spécifiées dans cette exigence.</p> <p><b>3.6.1.2.b</b> Examiner les configurations système et les emplacements de stockage des clés afin de vérifier que les clés cryptographiques utilisées pour chiffrer/déchiffrer les données de carte stockées existent dans une (ou plusieurs) des formes spécifiées dans cette exigence.</p> <p><b>3.6.1.2.c</b> Partout où des clés de chiffrement des clés sont utilisées, examiner les configurations système et les emplacements de stockage des clés afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• Les clés de chiffrement des clés sont au moins aussi robustes que les clés de chiffrement des données qu'elles protègent.</li> <li>• Les clés de chiffrement des clés sont stockées séparément des clés de chiffrement de données.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés secrètes et privées sont stockées sous une forme sécurisée qui empêche la récupération ou l'accès non autorisés</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>Le stockage sécurisé des clés cryptographiques empêche les accès non autorisés ou inutiles qui pourraient entraîner l'exposition des données de carte stockées. Le stockage séparé des clés signifie qu'elles sont stockées de sorte que si l'emplacement d'une clé est compromis, la deuxième clé ne l'est pas également.</p> <p><b>Bonne Pratique</b></p> <p>Lorsque des clés de chiffrement de données sont stockées dans un HSM, le canal d'interaction HSM doit être protégé pour empêcher l'interception des opérations de chiffrement ou de déchiffrement.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes.</p> <p>Les clés cryptographiques stockées dans le cadre d'un système de gestion des clés (KMS) qui utilise des SCD sont acceptables.</p> <p>Une clé cryptographique divisée en deux parties ne répond pas à cette exigence. Les clés secrètes ou privées stockées en tant que composants de clé ou partages de clé doivent être générées via l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> <li>• À l'aide d'un générateur de chiffres aléatoires approuvé et au sein d'un SCD,</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• Selon ISO 19592 ou une standard industrielle équivalente pour la génération de partages de clés secrètes.</li> </ul>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.6.1.3</b> L'accès aux composants de clé cryptographique en texte clair est limité au plus petit nombre d'opérateurs nécessaire.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>L'accès aux composants de clé cryptographique en texte clair est limité au personnel nécessaire.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.6.1.3</b> Examiner les listes d'accès des utilisateurs afin de vérifier que l'accès aux composants de clé cryptographique en texte clair est limité au plus petit nombre d'opérateurs nécessaires.</p> <p><b>Objectif</b> La restriction du nombre de personnes ayant accès aux composants de clé cryptographique en texte clair réduit le risque que les données de carte stockées soient récupérées ou rendues visibles par des personnes non autorisées.</p> <p><b>Bonne Pratique</b> Seul un personnel ayant des responsabilités définies d'opérateur de clés (création, modification, rotation, distribution ou maintenance des clés cryptographiques) doit avoir accès aux composants de clés. Idéalement, ce sera un nombre très réduit de personnes.</p>
<b>Exigences de L'approche Définie</b> <p><b>3.6.1.4</b> Les clés cryptographiques sont stockées dans le moins d'emplacements possibles.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés cryptographiques ne sont conservées qu'en cas de nécessité.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.6.1.4</b> Examiner les emplacements de stockage des clés et observer les processus afin de vérifier que les clés sont stockées dans le moins d'emplacements possibles.</p> <p><b>Objectif</b> Le stockage de toutes les clés cryptographiques dans le moins d'emplacements permet à une entreprise de suivre et de surveiller tous les emplacements des clés et de minimiser le risque que les clés soient exposées à des parties non autorisées.</p>

## Exigences et Procédures de Test

## Directives

3.7 Lorsque la cryptographie est utilisée pour protéger les données de carte stockées, des processus et procédures de gestion des clés couvrant tous les aspects du cycle de vie des clés sont définis et mis en œuvre.

Exigences de L'approche Définie	Procédures de Test de L'approche Définie	Objectif
<p><b>3.7.1</b> Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la génération de clés cryptographiques robustes utilisées pour protéger les données de carte stockées.</p>	<p><b>3.7.1.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées afin de vérifier qu'elles définissent la génération de clés cryptographiques robustes.</p> <p><b>3.7.1.b</b> Observer la méthode de génération des clés afin de vérifier que des clés robustes sont générées.</p>	<p><b>Objectif</b> L'utilisation de clés cryptographiques robustes augmente considérablement le niveau de sécurité des données de carte chiffrées.</p> <p><b>Informations Complémentaires</b> Voir les sources référencées dans la section « Génération de clés cryptographiques à l'Annexe G. »</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des clés cryptographiques robustes sont générées.</p>		
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.7.2</b> Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la distribution de clés cryptographiques utilisées pour protéger les données de carte stockées.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.7.2.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées afin de vérifier qu'elles définissent la distribution de clés cryptographiques.</p> <p><b>3.7.2.b</b> Observer la méthode de distribution des clés afin de vérifier que les clés sont distribuées de manière sécurisée.</p>	<p><b>Objectif</b> La distribution ou la transmission sécurisée de clés cryptographiques secrètes ou privées signifie que les clés ne sont distribuées qu'aux opérateurs autorisés, tels qu'identifiés dans l'exigence 3.6.1.2, et ne sont jamais distribuées de manière non sécurisée.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés cryptographiques sont sécurisées lors de la distribution.</p>		

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.7.3</b> Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure le stockage de clés cryptographiques utilisées pour protéger les données de carte stockées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.7.3.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées afin de vérifier qu'elles définissent le stockage de clés cryptographiques.</p> <p><b>3.7.3.b</b> Observer la méthode de stockage des clés afin de vérifier que les clés sont stockées de manière sécurisée.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les clés cryptographiques sont sécurisées lors du stockage.</p>	<b>Objectif</b> Le stockage des clés sans protection adéquate pourrait permettre l'accès à des attaques, entraînant le déchiffrement et l'exposition des données du compte. <b>Bonne Pratique</b> Les clés cryptographiques des données peuvent être protégées en les chiffrant avec une clé de chiffrement de clé. Les clés peuvent être stockées dans un module de sécurité matérielle (HSM). Les clés secrètes ou privées qui peuvent déchiffrer les données ne doivent jamais être présentes dans le code source.
<b>Exigences de L'approche Définie</b> <p><b>3.7.4</b> Les politiques et procédures de gestion des clés sont mises en œuvre pour les changements de clés cryptographiques pour les clés qui ont atteint la fin de leur cryptopériode, telles que définies par le fournisseur d'applications associé ou le propriétaire de la clé, et basées sur les meilleures pratiques et directives de l'industrie, y compris ce qui suit :</p> <ul style="list-style-type: none"> <li>• Une cryptopériode définie pour chaque type de clé utilisé.</li> <li>• Un processus pour les changements de clé à la fin de la cryptopériode définie.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.7.4.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées afin de vérifier qu'elles définissent les changements apportés aux clés cryptographiques qui ont atteint la fin de leur cryptopériode et incluent tous les éléments spécifié dans cette exigence.</p> <p><b>3.7.4.b</b> Interroger le personnel, examiner la documentation et observer les emplacements de stockage des clés afin de vérifier que les clés sont modifiées à la fin de la ou des cryptopériodes définies.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les clés cryptographiques ne sont pas utilisées au-delà de leur cryptopériode définie.</p>	<b>Objectif</b> Il est impératif de changer les clés cryptographiques lorsqu'elles atteignent la fin de leur période de cryptographie afin de minimiser le risque que quelqu'un obtienne les clés cryptographiques et les utilise pour déchiffrer des données. <b>Définitions</b> Une cryptopériode est la durée pendant laquelle une clé cryptographique peut être utilisée pour son but défini. Les cryptopériodes sont souvent définies en fonction de la période pendant laquelle la clé est active et/ou de la quantité de texte de chiffrement produite par la clé. Les considérations pour définir la cryptopériode incluent, sans toutefois s'y limiter, la robustesse 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 chiffrées. <i>(suite à la page suivante)</i>

Exigences et Procédures de Test	Directives
	<p><b>Informations Complémentaires</b></p> <p><i>NIST SP 800-57 Partie 1, Révision 5, Section 5.3 Cryptopériodes</i> - fournit des conseils pour établir la période pendant laquelle une clé spécifique est autorisée à être utilisée par des entités légitimes, ou les clés d'un système donné resteront en vigueur.</p> <p>Voir le tableau 1 de <i>SP 800-57 Partie 1</i> pour les cryptopériodes suggérées pour différents types de clés.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.7.5</b> Les procédures et politiques de gestion des clés sont mises en œuvre pour inclure le retrait, le remplacement ou la destruction des clés utilisées pour protéger les données de carte stockées, comme jugé nécessaire lorsque :</p> <ul style="list-style-type: none"> <li>• La clé a atteint la fin de sa cryptopériode définie.</li> <li>• L'intégrité de la clé a été affaiblie, notamment lorsque le personnel connaissant un composant de clé en texte clair quitte l'entreprise ou le rôle pour lequel le composant de clé était connu.</li> <li>• La clé est suspectée ou avérée être compromise.</li> </ul> <p>Les clés retirées ou remplacées ne sont pas utilisées pour les opérations de chiffrement.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.7.5.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées et vérifier qu'elles définissent le retrait, le remplacement ou la destruction des clés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>3.7.5.b</b> Interroger le personnel afin de vérifier que les processus sont mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés sont retirées de l'utilisation active lorsqu'il est soupçonné ou connu que l'intégrité de la clé est affaiblie.</p>	<p><b>Objectif</b></p> <p>Les clés qui ne sont plus nécessaires, les clés dont l'intégrité est affaiblie et les clés dont on sait ou soupçonne qu'elles sont compromises doivent être archivées, révoquées et/ou détruites afin de garantir que les clés ne pourront plus être utilisées.</p> <p>Si de telles clés doivent être conservées (par exemple, pour prendre en charge les données chiffrées archivées), elles doivent être fortement protégées.</p> <p><b>Bonne Pratique</b></p> <p>Les clés cryptographiques archivées ne doivent être utilisées qu'à des fins de déchiffrement/vérification.</p> <p>La solution de chiffrement doit prévoir et faciliter un processus de remplacement des clés qui doivent être remplacées ou dont on sait ou soupçonne qu'elles sont compromises. De plus, toutes les clés avérées ou soupçonnées d'être compromises doivent être gérées selon le plan de réponse aux incidents de l'entité conformément à l'exigence 12.10.1.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Si des clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, à l'aide d'une clé de chiffrement de clé).</p>	<p><b>Informations Complémentaires</b></p> <p>Les meilleures pratiques de l'industrie pour l'archivage des clés retirées sont décrites dans <i>NIST SP 800-57 Partie 1, Révision 5, Section 8.3.1</i>, et comportent la maintenance de l'archive avec un tiers de confiance et le stockage des informations sur les clés archivées séparément des données opérationnelles.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.7.6</b> Lorsque les opérations manuelles de gestion des clés cryptographiques en texte clair sont effectuées par le personnel, les politiques et procédures de gestion des clés sont mises en œuvre, notamment la gestion de ces opérations à l'aide du fractionnement des connaissances et du double contrôle.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés secrètes ou privées en texte clair ne peuvent être connues de personne. Les opérations impliquant des clés en texte clair ne peuvent pas être effectuées par une seule personne.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.7.6.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées et vérifier qu'elles sont définies à l'aide du fractionnement des connaissances et du double contrôle.</p> <p><b>3.7.6.b</b> Interroger le personnel et/ou observer les processus afin de vérifier que les clés manuelles en texte clair sont gérées avec un fractionnement des connaissances et un double contrôle.</p> <p><b>Objectif</b> Le fractionnement des connaissances et le double contrôle des clés sont utilisés afin d'éliminer la possibilité qu'une seule personne ait accès à l'ensemble de la clé et puisse donc accéder aux données sans autorisation.</p> <p><b>Définitions</b> Le fractionnement des connaissances est une méthode dans laquelle deux personnes ou plus ont séparément des composants de clés, où chaque personne ne connaît que son propre composant de clé, et les composants de clés individuels ne transmettent aucune connaissance des autres composants ou de la clé cryptographique d'origine.</p> <p>Le double contrôle nécessite deux personnes ou plus pour authentifier l'utilisation d'une clé cryptographique ou exécuter une fonction de gestion des clés. Aucune personne ne peut accéder ou utiliser le facteur d'authentification (par exemple, le mot de passe, le code PIN ou la clé) d'une autre personne.</p> <p><b>Bonne Pratique</b> Lorsque des composants de clé ou des partages de clé sont utilisés, les procédures devraient garantir que jamais un opérateur n'a accès à suffisamment de composants ou de partages de clé pour reconstruire la clé cryptographique. (suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette mesure s'applique aux opérations manuelles de gestion des clés.</p> <p>Une clé cryptographique simplement divisée en deux parties ne répond pas à cette exigence. Les clés secrètes ou privées stockées en tant que composants de clé ou partages de clé doivent être générées via l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> <li>• L'utilisation d'un générateur de chiffres aléatoires approuvé et dans un dispositif cryptographique sécurisé (SCD), tel qu'un module de sécurité matérielle (HSM) ou un dispositif de point d'interaction approuvé PTS,</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• Selon ISO 19592 ou une standard industrielle équivalente pour la génération de partages de clés secrètes.</li> </ul>	<p>Par exemple, dans un schéma m-sur-n (par exemple, Shamir), où seuls deux des trois composants sont nécessaires pour reconstruire la clé cryptographique, un opérateur ne doit pas avoir une connaissance actuelle ou antérieure de plus d'un composant.</p> <p>Si un opérateur s'est déjà vu attribuer le composant A, qui a ensuite été réattribué, l'opérateur ne devrait pas alors se voir attribuer le composant B ou C, car cela donnerait à l'opérateur la connaissance de deux composants et la possibilité de recréer la clé.</p> <p><b>Exemples</b></p> <p>Les opérations de gestion des clés pouvant être effectuées manuellement incluent, sans toutefois s'y limiter, la génération, la transmission, le chargement, le stockage et la destruction des clés.</p> <p><b>Informations Complémentaires</b></p> <p>Les standards de l'industrie pour la gestion des composants de clés incluent :</p> <ul style="list-style-type: none"> <li>• <i>NIST SP 800-57 Partie 2, Révision 1 -- Recommandation pour la gestion des clés : Partie 2 – Meilleures pratiques pour les entreprises de gestion des clés [4.6 Distribution de matériel de génération de clés]</i></li> <li>• <i>ISO 11568-1 Banking — Key management (retail) — Part 1 : Chiffrements symétriques, la gestion de leurs clés et leur cycle de vie [4.7.2.3 Composants de clés et 4.9.3 Composants de clés]</i></li> <li>• <i>Directives EPC342-08 du Conseil européen des paiements sur l'utilisation des algorithmes cryptographiques et la gestion des clés [en particulier 4.1.4 Installation des clés]</i>.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.7.7</b> Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure la prévention de la substitution non autorisée de clés cryptographiques.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.7.7.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées et vérifier qu'elles définissent la prévention de la substitution non autorisée de clés cryptographiques.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clés cryptographiques ne peuvent pas être remplacées par du personnel non autorisé.</p>	<p><b>Objectif</b> Si un attaquant est capable de remplacer la clé d'une entité par une clé qu'il connaît, l'attaquant pourra déchiffrer toutes les données chiffrées avec cette clé.</p> <p><b>Bonne Pratique</b> La solution de chiffrement ne doit pas permettre ou accepter la substitution de clés provenant de sources non autorisées ou de processus inattendus.</p> <p>Les mesures de sécurité doivent inclure la garantie que les personnes ayant accès aux composants ou partages de clés n'ont pas accès à d'autres composants ou partages qui forment le seuil nécessaire pour dériver la clé.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>3.7.8</b> Des politiques et procédures de gestion des clés sont mises en œuvre pour inclure que les opérateurs de clés cryptographiques reconnaissent formellement (par écrit ou par voie électronique) qu'ils comprennent et acceptent leurs responsabilités d'opérateurs de clés.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>3.7.8.a</b> Examiner les politiques et procédures de gestion des clés documentées pour les clés utilisées dans la protection des données de carte stockées et vérifier qu'elles définissent des reconnaissances par les opérateurs de clés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>3.7.8.b</b> Examiner la documentation ou d'autres preuves indiquant que les principaux opérateurs ont fourni des reconnaissances conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les opérateurs chargés de la gestion des clés connaissent leurs responsabilités en matière d'opérations cryptographiques et peuvent accéder à une assistance et à des conseils en cas de besoin.</p>	<b>Objectif</b> <p>Ce processus aidera à garantir que les personnes qui agissent en tant qu'opérateurs de clés s'engagent à jouer le rôle d'opérateur de clés et comprennent et acceptent les responsabilités. Une réaffirmation annuelle peut aider à rappeler aux principaux opérateurs leurs responsabilités.</p> <p><b>Informations Complémentaires</b></p> <p>Les directives de l'industrie pour les opérateurs de clés et leurs rôles et responsabilités comprennent :</p> <ul style="list-style-type: none"> <li>• <i>NIST SP 800-130 Un cadre pour la conception de systèmes de gestion de clés cryptographiques</i> [5. Rôles et responsabilités (en particulier) des opérateurs de clés]</li> <li>• <i>ISO 11568-1 Banking — Key management (retail) — Part 1 : Principes</i> [5 Principes de gestion des clés (en particulier b)]</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>3.7.9 Exigences supplémentaires pour les prestataires de services uniquement :</b> Lorsqu'un prestataire de services partage des clés cryptographiques avec ses clients pour la transmission ou le stockage de données de carte, des conseils sur la transmission, le stockage et la mise à jour sécurisés de ces clés sont documentés et distribués aux clients des prestataires de services.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les clients reçoivent des conseils appropriés sur la gestion des clés chaque fois qu'ils reçoivent des clés cryptographiques partagées.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>3.7.9 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Si le prestataire de services partage des clés cryptographiques avec ses clients pour la transmission ou le stockage des données de carte, examiner la documentation que le prestataire de services fournit à ses clients, afin de vérifier qu'elle comprend des conseils sur la façon de transmettre, de stocker et de mettre à jour de manière sécurisée les clés des clients conformément à tous les éléments spécifiés dans les exigences 3.7.1 à 3.7.8 ci-dessus.</p> <p><b>Objectif</b> La fourniture de conseils aux clients sur la manière de transmettre, de stocker et de mettre à jour les clés cryptographiques de manière sécurisée peut aider à empêcher que les clés ne soient mal gérées ou divulguées à des entités non autorisées.</p> <p><b>Informations Complémentaires</b> De nombreux standards de l'industrie régissant la gestion des clés sont cités ci-dessus dans le Guide des exigences 3.7.1-3.7.8.</p>

## ***Exigence 4 : Protéger les Données des Titulaires de Cartes Grâce à une Cryptographie Robuste Lors de la Transmission sur des Réseaux Publics Ouverts***

### **Sections**

- 4.1** Des processus et des mécanismes de protection des données des titulaires de carte avec une cryptographie robuste lors de la transmission sur des réseaux publics ouverts, sont définis et compris.
- 4.2** Le PAN est protégé par une cryptographie robuste pendant la transmission.

### **Aperçu**

L'utilisation d'une cryptographie robuste offre une plus grande assurance pour la préservation de la confidentialité, de l'intégrité et de la non-répudiation des données.

Pour se protéger contre la compromission, le PAN doit être chiffré lors de la transmission sur des réseaux facilement accessibles par des personnes malveillantes, y compris des réseaux publics et non fiables. Les réseaux sans fil mal configurés et les vulnérabilités des protocoles de chiffrement et d'authentification hérités continuent d'être ciblés par des personnes malveillantes cherchant à exploiter ces vulnérabilités afin d'obtenir un accès privilégié aux environnements de données des titulaires de carte (CDE). Toute transmission de données de titulaires de cartes sur le ou les réseaux internes d'une entité placera naturellement ce réseau dans le périmètre de du standard PCI DSS, car ce réseau stocke, traite ou transmet les données de titulaires de cartes. Tous ces réseaux doivent être évalués et expertisés par rapport aux exigences applicables du standard PCI DSS.

L'exigence 4 s'applique à la transmission du PAN, sauf indication contraire dans une exigence individuelle.

Les transmissions des PAN peuvent être protégées en chiffrant les données avant leur transmission, ou en chiffrant la session dans laquelle les données sont transmises, ou les deux. Bien qu'il ne soit pas obligatoire d'appliquer une cryptographie robuste au niveau des données et au niveau de la session, cela est recommandé.

Se reporter à [\*l'Annexe G\*](#) pour les définitions de « cryptographie robuste » et d'autres termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<p><b>4.1 Les processus et des mécanismes de protection des données des titulaires de carte avec une cryptographie robuste lors de la transmission sur des réseaux publics ouverts, sont définis et compris.</b></p>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>4.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 4 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>4.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 4 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attentes, les mesures de sécurité et la surveillance des activités de réunion dans l'exigence 4 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<p><b>Objectif</b> L'exigence 4.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 4. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 4, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique.</p> <p><b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique. Les politiques et procédures, y compris les mises à jour, sont activement communiquées à tout le personnel concerné et sont justifiées par des procédures opérationnelles décrivant la manière d'effectuer les activités.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>4.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 4 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>4.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 4 sont documentées et attribuées.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 4 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts.</p> <p>Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>4.2 Le PAN est protégé par une cryptographie robuste pendant la transmission.</b>	
<b>Exigences de L'approche Définie</b> <p><b>4.2.1</b> Des protocoles de chiffrement et de sécurité robustes sont mis en œuvre comme suit afin de protéger le PAN pendant la transmission sur des réseaux publics ouverts :</p> <ul style="list-style-type: none"> <li>• Seuls les clés et certificats de confiance sont acceptés.</li> <li>• Les certificats utilisés pour protéger le PAN lors de la transmission sur des réseaux publics ouverts sont confirmés comme valides et ne sont ni expirés ni révoqués. <i>Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</i></li> <li>• Le protocole utilisé ne prend en charge que les versions ou configurations sécurisées et ne prend pas en charge le basculement ou l'utilisation de versions, d'algorithmes, de tailles de clé ou de mises en œuvre non sécurisés.</li> <li>• La robustesse du chiffrement est adéquate pour la méthodologie de chiffrement utilisée.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>4.2.1.a</b> Examiner les politiques et procédures documentées et interroger le personnel afin de vérifier que des processus sont définis pour inclure tous les éléments spécifiés dans cette exigence.</p> <p><b>4.2.1.b</b> Examiner les configurations du système afin de vérifier que des protocoles de cryptographie et de sécurité robustes sont mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>4.2.1.c</b> Examiner les transmissions de données des titulaires de cartes afin de vérifier que tous les PAN sont chiffrés avec une cryptographie robuste lorsqu'ils sont transmis sur des réseaux publics ouverts.</p> <p><b>4.2.1.d</b> Examiner les configurations du système afin de vérifier que les clés et/ou les certificats qui ne peuvent pas être vérifiés comme étant de confiance sont rejetés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les PAN en texte clair ne peuvent pas être lus ou interceptés à partir de toute transmission sur des réseaux publics ouverts.</p>	<b>Objectif</b> <p>Les informations sensibles doivent être chiffrées lors de leur transmission sur les réseaux publics, car il est facile et courant pour une personne malveillante d'intercepter et/ou de détourner des données en transit.</p> <p><b>Bonne Pratique</b></p> <p>Les diagrammes de flux de données et de réseau définis dans l'exigence 1 sont des ressources utiles pour identifier tous les points de connexion par lesquels les données de carte sont transmises ou reçues sur des réseaux publics ouverts.</p> <p>Bien que cela ne soit pas obligatoire, il est considéré comme une Bonne Pratique pour les entités de chiffrer également le PAN sur leurs réseaux internes et pour les entités d'établir de nouvelles mises en œuvre de réseau avec des communications chiffrées.</p> <p>Les transmissions des PAN peuvent être protégées en chiffrant les données avant leur transmission, ou en chiffrant la session dans laquelle les données sont transmises, ou les deux. Bien qu'il ne soit pas obligatoire d'appliquer une cryptographie robuste au niveau des données et au niveau de la session, cela est fortement recommandé. Si elles sont chiffrées au niveau des données, les clés cryptographiques utilisées pour protéger les données peuvent être gérées conformément aux exigences 3.6 et 3.7. Si les données sont chiffrées au niveau de la session, des opérateurs de clés désignés devraient être chargés de la gestion des clés de transmission et des certificats.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Un certificat auto-signé peut également être acceptable si le certificat est émis par une autorité de certification interne au sein de l'entreprise, que l'auteur du certificat est confirmé et que le certificat est vérifié (par exemple, par hachage ou signature) et qu'il n'a pas expiré.</p> <p><i>Le point ci-dessus (pour confirmer que les certificats utilisés pour protéger le PAN pendant la transmission sur des réseaux publics ouverts sont valides et n'ont pas expiré ni été révoqués) est une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera requise dans le cadre de l'exigence 4.2.1. et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	<p>Certaines mises en œuvre de protocoles (telles que SSL, SSH v1.0 et TLS initial) présentent des vulnérabilités connues qu'un attaquant peut utiliser pour accéder aux données en texte clair. Il est essentiel que les entités restent informées des dates d'obsolescence définies par l'industrie pour les suites de chiffrement qu'elles utilisent et soient prêtes à migrer vers des versions ou des protocoles plus récents lorsque les plus anciens ne sont plus considérés comme sécurisés.</p> <p>Vérifier que les certificats sont approuvés permet de garantir l'intégrité de la connexion sécurisée. Pour être considéré comme approuvé, un certificat doit provenir d'une source de confiance, telle qu'une autorité de certification (CA) de confiance, et ne pas avoir expiré. Des listes de révocation de certificats (CRL) à jour ou le protocole OCSP (Online Certificate Status Protocol) peuvent être utilisés pour valider les certificats.</p> <p>Les techniques de validation des certificats peuvent inclure le certificate pinning et le public key pinning, où le certificat de confiance ou une clé publique est fixé soit pendant le développement, soit lors de sa première utilisation. Les entités peuvent également confirmer avec les développeurs ou examiner le code source afin de s'assurer que les clients et les serveurs refusent les connexions si le certificat n'est pas bon.</p> <p>Pour les certificats TLS basés sur un navigateur, la confiance du certificat peut souvent être vérifiée en cliquant sur l'icône de cadenas qui apparaît à côté de la barre d'adresse.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p><b>Exemples</b>            Les réseaux publics ouverts comprennent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Les technologies Internet et</li> <li>• Sans fil, y compris le Wi-Fi, le Bluetooth, les technologies cellulaires et les communications par satellite.</li> </ul> <p><b>Informations Complémentaires</b>            Les recommandations des fournisseurs et les meilleures pratiques de l'industrie peuvent être consultées afin d'obtenir des informations sur la robustesse appropriée de chiffrement spécifique à la méthodologie de chiffrement utilisée.            Pour plus d'informations sur la cryptographie robuste et les protocoles sécurisés, consultez les normes et standards de l'industrie et les meilleures pratiques telles que <i>NIST SP 800-52</i> et <i>SP 800-57</i>.            Pour plus d'informations sur les clés et les certificats approuvés, consultez <i>la publication spéciale 1800-16 du NIST Guide des pratiques de cybersécurité, Sécurisation des transactions Web : Gestion des certificats du serveur TLS (Transport Layer Security)</i>.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>4.2.1.1</b> Un inventaire des clés et des certificats approuvés par l'entité utilisés pour protéger le PAN pendant la transmission, est maintenu.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>4.2.1.1.a</b> Examiner les politiques et procédures documentées afin de vérifier que des processus sont définis pour que l'entité conserve un inventaire de ses clés et certificats approuvés.</p> <p><b>4.2.1.1.b</b> Examiner l'inventaire des clés et des certificats approuvés afin de vérifier qu'il est tenu à jour.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Toutes les clés et tous les certificats utilisés pour protéger le PAN pendant la transmission sont identifiés et confirmés comme étant approuvés.</p>	
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>4.2.1.2</b> Les réseaux sans fil transmettant le PAN ou connectés au CDE utilisent les meilleures pratiques de l'industrie pour mettre en œuvre une cryptographie robuste pour l'authentification et la transmission.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les PAN en texte clair ne peuvent pas être lus ou interceptés à partir de toute transmission via des réseaux sans fil.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>4.2.1.2</b> Examiner les configurations du système afin de vérifier que les réseaux sans fil transmettant le PAN ou connectés au CDE utilisent les meilleures pratiques de l'industrie pour mettre en œuvre une cryptographie robuste pour l'authentification et la transmission.</p> <p><b>Objectif</b></p> <p>Étant donné que les réseaux sans fil ne nécessitent pas de support physique pour se connecter, il est important d'établir des mesures de sécurité limitants qui peut se connecter et quels protocoles de transmission seront utilisés. Les utilisateurs malveillants utilisent des outils libres d'accès et largement disponibles pour espionner les communications sans fil. L'utilisation d'une cryptographie robuste peut aider à limiter la divulgation d'informations sensibles sur les réseaux sans fil.</p> <p>Les réseaux sans fil présentent des risques uniques pour une entreprise ; par conséquent, ils doivent être identifiés et protégés conformément aux exigences de l'industrie. Une cryptographie forte pour l'authentification et la transmission du PAN est requise afin d'empêcher les utilisateurs malveillants d'accéder au réseau sans fil ou d'utiliser des réseaux sans fil pour accéder à d'autres réseaux ou données internes.</p> <p><b>Bonne Pratique</b></p> <p>Les réseaux sans fil ne doivent pas permettre le basculement ou la rétrogradation vers un protocole non sécurisé ou une robustesse de chiffrement inférieure qui ne répond pas à l'intention d'une cryptographie robuste.</p> <p><b>Informations Complémentaires</b></p> <p>Consulter la documentation spécifique du fournisseur pour plus de détails sur le choix des protocoles, des configurations et des paramètres liés à la cryptographie.</p>

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>4.2.2</b> Le PAN est sécurisé avec une cryptographie robuste chaque fois qu'il est envoyé via les technologies de messagerie des utilisateurs finaux.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>4.2.2.a</b> Examiner les politiques et procédures documentées afin de vérifier que les processus sont définis pour sécuriser les PAN avec une cryptographie robuste chaque fois qu'ils sont envoyés via les technologies de messagerie des utilisateurs finaux.</p> <p><b>4.2.2.b</b> Examiner les configurations système et la documentation du fournisseur afin de vérifier que le PAN est sécurisé avec une cryptographie robuste chaque fois qu'il est envoyé via les technologies de messagerie des utilisateurs finaux.</p>	<b>Objectif</b> Les technologies de messagerie des utilisateurs finaux peuvent généralement être facilement interceptées par 'sniffing' de paquets lors de l'envoi sur les réseaux internes et publics. <b>Bonne Pratique</b> L'utilisation de la technologie de messagerie des utilisateurs finaux pour envoyer le PAN ne doit être envisagée que lorsqu'il existe un besoin professionnel défini et devrait être contrôlé via les Politiques d'Utilisation Acceptable pour les technologies d'utilisateurs finaux définies l'entité conformément à l'Exigence 12.2.1. <b>Exemples</b> Le courrier électronique, la messagerie instantanée, les SMS et le chat sont des exemples du type de technologie de messagerie d'utilisateurs finaux auquel cette exigence fait référence.
<b>Objectif de L'approche Personnalisée</b> Le PAN en texte clair ne peut pas être lu ou intercepté à partir des transmissions utilisant les technologies de messagerie des utilisateurs finaux.		
<b>Notes D'applicabilité</b> <p>Cette exigence s'applique également si un consommateur, ou un autre tiers, demande que le PAN lui soit envoyé via les technologies de messagerie des utilisateurs finaux.</p> <p>Il peut arriver qu'une entité reçoive des données non sollicitées de titulaires de cartes via un canal de communication non sécurisé qui n'était pas destiné aux fins de recevoir des données sensibles. Dans cette situation, l'entité peut choisir soit d'inclure le canal dans le périmètre de son CDE et de le sécuriser conformément au standard PCI DSS, soit de supprimer les données du titulaire de carte et mettre en œuvre des mesures afin d'empêcher l'utilisation du canal pour les données de titulaires de cartes.</p>		

## Maintenir un Programme de Gestion des Vulnérabilités

### ***Exigence 5 : Protéger Tous les Systèmes et Réseaux Contre les Logiciels Malveillants***

#### Sections

- 5.1** Les processus et mécanismes de protection de tous les systèmes et réseaux contre les logiciels malveillants sont définis et compris.
- 5.2** Les logiciels malveillants (malware) sont empêchés ou détectés et traités.
- 5.3** Les mécanismes et processus anti-programmes malveillants sont actifs, maintenus et surveillés.
- 5.4** Les mécanismes anti-hameçonnage protègent les utilisateurs contre les attaques par hameçonnage.

#### Aperçu

Un logiciel malveillant (malware) est un logiciel ou un micrologiciel conçu pour infiltrer ou endommager un système informatique à l'insu ou sans le consentement du propriétaire, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, les applications ou le système d'exploitation du propriétaire.

Des exemples comportent les virus, les vers, les chevaux de Troie, les logiciels espions, les logiciels de rançon, les enregistreurs de frappe et rootkits, les codes malveillants, les scripts et les liens.

Les logiciels malveillants peuvent pénétrer dans le réseau lors de nombreuses activités approuvées par l'entreprise, y compris la messagerie électronique des employés (par exemple, via l'hameçonnage) et l'utilisation d'Internet, des ordinateurs portables et des périphériques de stockage, entraînant l'exploitation des vulnérabilités du système.

L'utilisation de solutions anti-programmes malveillants qui traitent tous les types de logiciels malveillants aide à protéger les systèmes contre les menaces actuelles et évolutives de logiciels malveillants.

Se reporter à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>5.1 Les processus et mécanismes de protection de tous les systèmes et réseaux contre les logiciels malveillants sont définis et compris.</b>	
<b>Exigences de L'approche Définie</b> <p><b>5.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 5 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>5.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 5 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les attentes, les mesures de sécurité et la surveillance des activités de réunion dans l'exigence 5 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<b>Objectif</b> L'exigence 5.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 5. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 5, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées. <b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique. <b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>5.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 5 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>5.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 5 sont documentées et attribuées.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 5 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, les réseaux et les systèmes peuvent ne pas être correctement protégés contre les logiciels malveillants.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test		Directives
<b>5.2 Les logiciels malveillants (malware) sont empêchés ou détectés et traités.</b>		
<b>Exigences de L'approche Définie</b>  <b>5.2.1</b> Une ou plusieurs solutions anti-programmes malveillants sont déployées sur tous les composants système, à l'exception des composants systèmes identifiés dans les évaluations périodiques conformément à l'exigence 5.2.3 qui conclut que les composants système ne sont pas à risque de logiciels malveillants.	<b>Procédures de Test de L'approche Définie</b>  <b>5.2.1.a</b> Examiner les composants système afin de vérifier qu'une ou plusieurs solutions anti-programmes malveillants sont déployées sur tous les composants système, à l'exception de ceux déterminés comme n'étant pas exposés aux logiciels malveillants sur la base d'évaluations périodiques conformément à l'exigence 5.2.3.  <b>5.2.1.b</b> Pour tous les composants système sans solution anti-programmes malveillants, examiner les évaluations périodiques afin de vérifier que le composant a été évalué et que l'évaluation a conclu que le composant n'est pas menacé par des logiciels malveillants.	<b>Objectif</b> Il existe un flux constant d'attaques ciblant les vulnérabilités nouvellement découvertes dans des systèmes précédemment considérés comme sécurisés. Sans solution anti-programmes malveillants régulièrement mise à jour, de nouvelles formes de malware peuvent être utilisées pour attaquer des systèmes, désactiver un réseau ou compromettre des données.  <b>Bonne Pratique</b> Il est avantageux pour les entités d'être au courant des attaques « zero-day » (celles qui exploitent une vulnérabilité auparavant inconnue) et d'envisager des solutions axées sur les caractéristiques comportementales et qui alertent sur et réagissent à un comportement inattendu.  <b>Définitions</b> Les composants système connus pour être touchés par des logiciels malveillants ont des exploits malveillants actifs disponibles dans le monde réel (pas uniquement des exploits théoriques).
<b>Objectif de L'approche Personnalisée</b>  Des mécanismes automatisés sont mis en œuvre pour empêcher les systèmes de devenir un vecteur d'attaque pour les logiciels malveillants.		

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>5.2.2</b> La ou les solutions anti-programmes malveillants déployées :</p> <ul style="list-style-type: none"> <li>• Détecte tous les types connus de logiciels malveillants.</li> <li>• Supprime, bloque ou contient tous les types connus de logiciels malveillants.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les logiciels malveillants ne peuvent pas exécuter ou infecter d'autres composants système.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>5.2.2</b> Examiner la documentation du fournisseur et les configurations de la ou des solutions anti-programmes malveillants afin de vérifier que la solution :</p> <ul style="list-style-type: none"> <li>• Détecte tous les types connus de logiciels malveillants.</li> <li>• Supprime, bloque ou contient tous les types connus de logiciels malveillants.</li> </ul> <p><b>Objectif</b> Il est important de se protéger contre tous les types et formes de logiciels malveillants afin d'empêcher tout accès non autorisé.</p> <p><b>Bonne Pratique</b> Les solutions anti-programmes malveillants peuvent inclure une combinaison de mesures de sécurité basés sur le réseau, de mesures de sécurité basés sur l'hôte et de solutions de sécurité des terminaux. En plus des outils basés sur les signatures, les capacités utilisées par les solutions anti-programmes malveillants modernes incluent le sandboxing, les mesures de sécurité d'élévation des priviléges et l'apprentissage automatique.</p> <p>Les techniques de solution consistent à empêcher les logiciels malveillants d'entrer dans le réseau et à supprimer ou contenir les logiciels malveillants qui pénètrent dans le réseau.</p> <p><b>Exemples</b> Les types de logiciels malveillants incluent, sans toutefois s'y limiter, les virus, les chevaux de Troie, les vers, les logiciels espions, les logiciels de rançon, les enregistreurs de frappe, les rootkits, les codes malveillants, les scripts et les liens.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>5.2.3</b> Tous les composants système qui ne présentent pas de risque de logiciels malveillants sont évalués périodiquement pour inclure les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Une liste documentée de tous les composants système ne présentant pas de risque de logiciels malveillants.</li> <li>• Identification et évaluation des menaces de logiciels malveillants en évolution pour ces composants système.</li> <li>• Confirmation indiquant si ces composants système continuent de ne pas nécessiter de protection anti-programmes malveillants.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>5.2.3.a</b> Examiner les politiques et procédures documentées afin de vérifier qu'un processus est défini pour les évaluations périodiques de tous les composants système qui ne sont pas à risque à l'égard des logiciels malveillants, qui incluent tous les éléments spécifiés dans cette exigence.</p> <p><b>5.2.3.b</b> Interroger le personnel afin de vérifier que les évaluations comportent tous les éléments spécifiés dans cette exigence.</p> <p><b>5.2.3.c</b> Examiner la liste des composants systèmes identifiés comme ne présentant pas de risque de logiciels malveillants et les comparer aux composants système sans solution anti-programmes malveillants déployée conformément à l'exigence 5.2.1 afin de vérifier que les composants système correspondent aux deux exigences.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'entité reste informée de l'évolution des menaces de logiciels malveillants afin de s'assurer que les systèmes non protégés contre les logiciels malveillants ne courent aucun risque d'infection.</p>	<p><b>Objectif</b></p> <p>Certains systèmes, à un moment donné, peuvent actuellement ne pas être habituellement ciblés ou touchés par des logiciels malveillants. Cependant, les tendances de l'industrie en matière de logiciels malveillants peuvent changer rapidement, il est donc important que les entreprises soient au courant des nouveaux logiciels malveillants susceptibles de toucher leurs systèmes, par exemple en surveillant les avis de sécurité des fournisseurs et les forums anti-programmes malveillants afin de déterminer si leurs systèmes pourraient être menacés par des logiciels malveillants nouveaux et en évolution.</p> <p><b>Bonne Pratique</b></p> <p>Si une entité détermine qu'un système particulier n'est sensible à aucun logiciel malveillant, la détermination doit être étayée par les preuves de l'industrie, les ressources des fournisseurs et les meilleures pratiques.</p> <p>Les étapes suivantes peuvent aider les entités lors de leurs évaluations périodiques :</p> <ul style="list-style-type: none"> <li>• Identification de tous les types de système précédemment déterminés comme ne nécessitant pas de protection contre les logiciels malveillants.</li> <li>• Examen des alertes et des avis de vulnérabilité de l'industrie afin de déterminer si de nouvelles menaces existent pour tout système identifié.</li> <li>• Une conclusion documentée indiquant si les types de systèmes restent insensibles aux logiciels malveillants.</li> </ul>
<p><b>Notes D'applicabilité</b></p> <p>Les composants systèmes couverts par cette exigence sont ceux pour lesquels aucune solution anti-programmes malveillants n'est déployée conformément à l'exigence 5.2.1.</p>	<p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<ul style="list-style-type: none"><li>Une stratégie pour ajouter une protection contre les logiciels malveillants pour tous les types de systèmes pour lesquels une protection contre les logiciels malveillants est devenue nécessaire.</li></ul> <p>Les tendances en matière de logiciels malveillants doivent être incluses dans l'identification des nouvelles vulnérabilités de sécurité dans l'exigence 6.3.1, et des méthodes pour répondre aux nouvelles tendances doivent être intégrées dans les standards de configuration et les mécanismes de protection de l'entité, si nécessaire.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>5.2.3.1</b> La fréquence des évaluations périodiques des composants systèmes identifiés comme ne présentant pas de risque de logiciels malveillants est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>5.2.3.1.a</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des évaluations périodiques des composants système identifiés comme ne présentant pas de risque de logiciels malveillants afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'Exigence 12.3.1.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les systèmes dont on ne sait pas qu'ils sont exposés à des logiciels malveillants sont réévalués à une fréquence qui tient compte du risque de l'entité.</p>	<p><b>5.2.3.1.b</b> Examiner les résultats documentés des évaluations périodiques des composants systèmes identifiés comme ne présentant pas de risque de logiciels malveillants et interroger le personnel afin de vérifier que les évaluations sont effectuées à la fréquence définie dans l'analyse de risque ciblée de l'entité effectuée pour cette exigence.</p>
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> <p>Les entités déterminent la période optimale pour entreprendre l'évaluation en fonction de critères tels que la complexité de l'environnement de chaque entité et le nombre de types de systèmes qui doivent être évalués.</p>

Exigences et Procédures de Test		Directives
<b>5.3 Les mécanismes et processus anti-programmes malveillants sont actifs, maintenus et surveillés.</b>		
<b>Exigences de L'approche Définie</b>  <b>5.3.1</b> La ou les solutions anti-programmes malveillants sont tenues à jour via des mises à jour automatiques.	<b>Procédures de Test de L'approche Définie</b>  <b>5.3.1.a</b> Examiner les configurations de la ou des solutions anti-programmes malveillants, y compris toute installation originale du logiciel, afin de vérifier que la solution est configurée pour effectuer des mises à jour automatiques.  <b>5.3.1.b</b> Examiner les composants et les journaux système, afin de vérifier que la ou les solutions et définitions anti-programmes malveillants sont à jour et ont été rapidement déployées.	<b>Objectif</b> Pour qu'une solution anti-programmes malveillants reste efficace, elle doit disposer des dernières mises à jour de sécurité, signatures, moteurs d'analyse des menaces et toute autre protection contre les logiciels malveillants sur laquelle repose la solution.  <b>Bonne Pratique</b> Avoir un processus de mise à jour automatisé évite de surcharger les utilisateurs finaux avec la responsabilité d'installer manuellement les mises à jour et offre une plus grande assurance que les mécanismes de protection anti-programmes malveillants sont mis à jour aussi rapidement que possible après la publication d'une mise à jour.  Les mécanismes anti-programmes malveillants doivent être mis à jour via une source fiable dès que possible une fois qu'une mise à jour est disponible. L'utilisation d'une source commune fiable pour distribuer les mises à jour aux systèmes des utilisateurs finaux permet de garantir l'intégrité et l'uniformité de l'architecture de la solution.  Les mises à jour peuvent être automatiquement téléchargées vers un emplacement centralisé, par exemple pour permettre des tests, avant d'être déployées sur des composants systèmes individuels.
<b>Objectif de L'approche Personnalisée</b>  Les mécanismes anti-programmes malveillants peuvent détecter et traiter les dernières menaces de logiciel malveillants.		

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>5.3.2</b> La ou les solutions anti-programmes malveillants :</p> <ul style="list-style-type: none"> <li>Effectue des analyses périodiques et des analyses actives ou en temps réel, <b>OU</b></li> <li>Effectue une analyse comportementale continue des systèmes ou des processus.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>5.3.2.a</b> Examiner les configurations de les solutions anti-programmes malveillants, y compris toute installation originale du logiciel, afin de vérifier que la ou les solutions sont configurées pour exécuter au moins un des éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les logiciels malveillants ne peuvent pas terminer l'exécution.</p>	<p><b>5.3.2.b</b> Examiner les composants système, y compris tous les types de système d'exploitation identifiés comme présentant un risque de logiciels malveillants afin de vérifier que la ou les solutions sont activées conformément à au moins un des éléments spécifiés dans cette exigence.</p> <p><b>5.3.2.c</b> Examiner les journaux et les résultats d'analyse afin de vérifier que la ou les solutions sont activées conformément à au moins un des éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b> Des analyses périodiques peuvent identifier les logiciels malveillants présents, mais actuellement inactifs, dans l'environnement. Certains logiciels malveillants, tels que les logiciels malveillants zero-day, peuvent pénétrer dans un environnement avant que la solution d'analyse ne soit capable de le détecter. La réalisation d'analyses périodiques régulières ou d'analyses comportementales continues des systèmes ou des processus permet de garantir que les logiciels malveillants auparavant indétectables peuvent être identifiés, supprimés et étudiés pour déterminer comment ils ont pu accéder à l'environnement.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p><b>Bonne Pratique</b></p> <p>L'utilisation d'une combinaison d'analyses périodiques (planifiées et à la demande) et d'analyses actives en temps réel (à l'accès) permet de garantir que les logiciels malveillants résidant dans les éléments statiques et dynamiques du CDE sont traités. Les utilisateurs doivent également être en mesure d'exécuter des analyses à la demande sur leurs systèmes si une activité suspecte est détectée - cela peut être utile dans la détection précoce des logiciels malveillants.</p> <p>Les analyses doivent inclure l'intégralité du système de fichiers, y compris tous les disques, la mémoire, les fichiers de démarrage et les enregistrements de démarrage (au redémarrage du système) pour détecter tous les logiciels malveillants lors de l'exécution du fichier, y compris tout logiciel pouvant résider sur un système mais qui n'est pas actuellement actif.</p> <p>Le périmètre de l'analyse doit inclure tous les systèmes et logiciels du CDE, y compris ceux qui sont souvent négligés, tels que les serveurs de messagerie, les navigateurs Web et les logiciels de messagerie instantanée.</p> <p><b>Définitions</b></p> <p>L'analyse active ou en temps réel recherche les fichiers malveillants lors de toute tentative d'ouvrir, de fermer, de renommer ou d'interagir avec un fichier, empêchant ainsi l'activation du logiciel malveillant.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>5.3.2.1</b> Si des analyses périodiques de logiciels malveillants sont effectuées pour répondre à l'exigence 5.3.2, la fréquence des analyses est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les analyses par la solution de logiciels malveillants sont effectuées à une fréquence qui répond au risque de l'entité.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique aux entités effectuant des analyses périodiques des logiciels malveillants pour satisfaire à l'exigence 5.3.2.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>5.3.2.1.a</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des analyses périodiques des logiciels malveillants afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p> <p><b>5.3.2.1.b</b> Examiner les résultats documentés des analyses périodiques des logiciels malveillants et interroger le personnel afin de vérifier que les analyses sont effectuées à la fréquence définie dans l'analyse de risques ciblée de l'entité, effectuée pour cette exigence.</p> <p><b>Objectif</b> Les entités peuvent déterminer la période optimale pour entreprendre des analyses périodiques en fonction de leur propre évaluation des risques posés à leur environnement.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>5.3.3</b> Pour les supports électroniques amovibles, la solution anti-programmes malveillants :</p> <ul style="list-style-type: none"> <li>Effectue des analyses automatiques lorsque le support est inséré, connecté ou monté logiquement,</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>Effectue une analyse comportementale continue des systèmes ou des processus lorsque le support est inséré, connecté ou monté logiquement.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>5.3.3.a</b> Examiner les configurations de la solution anti-programmes malveillants afin de vérifier que, pour les supports électroniques amovibles, la solution est configurée pour exécuter au moins un des éléments spécifiés dans cette exigence.</p> <p><b>5.3.3.b</b> Examiner les composants système avec des supports électroniques amovibles connectés afin de vérifier que la ou les solutions sont activées conformément à au moins un des éléments spécifiés dans cette exigence.</p> <p><b>5.3.3.c</b> Examiner les journaux et les résultats d'analyse afin de vérifier que la ou les solutions sont activées conformément à au moins un des éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les logiciels malveillants ne peuvent pas être introduits dans les composants système via un support amovible externe.</p>	
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>5.3.4</b> Les journaux d'audit pour la solution anti-programmes malveillants sont activés et conservés conformément à l'exigence 10.5.1.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>5.3.4</b> Examiner les configurations de la solution anti-programmes malveillants afin de vérifier que les journaux sont activés et conservés conformément à l'exigence 10.5.1.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les enregistrements de l'historique des actions anti-programmes malveillants sont immédiatement disponibles et conservés pendant au moins 12 mois.</p>	<b>Objectif</b> Il est important de suivre l'efficacité des mécanismes anti-programmes malveillants ; par exemple, en confirmant que les mises à jour et les analyses sont effectuées comme prévu, et que les logiciels malveillants sont identifiés et traités. Les journaux d'audit permettent également à une entité de déterminer comment les logiciels malveillants sont entrés dans l'environnement et de suivre leur activité lorsqu'ils se trouvent à l'intérieur du réseau de l'entité.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>5.3.5</b> Les mécanismes anti-programmes malveillants ne peuvent pas être désactivés ou modifiés par les utilisateurs, à moins qu'ils ne soient spécifiquement documentés et autorisés par la direction au cas par cas pour une durée limitée dans le temps.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>5.3.5.a</b> Examiner les configurations anti-programmes malveillants, afin de vérifier que les mécanismes anti-programmes malveillants ne peuvent pas être désactivés ou modifiés par les utilisateurs.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les mécanismes anti-programmes malveillants ne peuvent pas être modifiés par du personnel non autorisé.</p>	<p><b>5.3.5.b</b> Interroger le personnel responsable et observer les processus afin de vérifier que toute demande de désactivation ou de modification des mécanismes anti-programmes malveillants est spécifiquement documentée et autorisée par la direction au cas par cas pendant une période limitée.</p>
<b>Notes D'applicabilité</b> <p>Les solutions anti-programmes malveillants ne peuvent être temporairement désactivés que s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la solution anti-programmes malveillants doit être désactivée dans un but précis, cette décision doit être formellement autorisée. Des mesures de sécurité supplémentaires peuvent également devoir être mises en œuvre pendant la période pendant laquelle la protection anti-programmes malveillants n'est pas active.</p>	<p><b>Objectif</b> Il est important que les mécanismes de défense soient toujours en cours d'exécution afin que les logiciels malveillants soient détectés en temps réel. Le démarrage et l'arrêt ad hoc des solutions anti-programmes malveillants pourraient permettre aux logiciels malveillants de se propager sans contrôle ni détection.</p> <p><b>Bonne Pratique</b> Lorsqu'il existe un besoin légitime de désactiver temporairement la protection anti-programmes malveillants d'un système ; par exemple, pour prendre en charge une activité de maintenance spécifique ou une enquête sur un problème technique, la raison de cette action doit être comprise et approuvée par un représentant approprié de la direction. Toute désactivation ou modification des mécanismes anti-programmes malveillants, y compris sur les propres appareils des administrateurs, doit être effectuée par du personnel autorisé.</p> <p>Il est reconnu que les administrateurs ont des priviléges qui peuvent leur permettre de désactiver l'anti-programmes malveillants sur leurs propres ordinateurs, mais il devrait y avoir des mécanismes d'alerte en place lorsqu'un tel logiciel est désactivé, puis qu'un suivi se produise afin de s'assurer que les processus corrects ont été suivis.</p> <p><b>Exemples</b> Des mesures de sécurité supplémentaires qui peuvent devoir être mises en œuvre pendant la période pendant laquelle la protection anti-programmes malveillants n'est pas active, incluent la déconnexion du système non protégé d'Internet pendant que la protection anti-programmes malveillants est désactivée et l'exécution d'une analyse complète une fois qu'elle est réactivée.</p>

Exigences et Procédures de Test	Directives
<b>5.4 Les mécanismes anti-hameçonnage protègent les utilisateurs contre les attaques par hameçonnage.</b>	
<b>Exigences de L'approche Définie</b>	<b>Procédures de Test de L'approche Définie</b>
<p><b>5.4.1</b> Des processus et des mécanismes automatisés sont en place pour détecter et protéger le personnel contre les attaques d'hameçonnage.</p>	<p><b>5.4.1</b> Examiner les processus et mécanismes mis en œuvre afin de vérifier que des mesures de sécurité sont en place pour détecter et protéger le personnel contre les attaques d'hameçonnage.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Des mécanismes sont en place pour protéger et atténuer les risques posés par les attaques d'hameçonnage.</p>	
<b>Notes D'applicabilité</b> <p>L'objectif de cette exigence est de protéger le personnel ayant accès aux composants système dans le périmètre du standard PCI DSS.</p> <p>Répondre à cette exigence de mesures de sécurité techniques et automatisés pour détecter et protéger le personnel contre l'hameçonnage n'est pas la même chose que l'exigence 12.6.3.1 pour la formation de sensibilisation à la sécurité. Répondre à cette exigence ne répond pas non plus à l'exigence de fournir au personnel une formation de sensibilisation à la sécurité, et vice versa.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> <p>Les mesures de sécurité techniques peuvent limiter le nombre d'occasions dont le personnel dispose pour évaluer la véracité d'une communication, et peuvent également limiter les effets des réponses individuelles à l'hameçonnage.</p> <p><b>Bonne Pratique</b></p> <p>Lors du développement de mesures anti-hameçonnage, les entités sont encouragées à envisager une combinaison d'approches. Par exemple, l'utilisation de mesures de détection d'usurpation tels que Domain-based Message Authentication, Reporting, and Conformance (DMARC), Sender Policy Framework (SPF) et Domain Keys Identified Mail (DKIM) aidera à empêcher les hameçonneurs d'usurper le domaine de l'entité et de se faire passer pour un membre du personnel.</p> <p>Le déploiement de technologies pour bloquer les courriels d'hameçonnage et les logiciels malveillants avant qu'ils n'atteignent le personnel, tels que les programmes de nettoyage des liens et les anti-programmes malveillants côté serveur, peut diminuer les incidents et réduire le temps nécessaire au personnel pour vérifier et signaler les attaques d'hameçonnage. De plus, former le personnel à reconnaître et signaler les courriels d'hameçonnage peut permettre d'identifier des courriels similaires et de les supprimer avant qu'ils ne soient ouverts.</p> <p>Il est recommandé (mais pas obligatoire) d'appliquer des mesures anti-hameçonnage à l'ensemble de l'organisation d'une entité.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p><b>Définitions</b>  L'hameçonnage est une forme d'ingénierie sociale et décrit les différentes méthodes utilisées par les attaquants pour amener le personnel à divulguer des informations sensibles, telles que les noms et mots de passe des comptes d'utilisateurs, et les données de carte. Les attaquants se déguisent généralement et tentent d'apparaître comme une source authentique ou digne de confiance, en demandant au personnel d'envoyer une réponse par courriel, de cliquer sur un lien Web ou de saisir des données sur un site Web compromis. Des mécanismes permettant de détecter et d'empêcher les tentatives d'hameçonnage sont souvent inclus dans les solutions anti-programmes malveillants.</p> <p><b>Informations Complémentaires</b>  Voir les sources suivantes pour plus d'informations sur l'hameçonnage :  <i>National Cyber Security Centre: Phishing Attacks: Defending your Organization.</i>  <i>US Cybersecurity &amp; Infrastructure Security Agency - Report Phishing Sites.</i></p>

## **Exigence 6 : Développer et Maintenir des Systèmes et des Logiciels Sécurisés**

### **Sections**

- 6.1** Les processus et mécanismes de développement et de maintenance de systèmes et de logiciels sécurisés sont définis et compris.
- 6.2** Des logiciels sur mesure et personnalisés sont développés de manière sécurisée.
- 6.3** Les vulnérabilités de sécurité sont identifiées et corrigées.
- 6.4** Les applications Web destinées au public sont protégées contre les attaques.
- 6.5** Les modifications apportées à tous les composants système sont gérées de manière sécurisée.

### **Aperçu**

Les acteurs mal intentionnés peuvent utiliser des failles de sécurité afin d'obtenir un accès privilégié aux systèmes. Bon nombre de ces vulnérabilités sont corrigées par des correctifs de sécurité fournis par le fournisseur, qui doivent être installés par les entités qui gèrent les systèmes. Tous les composants système doivent disposer de tous les correctifs logiciels appropriés pour se protéger contre l'exploitation et la compromission des données de carte par des personnes malveillantes et des logiciels malveillants.

Les correctifs logiciels appropriés sont les correctifs qui ont été évalués et testés suffisamment pour déterminer qu'ils n'entrent pas en conflit avec les configurations de sécurité existantes. Pour les logiciels sur mesure et personnalisés, de nombreuses vulnérabilités peuvent être évitées en appliquant des processus de cycle de vie du logiciel (SLC) et des techniques de codage sécurisées.

Les référentiels de code qui stockent le code des applications, les configurations système ou d'autres données de configuration pouvant avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles sont dans le périmètre des évaluations du standard PCI DSS.

Voir [Relation entre le PCI DSS et les standards logiciels du PCI SSC](#) à la page 8 pour plus d'informations sur l'utilisation de logiciels et de fournisseurs de logiciels validés par le PCI SSC, et sur la manière dont l'utilisation des standards logiciels du PCI SSC peut aider à satisfaire aux mesures de sécurité de l'exigence 6.

Se reporter à [l'Annexe G](#) pour les définitions des termes de standard PCI DSS.

**Remarque :** L'exigence 6 s'applique à tous les composants système, à l'exception de la section 6.2 pour le développement de logiciels de manière sécurisée, qui s'applique uniquement aux logiciels sur mesure et personnalisés utilisés sur tout composant système inclus dans, ou connecté au CDE.

Exigences et Procédures de Test	Directives
<b>6.1 Les processus et mécanismes de développement et de maintenance de systèmes et de logiciels sécurisés sont définis et compris.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 6 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 6 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attentes, les mesures de sécurité et la surveillance des activités de réunion dans l'exigence 6 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<p><b>Objectif</b> L'exigence 6.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 6. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 6, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique.</p> <p><b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 6 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 6 sont documentées et attribuées.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 6 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas formellement attribués, les systèmes ne seront pas maintenus de manière sécurisée et leur niveau de sécurité sera réduit.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>6.2 Les logiciels sur mesure et personnalisés sont développés de manière sécurisée.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.2.1</b> Les logiciels sur mesure et personnalisés sont développés de manière sécurisée comme suit :</p> <ul style="list-style-type: none"> <li>• Sur la base des normes et standards de l'industrie et/ou des meilleures pratiques pour un développement sécurisé.</li> <li>• Conformément au standard PCI DSS (par exemple, authentification et journalisation sécurisées).</li> <li>• Intégration de la prise en compte des problèmes de sécurité de l'information à chaque étape du cycle de vie du développement logiciel.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.2.1</b> Examiner les procédures de développement logiciel documentées afin de vérifier que des processus sont définis et comportent tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les logiciels sur mesure et personnalisés sont développés conformément au standard PCI DSS et aux processus de développement sécurisés tout au long du cycle de vie du logiciel.</p>	
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à tous les logiciels développés pour ou par l'entité pour son propre usage. Cela inclut des logiciels à la fois sur mesure et personnalisés. Ceci ne s'applique pas aux logiciels tiers.</p>	<p><b>Objectif</b> Sans l'inclusion de la sécurité lors des phases de définition des exigences, de conception, d'analyse et de test du développement logiciel, des vulnérabilités de sécurité peuvent être introduites par inadvertance ou par malveillance dans l'environnement de production.</p> <p><b>Bonne Pratique</b> Comprendre comment les données sensibles sont gérées par l'application, y compris lorsqu'elles sont stockées, transmises et en mémoire, peut aider à identifier où les données doivent être protégées.</p> <p>Les exigences du standard PCI DSS doivent être prises en compte lors du développement de logiciels afin de répondre à ces exigences dès la conception, plutôt que d'essayer de réajuster le logiciel ultérieurement.</p> <p><b>Exemples</b> Les méthodologies et les cadres de gestion du cycle de vie des logiciels sécurisés incluent PCI Secure Software Framework, BSIMM, OPENSAMM et les travaux de NIST, ISO et SAFE Code.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.2.2</b> Le personnel développeur de logiciels travaillant sur des logiciels sur mesure et personnalisés est formé au moins une fois tous les 12 mois comme suit :</p> <ul style="list-style-type: none"> <li>• Sur la sécurité des logiciels en rapport avec leur fonction et leurs langages de développement.</li> <li>• Inclure la conception de logiciels sécurisés et les techniques de codage sécurisé.</li> <li>• Inclure, si des outils de test de sécurité sont utilisés, la manière d'utiliser les outils pour détecter les vulnérabilités dans les logiciels.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.2.2.a</b> Examiner les procédures de développement de logiciels afin de vérifier que les processus sont définis pour la formation du personnel développeur de logiciels, développant des logiciels sur mesure et personnalisés qui incluent tous les éléments spécifiés dans cette exigence.</p> <p><b>6.2.2.b</b> Examiner l'historique des formations et interroger le personnel afin de vérifier que le personnel développeur de logiciels travaillant sur des logiciels sur mesure et personnalisés a reçu une formation en sécurité logicielle adaptée à sa fonction et ses langages de développement conformément à tous les éléments spécifiés dans la présente exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le personnel développeur de logiciels reste informé des pratiques de développement sécurisé ; de la sécurité des logiciels ; et des attaques contre les langages, les frameworks ou les applications qu'ils développent. Le personnel peut accéder à une assistance et à des conseils en cas de besoin.</p>	<p><b>Objectif</b> Le fait d'avoir du personnel connaissant les méthodes de codage sécurisé, y compris les techniques définies dans l'exigence 6.2.4, aidera à minimiser le nombre de vulnérabilités de sécurité introduites par de mauvaises pratiques de codage.</p> <p><b>Bonne Pratique</b> La formation des développeurs peut être assurée en interne ou par des tiers.</p> <p>La formation doit inclure, sans toutefois s'y limiter, les langages de développement utilisés, la conception de logiciels sécurisés, les techniques de codage sécurisé, l'utilisation de techniques/méthodes pour déceler des vulnérabilités dans le code, les processus pour empêcher la réintroduction de vulnérabilités précédemment résolues et la manière d'utiliser des outils de tests de sécurité automatisés pour détecter les vulnérabilités dans les logiciels.</p> <p>À mesure que les pratiques de codage sécurisé acceptées par l'industrie changent, les pratiques de codage organisationnel et la formation des développeurs peuvent devoir être mises à jour pour faire face aux nouvelles menaces.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.2.3</b> Les logiciels sur mesure et personnalisés sont examinés avant d'être mis en production ou envoyés aux clients, afin d'identifier et de corriger les vulnérabilités de codage potentielles, comme suit :</p> <ul style="list-style-type: none"> <li>• Les examens de code garantissent que le code est développé conformément aux directives de codage sécurisé.</li> <li>• Les examens de code recherchent les vulnérabilités logicielles existantes et émergentes.</li> <li>• Des corrections appropriées sont mises en œuvre avant la publication.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.2.3.a</b> Examiner les procédures de développement de logiciels documentées et interroger le personnel responsable afin de vérifier que les processus sont définis et que tous les logiciels sur mesure et personnalisés doivent être examinés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>6.2.3.b</b> Examiner les preuves des modifications apportées aux logiciels sur mesure et personnalisés afin de vérifier que les modifications du code ont été examinées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les logiciels sur mesure et personnalisés ne peuvent pas être exploités via des vulnérabilités de codage.</p>	<p><b>Objectif</b> Les failles de sécurité des logiciels sur mesure et personnalisés sont couramment exploitées par des personnes malveillantes pour accéder à un réseau et compromettre les données de carte. Un code vulnérable est beaucoup plus difficile et coûteux à traiter une fois qu'il a été déployé ou publié dans des environnements de production. L'exigence d'un examen formel et d'une approbation par la direction avant la publication permet de garantir que le code est approuvé et a été développé conformément aux politiques et procédures.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence d'examen de code s'applique à tous les logiciels sur mesure et personnalisés (à la fois internes et publics), dans le cadre du cycle de vie du développement système.</p> <p>Les applications Web accessibles au public sont également soumises à des mesures de sécurité supplémentaires, afin de faire face aux menaces et vulnérabilités en cours après la mise en œuvre, comme défini dans l'exigence 6.4 du standard PCI DSS.</p> <p>Les examens de code peuvent être effectués à l'aide de processus manuels ou automatisés, ou d'une combinaison des deux.</p>	<p><b>Bonne Pratique</b> Les éléments suivants doivent être pris en compte pour l'inclusion dans les examens du code :</p> <ul style="list-style-type: none"> <li>• Recherche de fonctionnalités non documentées (outils d'implantation, portes dérobées).</li> <li>• Confirmation que le logiciel utilise de manière sécurisée les fonctions des composants externes (bibliothèques, frameworks, API, etc.). Par exemple, si une bibliothèque tierce fournissant des fonctions cryptographiques est utilisée, vérifiez qu'elle a été intégrée de manière sécurisée.</li> <li>• Vérification de la bonne utilisation de la journalisation afin d'empêcher les données sensibles d'entrer dans les journaux.</li> <li>• Analyse des structures non sécurisées du code pouvant contenir des vulnérabilités potentielles liées aux attaques logicielles courantes identifiées dans l'Exigences 6.2.4.</li> <li>• Vérification du comportement de l'application afin de détecter des vulnérabilités logiques.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.2.3.1</b> Si des examens manuels du code sont effectués sur des logiciels sur mesure et personnalisés avant la mise en production, les modifications de code sont :</p> <ul style="list-style-type: none"> <li>• Examinées par des personnes autres que l'auteur du code d'origine, et qui connaissent les techniques d'examen du code et les pratiques de codage sécurisé.</li> <li>• Examinées et approuvées par la direction avant la publication.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.2.3.1.a</b> Si des examens manuels du code sont effectués sur des logiciels sur mesure et personnalisés avant la mise en production, examiner les procédures de développement de logiciels documentées et interroger le personnel responsable afin de vérifier que les processus sont définis pour les examens manuels de code à effectuer, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>6.2.3.1.b</b> Examiner les preuves des modifications apportées aux logiciels sur mesure et personnalisés et interroger le personnel afin de vérifier que les examens manuels du code ont été effectués conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le processus d'examen de code manuel ne peut pas être contourné et est efficace pour découvrir les vulnérabilités de sécurité.</p>	<p><b>Objectif</b> Faire examiner le code par une personne autre que l'auteur d'origine, qui soit à la fois expérimentée dans les examens de code et bien informée sur les pratiques de codage sécurisé, minimise la possibilité qu'un code, contenant des erreurs de sécurité ou de logique et pouvant avoir une incidence sur la sécurité des données des titulaires de cartes soit publié dans un environnement de production. Exiger l'approbation de la direction que le code a été examiné limite la possibilité de contourner le processus.</p> <p><b>Bonne Pratique</b> Il a été constaté que le fait d'avoir une méthodologie d'examen formelle et des listes de contrôle des examens améliore la qualité du processus d'examen de code. L'examen de code est un processus fatigant, et pour cette raison, il est plus efficace lorsque les examinateurs ne n'examinent que de petites quantités de code à la fois. Pour maintenir l'efficacité des examens de code, il est avantageux de surveiller la charge de travail générale des examinateurs et de les faire examiner les applications avec lesquelles ils sont familiers. Les examens de code peuvent être effectués à l'aide de processus manuels ou automatisés, ou d'une combinaison des deux. Les autorisations qui reposent uniquement sur l'examen manuel du code doivent s'assurer que les examinateurs maintiennent leurs compétences grâce à une formation régulière à mesure que de nouvelles vulnérabilités sont découvertes et que de nouvelles méthodes de codage sécurisé sont recommandées. (suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Les examens manuels du code peuvent être effectués par du personnel interne compétent ou par du personnel tiers compétent.</p> <p>Une personne à qui la responsabilité du contrôle des versions a été officiellement confiée et qui n'est ni l'auteur du code d'origine ni l'examinateur du code remplit les critères de gestion.</p>	<p><b>Informations Complémentaires</b></p> <p>Voir le <i>Guide d'examen de code OWASP</i></p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.2.4</b> Des techniques d'ingénierie logicielle ou d'autres méthodes sont définies et utilisées par le personnel de développement de logiciels afin de prévenir ou d'atténuer les attaques logicielles courantes et les vulnérabilités associées, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>Attaques par injection, y compris SQL, LDAP, XPath ou d'autres failles de type commande, paramètre, objet, erreur ou injection.</li> <li>Attaques ciblant les données et les structures de données, y compris les tentatives de manipulation de tampons, de pointeurs, de données d'entrée ou de données partagées.</li> <li>Attaques ciblant l'utilisation de la cryptographie, y compris les tentatives d'exploitation d'implémentations cryptographiques, d'algorithmes, de suites de chiffrement ou de modes de fonctionnement faibles, non sécurisés ou inadéquats.</li> <li>Attaques contre la logique métier, y compris les tentatives d'abus ou de contournement des caractéristiques et fonctionnalités des applications via la manipulation d'API, de protocoles et de canaux de communication, de fonctionnalités côté consommateur ou d'autres fonctions et ressources du système ou de l'application. Cela comprend les scripts de site à site (XSS) et les altérations de requêtes de site à site (CSRF).</li> <li>Attaques contre les mécanismes de contrôle d'accès, y compris les tentatives pour contourner ou d'abuser des « credentials », de l'authentification ou des mécanismes d'autorisation, ou des tentatives d'exploiter les faiblesses de la mise en œuvre de ces mécanismes.</li> </ul> <p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.2.4</b> Examiner les procédures documentées et interroger le personnel responsable du développement de logiciels afin de vérifier que les techniques d'ingénierie logicielle ou d'autres méthodes sont définies et utilisées par les développeurs de logiciels sur mesure et personnalisés afin de prévenir ou atténuer toutes les attaques logicielles courantes, comme spécifié dans cette exigence.</p>	<p><b>Objectif</b></p> <p>La détection ou la prévention précoce des erreurs courantes qui entraînent un code vulnérable dans le processus de développement logiciel réduit la probabilité que de telles erreurs parviennent à la production et conduisent à une compromission. L'intégration de techniques et d'outils d'ingénierie formels dans le processus de développement permettra de détecter rapidement ces erreurs. Cette philosophie est parfois appelée « shift-left security ».</p> <p><b>Bonne Pratique</b></p> <p>Pour les logiciels sur mesure et personnalisés, l'entité doit s'assurer que le code est développé en se concentrant sur la prévention ou l'atténuation des attaques logicielles courantes, notamment :</p> <ul style="list-style-type: none"> <li>Tentative d'exploiter des vulnérabilités courantes de codage (bogues).</li> <li>Tentative d'exploiter les failles de conception du logiciel.</li> <li>Tentative d'exploiter les failles d'implémentation ou de configuration.</li> <li>Attaques d'énumération - attaques automatisées qui sont activement exploitées dans les mécanismes de paiement et de « credentials », d'authentification ou d'autorisation. Voir <i>PCI Perspectives blog</i> article <i>“Beware of Account Testing Attacks.”</i></li> </ul> <p>La recherche et la documentation de techniques d'ingénierie logicielle ou d'autres méthodes aident à définir comment les développeurs de logiciels empêchent ou atténuent diverses attaques logicielles par des fonctionnalités ou des contre-mesures qu'ils intègrent au logiciel.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<ul style="list-style-type: none"> <li>Attaques via toutes les vulnérabilités « à haut risque » identifiées dans le processus d'identification des vulnérabilités, telles qu'elles sont définies dans l'exigence 6.3.1.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les logiciels sur mesure et personnalisés ne peuvent pas être exploités via des attaques habituelles et des vulnérabilités associées.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à tous les logiciels développés pour ou par l'entité pour son propre usage. Cela inclut des logiciels à la fois sur mesure et personnalisés. Ceci ne s'applique pas aux logiciels tiers.</p>	<p>Cela peut inclure des mécanismes d'identification ou d'authentification, un contrôle d'accès, des routines de validation de saisie, etc. Les développeurs doivent être familiarisés avec les différents types de vulnérabilités et d'attaques potentielles, et utiliser des mesures afin d'éviter les vecteurs d'attaque potentiels lors du développement du code.</p> <p><b>Exemples</b></p> <p>Les techniques incluent des processus et des pratiques automatisés qui analysent le code au début du cycle de développement lorsque le code est archivé pour confirmer qu'aucune vulnérabilité n'est présente.</p>

Exigences et Procédures de Test	Directives
<p><b>6.3 Les vulnérabilités de sécurité sont identifiées et corrigées.</b></p> <p><b>Exigences de L'approche Définie</b></p> <p><b>6.3.1</b> Les vulnérabilités de sécurité sont identifiées et gérées de la manière suivante :</p> <ul style="list-style-type: none"> <li>• Les nouvelles vulnérabilités de sécurité sont identifiées à l'aide de sources reconnues par l'industrie pour les informations sur les vulnérabilités de sécurité, y compris les alertes des équipes internationales et nationales d'intervention en cas d'urgence informatique (CERT).</li> <li>• Les vulnérabilités se voient attribuer un classement de risques basé sur les meilleures pratiques de l'industrie et la prise en compte de l'incidence potentielle.</li> <li>• Les classements des risques identifient, au minimum, toutes les vulnérabilités considérées comme à haut risque ou critiques pour l'environnement.</li> <li>• Les vulnérabilités des logiciels sur mesure et personnalisés et des logiciels de tiers (par exemple les systèmes d'exploitation et les bases de données) sont couvertes.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les nouvelles vulnérabilités du système et des logiciels susceptibles d'avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles sont surveillées, cataloguées et évaluées en fonction des niveaux de risque.</p> <p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.3.1.a</b> Examiner les politiques et procédures d'identification et de gestion des vulnérabilités de sécurité afin de vérifier que les processus sont définis conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>6.3.1.b</b> Interroger le personnel responsable, examiner la documentation et observer les processus afin de vérifier que les vulnérabilités de sécurité sont identifiées et gérées conformément à tous les éléments spécifiés dans cette exigence.</p>	<p><b>Objectif</b></p> <p>La classification des risques (par exemple, comme critique, élevé, moyen ou faible) permet aux entreprises d'identifier, de hiérarchiser et de traiter plus rapidement les éléments présentant le risque le plus élevé et de réduire la probabilité que les vulnérabilités présentant le plus grand risque soient exploitées.</p> <p><b>Bonne Pratique</b></p> <p>Les méthodes d'évaluation des vulnérabilités et d'attribution des niveaux de risque varieront en fonction de l'environnement et de la stratégie d'évaluation des risques d'une entreprise. Lorsqu'une entité attribue des classements de son risque, elle doit envisager d'utiliser une méthodologie formelle, objective et justifiable qui décrit avec précision les risques des vulnérabilités qui soient pertinentes pour l'entreprise et qui se traduisent par une priorité de résolution appropriée attribuée par l'entité.</p> <p>La classification des risques doit au moins identifier toutes les vulnérabilités considérées comme un « haut risque » à l'environnement. En plus de la classification des risques, les vulnérabilités peuvent être considérées comme « critiques » si elles posent une menace imminente à l'environnement, ont une incidence sur les systèmes critiques et/ou pourraient potentiellement les mettre en péril si elles ne sont pas traitées. Des exemples de systèmes critiques peuvent comprendre des systèmes de sécurité, des dispositifs et systèmes destinés au public, des bases de données et autres systèmes qui stockent, traitent ou transmettent les données de titulaires de carte.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence n'est pas satisfaite par, et s'ajoute à l'exécution des analyses des vulnérabilités conformément aux exigences 11.3.1 et 11.3.2. Cette exigence vise un processus visant la surveillance active des sources de l'industrie pour les informations sur les vulnérabilités et pour que l'entité détermine la catégorisation des risques à associer à chaque vulnérabilité.</p>	<p>Les processus d'une organisation pour gérer les vulnérabilités doivent être intégrés à d'autres processus de gestion ; par exemple, la gestion des risques, la gestion des changements, la gestion des correctifs, la réponse aux incidents, la sécurité des applications, ainsi qu'une surveillance et une journalisation appropriées de ces processus. Ce processus devra inclure plusieurs sources d'informations sur les vulnérabilités, y compris des bases de données reconnues de l'industrie (par exemple, la US National Vulnerability Database), CERTS, les flux RSS, les informations obtenues des commerçants et de tiers, et les vulnérabilités identifiées via des analyses de vulnérabilités internes et externes (Exigences 11.3.1 et 11.3.2). Cela aidera à garantir que toutes les vulnérabilités sont correctement identifiées et traitées. Les processus doivent prendre en charge l'évaluation continue des vulnérabilités. Par exemple, une vulnérabilité initialement identifiée comme à faible risque pourrait passer à un risque plus élevé plus tard.</p> <p>En outre, des vulnérabilités, considérées individuellement comme présentant un risque faible ou moyen, pourraient collectivement présenter un risque élevé ou critique si elles sont présentes sur le même système, ou si elles sont exploitées sur un système à faible risque pouvant entraîner l'accès au CDE.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p><b>Exemples</b></p> <p>Certaines organisations qui émettent des alertes pour informer les entités des vulnérabilités urgentes nécessitant des correctifs/mises à jour immédiats sont les équipes nationales de préparation/réponse aux urgences informatiques (CERT) et les fournisseurs.</p> <p>Les critères de classement des vulnérabilités peuvent inclure la criticité d'une vulnérabilité identifiée dans une alerte du Forum of Incident Response and Security Teams (FIRST) ou d'une CERT, la prise en compte du score CVSS, la classification par le fournisseur et/ou le type de systèmes impactés.</p> <p><b>Informations Complémentaires</b></p> <p>Les sources fiables d'informations sur les vulnérabilités incluent les sites Web des fournisseurs, les listes de diffusion, ect.</p> <p>Si le logiciel est développé en interne, l'équipe de développement interne doit également prendre en compte les sources d'informations sur les nouvelles vulnérabilités susceptibles d'avoir des incidences sur les applications développées en interne. D'autres méthodes pour s'assurer que les nouvelles vulnérabilités sont identifiées comportent des solutions qui reconnaissent et émettent automatiquement des alertes lors de la détection d'un comportement inhabituel. Les processus doivent tenir compte des codes malveillants largement publiés ainsi que des attaques « zero-day », qui ciblent des vulnérabilités auparavant inconnues.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p>Pour les logiciels sur mesure et personnalisés, l'entreprise peut obtenir des informations sur les bibliothèques, les frameworks, les compilateurs, les langages de programmation, etc. à partir de sources publiques de confiance (par exemple, des ressources spéciales et des ressources de développeurs de composants). L'entreprise peut également analyser indépendamment des composants tiers et identifier les vulnérabilités.</p> <p>Pour contrôler les logiciels développés en interne, l'entreprise peut recevoir ces informations de sources externes. L'entreprise peut envisager d'utiliser un programme de « bug bounty » où elle publie des informations (par exemple, sur son site Web) afin que des tiers puissent contacter l'entreprise avec des informations sur la vulnérabilité.</p> <p>Les sources externes peuvent inclure des enquêteurs indépendants ou des entreprises qui rendent compte à l'organisation des vulnérabilités identifiées et peuvent inclure des sources telles que le Common Vulnerability Scoring System (CVSS) ou la méthodologie d'évaluation des risques de l'OWASP.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>6.3.2</b> Un inventaire des logiciels sur mesure et personnalisés ainsi que des composants logiciels tiers intégrés dans des logiciels sur mesure et personnalisés est conservé afin de faciliter la gestion des vulnérabilités et des correctifs.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>6.3.2.a</b> Examiner la documentation et interroger le personnel afin de vérifier qu'un inventaire des logiciels sur mesure et personnalisés et des composants logiciels tiers intégrés aux logiciels sur mesure et personnalisés est maintenu, et que l'inventaire est utilisé afin d'identifier et corriger les vulnérabilités.</p> <p><b>6.3.2.b</b> Examiner la documentation du logiciel, y compris pour les logiciels sur mesure et personnalisés qui intègrent des composants logiciels tiers, et la comparer à l'inventaire afin de vérifier que l'inventaire comprend les logiciels sur mesure et personnalisés et les composants logiciels tiers.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les vulnérabilités connues dans les composants logiciels tiers ne peuvent pas être exploitées dans les logiciels sur mesure et personnalisés.</p>	
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> L'identification et l'énumération de tous les logiciels sur mesure et personnalisés de l'entité, ainsi que de tout logiciel tiers intégré aux logiciels sur mesure et personnalisés de l'entité, permettent à l'entité de gérer les vulnérabilités et les correctifs. Les vulnérabilités des composants tiers (y compris les bibliothèques, les API, etc.) intégrés au logiciel d'une entité rendent également ces applications vulnérables aux attaques. Il est essentiel de savoir quels composants tiers sont utilisés dans le logiciel de l'entité et de surveiller la disponibilité des correctifs de sécurité pour corriger les vulnérabilités connues afin de garantir la sécurité du logiciel. <b>Bonne Pratique</b> L'inventaire d'une entité doit couvrir tous les composants et dépendances du logiciel de paiement, y compris les plates-formes ou environnements d'exécution pris en charge, les bibliothèques tierces, les services et autres fonctionnalités obligatoires. Il existe de nombreux types de solutions qui peuvent aider à gérer les inventaires de logiciels, tels que les outils d'analyse de la composition logicielle, les outils de découverte d'applications et la gestion des appareils mobiles.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.3.3</b> Tous les composants système sont protégés contre les vulnérabilités connues en installant les correctifs/mises à jour de sécurité applicables comme suit :</p> <ul style="list-style-type: none"> <li>• Les correctifs/mises à jour pour des vulnérabilités critiques (identifiés selon le processus de classement des risques énoncé à l'exigence 6.3.1) sont installés dans le mois suivant leur publication.</li> <li>• Tous les autres correctifs/mises à jour de sécurité applicables sont installés dans un délai approprié déterminé par l'évaluation par l'entité de la criticité du risque à l'environnement tel qu'identifié selon le processus de classification des risques dans l'Exigence 6.3.1.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.3.3.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour traiter les vulnérabilités en installant les correctifs/mises à jour de sécurité applicables conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>6.3.3.b</b> Examiner les composants système et les logiciels associés et comparer la liste des correctifs/mises à jour de sécurité installés aux informations les plus récentes sur les correctifs/mises à jour de sécurité afin de vérifier que les vulnérabilités sont corrigées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les composants système ne peuvent pas être compromis par l'exploitation d'une vulnérabilité connue.</p>	<p><b>Objectif</b> De nouveaux exploits sont constamment découverts, et ceux-ci peuvent permettre des attaques contre des systèmes qui étaient auparavant considérés comme sécurisés. Si les correctifs/mises à jour de sécurité les plus récents ne sont pas mis en œuvre sur les systèmes critiques dès que possible, une personne malveillante peut utiliser ces exploits pour attaquer ou désactiver un système ou accéder à des données sensibles.</p> <p><b>Bonne Pratique</b> La hiérarchisation des correctifs/mises à jour de sécurité pour les infrastructures critiques garantit que les systèmes et appareils hautement prioritaires sont protégés des vulnérabilités dès que possible après la publication d'un correctif. La fréquence de mise à jour d'une entité doit tenir compte de toute réévaluation des vulnérabilités et des changements ultérieurs de la criticité d'une vulnérabilité conformément à l'exigence 6.3.1. Par exemple, une vulnérabilité initialement identifiée comme à faible risque pourrait passer à un risque plus élevé plus tard. En outre, des vulnérabilités, considérées individuellement comme présentant un risque faible ou moyen, pourraient collectivement présenter un risque élevé ou critique si elles sont présentes sur le même système, ou si elles sont exploitées sur un système à faible risque pouvant entraîner l'accès au CDE.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Il est recommandé que l'entité mène une analyse de risques ciblée (TRA) conformément à l'Exigence 12.3.1 pour documenter la fréquence d'installation de tous les autres correctifs/mises à jour. Cette TRA comporterait une considération de l'évaluation par l'entité de la criticité du risque à leur environnement comme identifié dans le processus de classification des risques dans l'Exigence 6.3.1.</p> <p><b>Exemples</b></p> <p>Un exemple de calendrier pour l'installation des correctifs/mises à jour pourrait être 60 jours pour les vulnérabilités à haut risque et 90 jours pour les autres, comme déterminé par l'évaluation des risques de l'entité.</p>

Exigences et Procédures de Test	Directives
<b>6.4 Les applications Web destinées au public sont protégées contre les attaques.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.4.1</b> Pour les applications Web destinées au public, les nouvelles menaces et vulnérabilités sont traitées en permanence, et ces applications sont protégées contre les attaques connues comme suit :</p> <ul style="list-style-type: none"> <li>• Examiner les applications Web accessibles au public grâce à des outils ou des méthodes manuels ou automatisés d'évaluation de la sécurité des vulnérabilités des applications, comme suit : <ul style="list-style-type: none"> <li>– Au moins une fois tous les 12 mois et après des modifications importantes.</li> <li>– Par une entité spécialisée dans la sécurité des applications.</li> <li>– Y compris, au minimum, toutes les attaques logicielles courantes énoncées dans l'exigence 6.2.4.</li> <li>– Toutes les vulnérabilités sont classées conformément à l'exigence 6.3.1.</li> <li>– Toutes les vulnérabilités sont corrigées.</li> <li>– L'application est réévaluée après les corrections</li> </ul> </li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• L'installation d'une ou plusieurs solutions techniques automatisées qui détectent et empêchent en permanence les attaques basées sur le Web, comme suit : <ul style="list-style-type: none"> <li>– Installé devant les applications Web destinées au public afin de détecter et empêcher les attaques Web.</li> </ul> <i>(suite à la page suivante)</i> </li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.4.1</b> Pour les applications Web destinées au public, s'assurer que l'une des méthodes requises est en place comme suit :</p> <ul style="list-style-type: none"> <li>• Si des outils ou des méthodes manuels ou automatisés d'évaluation de la sécurité des vulnérabilités sont utilisés, examiner les processus documentés, interroger le personnel et examiner les enregistrements des évaluations de la sécurité des applications afin de vérifier que les applications Web destinées au public sont examinées conformément à tous les éléments de cette exigence spécifiques à l'outil ou à la méthode.</li> </ul> <p><b>OU</b></p> <ul style="list-style-type: none"> <li>• Si une ou plusieurs solutions techniques automatisées sont installées qui détectent et empêchent en permanence les attaques Web, examiner les paramètres de configuration du système et les journaux d'audit, et interroger le personnel responsable afin de vérifier que la ou les solutions techniques automatisées sont installées conformément à tous les éléments de cette exigence spécifique à la ou aux solutions.</li> </ul>

Exigences et Procédures de Test	Directives
<ul style="list-style-type: none"> <li>– En exécution active et à jour, le cas échéant.</li> <li>– Génération de journaux d'audit.</li> <li>– Configuré pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée.</li> </ul>	<p>Les technologies RASP (Runtime Application Self-Protection) sont un autre exemple de solution technique automatisée. Lorsqu'elles sont correctement mises en œuvre, les solutions RASP peuvent détecter et bloquer les comportements anormaux du logiciel pendant l'exécution. Alors que les WAF surveillent généralement le périmètre de l'application, les solutions RASP surveillent et bloquent le comportement au sein de l'application.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les applications Web destinées au public sont protégées contre les attaques malveillantes.</p>	
<b>Notes D'applicabilité</b> <p>Cette évaluation n'est pas la même que les analyses de vulnérabilité effectuées pour les exigences 11.3.1 et 11.3.2.</p> <p>Cette exigence sera remplacée par l'exigence 6.4.2 après le 31 mars 2025 lorsque l'exigence 6.4.2 entrera en vigueur.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.4.2</b> Pour les applications Web destinées au public, une solution technique automatisée est déployée qui détecte et empêche en permanence les attaques Web, avec au moins les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Est installée devant les applications Web destinées au public et configurée afin de détecter et empêcher les attaques Web.</li> <li>• En exécution active et à jour, le cas échéant.</li> <li>• Génération de journaux d'audit.</li> <li>• Configurée pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.4.2</b> Pour les applications Web destinées au public, examiner les paramètres de configuration système et les journaux d'audit, et interroger le personnel responsable afin de vérifier qu'une solution technique automatisée qui détecte et empêche les attaques Web est en place conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les applications Web destinées au public sont protégées en temps réel contre les attaques malveillantes.</p>	<p><b>Objectif</b> Les applications destinées au public sont les principales cibles des attaques, et les applications Web mal codées offrent aux attaques un moyen facile d'accéder aux données et systèmes sensibles.</p> <p><b>Bonne Pratique</b> Lors de l'utilisation de solutions techniques automatisées, il est important d'inclure des processus qui facilitent les réponses rapides aux alertes générées par les solutions afin que toute attaque détectée puisse être atténuée. Ces solutions peuvent également être utilisées pour automatiser l'atténuation, par exemple des mesures de sécurité de limitation de débit, qui peuvent être mis en œuvre afin d'atténuer les attaques par force brute et les attaques par énumération.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette nouvelle exigence remplacera l'exigence 6.4.1 une fois sa date d'entrée en vigueur atteinte.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Exemples</b> Un pare-feu d'applications Web (WAF), qui peut être sur site ou basé sur le cloud, installé devant les applications Web destinées au public pour vérifier tout le trafic est un exemple de solution technique automatisée qui détecte et empêche les attaques Web (par exemple, les attaques énoncées dans l'exigence 6.2.4). Les WAF filtrent et bloquent le trafic non essentiel au niveau de la couche application. Un WAF correctement configuré permet d'empêcher les attaques de la couche application sur les applications mal codées ou mal configurées.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.4.3</b> Tous les scripts de la page de paiement qui sont chargés et exécutés dans le navigateur du consommateur sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>• Une méthode est mise en œuvre pour confirmer que chaque script est autorisé.</li> <li>• Une méthode est mise en œuvre pour assurer l'intégrité de chaque script.</li> <li>• Un inventaire de tous les scripts est maintenu avec une justification commercial ou technique écrite expliquant pourquoi chacun est nécessaire.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.4.3.a</b> Examiner les politiques et procédures afin de vérifier que des processus sont définis pour gérer tous les scripts de page de paiement qui sont chargés et exécutés dans le navigateur du consommateur, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>6.4.3.b</b> Interroger le personnel responsable et examiner les enregistrements d'inventaire et les configurations système afin de vérifier que tous les scripts de page de paiement qui sont chargés et exécutés dans le navigateur du consommateur sont gérés conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un code non autorisé ne peut pas être exécuté sur la page de paiement car il est affiché dans le navigateur du consommateur.</p>	<p><b>Objectif</b></p> <p>Les scripts chargés et exécutés dans la page de paiement peuvent voir leur fonctionnalité modifiée à l'insu de l'entité et peuvent également avoir la fonctionnalité de charger d'autres scripts externes (par exemple, publicité et suivi, systèmes de gestion des balises). Ces scripts apparemment inoffensifs peuvent être utilisés par des attaquants potentiels pour télécharger des scripts malveillants capables de lire et d'exfiltrer les données des titulaires de cartes à partir du navigateur du consommateur. S'assurer que la fonctionnalité de tous ces scripts est comprise comme étant nécessaire au fonctionnement de la page de paiement minimise le nombre de scripts qui pourraient être falsifiés. S'assurer que les scripts ont été explicitement autorisés réduit la probabilité que des scripts inutiles soient ajoutés à la page de paiement sans l'approbation adéquate de la direction. Lorsqu'il s'avère irréalisable que cette autorisation ait lieu avant qu'un script ne soit modifié ou un nouveau script ajouté à la page, l'autorisation devra être confirmée dès que possible après la mise en œuvre de la modification. L'utilisation de techniques pour empêcher l'altération du script minimisera la probabilité que le script soit modifié pour effectuer un comportement non autorisé, tel que l'écrémage des données des titulaires de cartes à partir de la page de paiement.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à tous les scripts chargés à partir de l'environnement de l'entité et aux scripts chargés à partir de tiers et de quatrièmes parties.</p> <p>Cette exigence s'applique également aux scripts présents dans la ou les pages Web de l'entité qui incluent la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un ou plusieurs cadres en ligne ou iframes).</p> <p>Cette exigence ne s'applique pas à une entité pour les scripts dans la page/formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, une ou plusieurs iframes), lorsque l'entité inclut la page/formulaire de paiement d'un TPSP/processeur de paiement sur sa page Web. Il incombe au TPSP/processeur de paiement de gérer les scripts dans la page/le formulaire de paiement intégré du TPSP/processeur de paiement conformément à cette exigence.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Bonne Pratique</b></p> <p>Les scripts peuvent être autorisés par des processus manuels ou automatisés (par exemple, flux de travail).</p> <p>Lorsque la page de paiement sera chargée dans un cadre en ligne (iframe), en restreignant l'emplacement à partir duquel la page de paiement peut être chargée, l'utilisation de la politique de sécurité du contenu (CSP) de la page parente peut aider à empêcher du contenu non autorisé de se substituer à la page de paiement.</p> <p>Lorsqu'une entité inclut la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement sur sa page Web, l'entité doit s'attendre à ce que le TPSP/processeur de paiement fournit la preuve que le TPSP/processeur de paiement satisfait à cette exigence, conformément à l'évaluation PCI DSS du TPSP/processeur de paiement et à l'Exigence 12.9.</p> <p><b>Exemples</b></p> <p>L'intégrité des scripts peut être renforcée par plusieurs mécanismes différents, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• L'intégrité des sous-ressources (SRI), qui permet au navigateur du consommateur de valider qu'un script n'a pas été falsifié.</li> <li>• Une CSP, qui limite les emplacements à partir desquels le navigateur du consommateur peut charger un script et y transmettre des données de carte.</li> <li>• Des systèmes de gestion de scripts ou de balises propriétaires, qui peuvent empêcher l'exécution de scripts malveillants.</li> </ul>

Exigences et Procédures de Test	Directives
<b>6.5 Les modifications apportées à tous les composants système sont gérées de manière sécurisée.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.5.1</b> Les modifications apportées à tous les composants système dans l'environnement de production sont effectuées conformément aux procédures établies qui comportent :</p> <ul style="list-style-type: none"> <li>• Raison et description du changement.</li> <li>• Documentation de l'impact sur la sécurité.</li> <li>• Approbation des changements documentée par les parties autorisées.</li> <li>• Tests pour vérifier que le changement n'a pas d'incidence négative sur la sécurité du système.</li> <li>• Pour les changements apportés aux logiciels sur mesure et personnalisés, toutes les mises à jour sont testées afin de vérifier leur conformité à l'exigence 6.2.4 avant d'être déployées en production.</li> <li>• Procédures pour la résolution des échecs et le retour à un état sécurisé.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.5.1.a</b> Examiner les procédures documentées de contrôle des modifications afin de vérifier que des procédures sont définies pour les modifications apportées à tous les composants système dans l'environnement de production afin d'inclure tous les éléments spécifiés dans cette exigence.</p> <p><b>6.5.1.b</b> Examiner les modifications récentes apportées aux composants système et retracer ces modifications jusqu'à la documentation de contrôle des modifications associée. Pour chaque modification examinée, vérifier que les modifications sont mises en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Toutes les modifications sont suivies, autorisées et évaluées en termes d'impact et de sécurité, et les modifications sont gérées afin d'éviter les effets imprévus sur la sécurité des composants système.</p>	<p><b>Objectif</b></p> <p>Des procédures de gestion des modifications doivent être appliquées à toutes les modifications, y compris l'ajout, la suppression ou la modification de tout composant système, dans l'environnement de production. Il est important de documenter la raison d'une modification et la description de la modification afin que les parties concernées comprennent et conviennent que la modification est nécessaire. De même, la documentation des impacts des modifications permet à toutes les parties concernées de planifier de manière appropriée toutes modifications apportées au traitement.</p> <p><b>Bonne Pratique</b></p> <p>L'approbation par les parties autorisées confirme que le changement est légitime et que les modifications sont sanctionnées par l'entreprise. Les modifications doivent être approuvées par des personnes ayant l'autorité et les connaissances appropriées pour comprendre l'impact des modifications.</p> <p>Des tests approfondis par l'entité confirment que la sécurité de l'environnement n'est pas réduite par la mise en œuvre d'un changement et que tous les mesures de sécurité de sécurité existants restent en place ou sont remplacés par des mesures de sécurité de sécurité égaux ou plus robustes après le changement. Les tests spécifiques à effectuer varieront en fonction du type de changement et des composants systèmes concernés.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Pour chaque modification, il est important d'avoir des procédures documentées qui résolvent toute défaillance et fournissent des instructions sur la façon de revenir à un état sécurisé au cas où la modification échouerait ou aurait une incidence négative sur la sécurité d'une application ou d'un système. Ces procédures permettront de restaurer l'application ou le système à son état sécurisé précédent.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.5.2</b> Suite à modifications importantes, toutes les exigences applicables du standard PCI DSS sont confirmées être en place sur tous les systèmes et réseaux nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.5.2</b> Examiner la documentation pour les modifications importantes, interroger le personnel et observer les systèmes/réseaux touchés afin de vérifier que l'entité a confirmé que les exigences applicables du standard PCI DSS étaient en place sur tous les systèmes et réseaux nouveaux ou modifiés et que la documentation a été mise à jour, le cas échéant.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Tous les composants du système sont vérifiés après une modification importante et qu'ils sont conformes aux exigences applicables du standard PCI DSS.</p>	<p><b>Objectif</b> Disposer de processus pour analyser les modifications importantes permet de garantir que tous les mesures de sécurité appropriée du standard PCI DSS sont appliquées à tous les systèmes ou réseaux ajoutés ou modifiés sur l'environnement dans le périmètre, et que les exigences du standard PCI DSS continuent d'être respectées pour sécuriser l'environnement.</p> <p><b>Bonne Pratique</b> L'intégration de cette validation dans les processus de gestion des modifications permet de garantir que les inventaires des appareils et les standards de configuration sont tenus à jour et que des mesures de sécurité de sécurité sont appliqués, si nécessaire.</p> <p><b>Exemples</b> Les exigences applicables du standard PCI DSS qui pourraient être touchées incluent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Les diagrammes de réseau et de flux de données sont mis à jour pour refléter les modifications.</li> <li>• Les systèmes sont configurés selon les standards de configuration, avec tous les mots de passe par défaut modifiés et les services inutiles désactivés.</li> <li>• Les systèmes sont protégés par les mesures requises, par exemple, la surveillance de l'intégrité des fichiers (FIM), anti-programmes malveillants, les correctifs et la journalisation des audits.</li> </ul> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Ces modifications importantes doivent également être capturées et reflétées dans l'activité annuelle de confirmation du périmètre du standard PCI DSS de l'entité conformément à l'exigence 12.5.2.</p>	<ul style="list-style-type: none"> <li>Les données d'authentification sensibles ne sont pas stockées et tout le stockage des données de carte est documenté et intégré à la politique et aux procédures de conservation des données.</li> <li>De nouveaux systèmes sont inclus dans le processus trimestriel d'analyse des vulnérabilités.</li> <li>Les systèmes sont analysés pour détecter les vulnérabilités internes et externes après des modifications importantes conformément aux exigences 11.3.1.3 et 11.3.2.1.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.5.3</b> Les environnements de pré-production sont séparés des environnements de production et la séparation est appliquée avec des mesures de sécurité d'accès.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.5.3.a</b> Examiner les politiques et procédures afin de vérifier que des processus sont définis pour séparer l'environnement de pré-production de l'environnement de production par des mesures de sécurité d'accès qui imposent la séparation.</p> <p><b>6.5.3.b</b> Examiner la documentation réseau et les configurations des mesures de sécurité de réseau afin de vérifier que l'environnement de pré-production est séparé du ou des environnements de production.</p> <p><b>6.5.3.c</b> Examiner les paramètres de contrôle d'accès afin de vérifier que des mesures de sécurité d'accès sont en place pour imposer la séparation entre les environnements de pré-production et de production.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les environnements de pré-production ne peuvent pas introduire de risques et de vulnérabilités dans les environnements de production.</p>	<p><b>Objectif</b> En raison de l'état en constante évolution des environnements de pré-production, ils sont souvent moins sécurisés que l'environnement de production.</p> <p><b>Bonne Pratique</b> Les entreprises doivent clairement comprendre quels environnements sont des environnements de test ou des environnements de développement et comment ces environnements interagissent au niveau des réseaux et des applications.</p> <p><b>Définitions</b> Les environnements de pré-production incluent le développement, les tests, les tests d'acceptation par l'utilisateur (UAT), etc. Même lorsque l'infrastructure de production est utilisée pour faciliter les tests ou le développement, les environnements de production doivent toujours être séparés (logiquement ou physiquement) des fonctionnalités de pré-production afin que les vulnérabilités introduites à la suite des activités de pré-production n'affectent pas négativement les systèmes de production.</p>

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>6.5.4</b> Les rôles et les fonctions sont séparés entre les environnements de production et de pré-production afin d'assurer la responsabilité de sorte que seules les modifications examinées et approuvées soient déployées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>6.5.4.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour séparer les rôles et les fonctions afin d'assurer la responsabilité de sorte que seules les modifications examinées et approuvées soient déployées.</p>	<b>Objectif</b> L'objectif de la séparation des rôles et des fonctions entre les environnements de production et de pré-production est de réduire le nombre de personnes ayant accès à l'environnement de production et aux données de carte, et ainsi minimiser le risque d'accès non autorisé, involontaire ou inapproprié aux données et aux composants système, et aider à garantir que l'accès est limité aux personnes ayant un besoin professionnel pour un tel accès.
<b>Objectif de L'approche Personnalisée</b> Les rôles et la responsabilité qui diffèrent les activités de pré-production et de production sont définis et gérés afin de minimiser le risque d'actions non autorisées, involontaires ou inappropriées.	<p><b>6.5.4.b</b> Observer les processus et interroger le personnel afin de vérifier que les mesures de sécurité mis en œuvre séparent les rôles et les fonctions et assurent la responsabilité de sorte que seules les modifications examinées et approuvées soient déployées.</p>	L'objectif de ce contrôle est de séparer les activités critiques pour assurer une surveillance et un examen afin de détecter les erreurs et de minimiser les risques de fraude ou de vol (puisque deux personnes devraient s'entendre pour masquer une activité).
<b>Notes D'applicabilité</b> Dans les environnements avec un personnel limité où les individus remplissent plusieurs rôles ou fonctions, ce même objectif peut être atteint avec des mesures de sécurité procéduraux supplémentaires qui garantissent la responsabilité. Par exemple, un développeur peut également être un administrateur qui utilise un compte de niveau administrateur avec des priviléges élevés dans l'environnement de développement ; et, pour son rôle de développeur, il utilise un compte distinct avec un accès de niveau utilisateur dans l'environnement de production.		La séparation des rôles et des fonctions, également appelée séparation ou ségrégation des tâches, est un concept de contrôle interne essentiel pour protéger les actifs d'une entité.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>6.5.5</b> Les PAN actifs ne sont pas utilisés dans les environnements de pré-production, sauf lorsque ces environnements sont inclus dans le CDE et protégés conformément à toutes les exigences applicables du standard PCI DSS.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>6.5.5.a</b> Examiner les politiques et procédures afin de vérifier que les processus sont définis pour ne pas utiliser de PAN actifs dans les environnements de pré-production, sauf lorsque ces environnements sont dans un CDE et protégés conformément à toutes les exigences applicables du standard PCI DSS.</p> <p><b>6.5.5.b</b> Observer les processus de test et interroger le personnel afin de vérifier que des procédures sont en place pour garantir que les PAN actifs ne sont pas utilisés dans les environnements de pré-production, sauf lorsque ces environnements sont dans un CDE et protégés conformément à toutes les exigences applicables du standard PCI DSS.</p> <p><b>6.5.5.c</b> Examiner les données de test de pré-production afin de vérifier que les PAN actifs ne sont pas utilisés dans les environnements de pré-production, sauf lorsque ces environnements sont dans un CDE et protégés conformément à toutes les exigences applicables du standard PCI DSS.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les PAN actifs ne peuvent pas être présents dans les environnements de pré-production en dehors du CDE.</p>	<p><b>Objectif</b> L'utilisation de PAN actifs en dehors des CDE protégés offre aux personnes malveillantes la possibilité d'accéder sans autorisation aux données des titulaires de cartes.</p> <p><b>Définitions</b> Les PAN actifs font référence à des PAN valides (pas des PAN de test) émis par, ou au nom d'une marque de paiement. De plus, lorsque les cartes de paiement expirent, le même PAN est souvent réutilisé avec une date d'expiration différente. Tous les PAN doivent être vérifiés comme étant incapables d'effectuer des transactions de paiement ou posent un risque de fraude au système de paiement avant d'être exclus du périmètre du standard PCI DSS. Il est de la responsabilité de l'entité de confirmer que les PAN ne sont pas actifs.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>6.5.6</b> Les données de test et les comptes de test sont supprimés des composants système avant que le système ne passe en production.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>6.5.6.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour la suppression des données de test et des comptes de test des composants système avant que le système ne passe en production.</p> <p><b>6.5.6.b</b> Observer les processus de test pour les logiciels standard et les applications internes, et interroger le personnel afin de vérifier que les données de test et les comptes de test sont supprimés avant qu'un système ne démarre en mode production.</p> <p><b>6.5.6.c</b> Examiner les données et les comptes des logiciels commerciaux et des applications internes récemment installés ou mis à jour afin de vérifier qu'il n'y a pas de données de test ou de comptes de test sur les systèmes de production.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les données de test et les comptes de test ne peuvent pas exister dans les environnements de production.</p>	<b>Objectif</b> Ces données peuvent divulguer des informations sur le fonctionnement d'une application ou d'un système et constituent une cible facile à exploiter par des personnes non autorisées pour accéder aux systèmes. La possession de ces informations pourrait faciliter la compromission du système et des données de carte associées.

## Mettre en œuvre des Mesures Robustes de Contrôle D'accès

### **Exigence 7 : Limiter L'accès aux Composants Système et aux Données des Titulaires de Cartes en Fonction des Besoins de L'entreprise**

#### Sections

- 7.1 Les processus et les mécanismes de restriction de l'accès aux composants système et aux données des titulaires de cartes par l'entreprise doivent être définis et compris.
- 7.2 L'accès aux composants système et aux données du système est défini et attribué de manière adéquate.
- 7.3 L'accès aux composants et aux données système est géré via un ou plusieurs systèmes de contrôle d'accès.

#### Aperçu

Des personnes non autorisées peuvent accéder à des données ou à des systèmes critiques en raison de règles et de définitions de contrôle d'accès inefficaces. Pour garantir que les données critiques ne sont accessibles qu'au personnel autorisé, des systèmes et des processus doivent être en place afin de limiter l'accès en fonction du besoin d'en connaître et en fonction des responsabilités du poste.

Un « accès » ou des « droits d'accès » sont créés par des règles qui permettent aux utilisateurs d'accéder aux systèmes, aux applications et aux données, tandis que les « priviléges » permettent à un utilisateur d'effectuer une action ou une fonction spécifique en relation avec ce système, cette application ou ces données. Par exemple, un utilisateur peut avoir des droits d'accès à des données spécifiques, mais le fait qu'il puisse uniquement lire ces données, ou puisse également modifier ou supprimer les données est déterminé par les priviléges attribués à l'utilisateur.

Le « besoin d'en connaître » fait référence à l'accès à la plus petite quantité de données nécessaires à l'exécution d'une tâche.

Les « moindres priviléges » font référence au fait de ne fournir que le niveau minimum de priviléges nécessaires pour effectuer une tâche.

Ces exigences s'appliquent aux comptes d'utilisateurs et à l'accès des employés, sous-traitants, consultants, fournisseurs internes et externes et autres tiers (par exemple, pour fournir des services d'assistance ou de maintenance). Certaines exigences s'appliquent également aux comptes d'applications et système utilisés par l'entité (également appelés « comptes de service »).

**Ces exigences ne s'appliquent pas aux consommateurs (titulaires de cartes).**

Se reporter à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>7.1 Les processus et les mécanismes de restriction de l'accès aux composants système et aux données des titulaires de cartes par l'entreprise doivent être définis et compris.</b>	

Exigences de L'approche Définie	Procédures de Test de L'approche Définie	Objectif
<b>7.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 7 sont : <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>7.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 7 sont gérées conformément à tous les éléments spécifiés dans cette exigence.	<b>L'objectif</b> L'exigence 7.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 7. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 7, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.
<b>Objectif de L'approche Personnalisée</b>  Les attentes, les mesures de sécurité et la surveillance des activités de réunion dans l'exigence 7 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.		<b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique.  <b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 7 sont documentés, attribués et compris.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 7 sont documentées et attribuées.</p> <p><b>7.1.2.b</b> Interroger le personnel chargé d'exécuter les activités de l'exigence 7 afin de vérifier que les rôles et les responsabilités sont assignés comme documentés et qu'ils sont compris.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 7 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>7.2 L'accès aux composants système et aux données du système est défini et attribué de manière adéquate.</b>	
<b>Exigences de L'approche Définie</b> <p><b>7.2.1</b> Un modèle de contrôle d'accès est défini et inclut l'octroi d'accès comme suit :</p> <ul style="list-style-type: none"> <li>• Accès approprié en fonction de l'activité de l'entité et des besoins d'accès.</li> <li>• Accès aux composants système et aux ressources de données en fonction de la classification et des fonctions des utilisateurs.</li> <li>• Les moindres priviléges requis (par exemple, utilisateur, administrateur) pour exécuter une fonction.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>7.2.1.a</b> Examiner les politiques et procédures documentées et interroger le personnel afin de vérifier que le modèle de contrôle d'accès est défini conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.1.b</b> Examiner les paramètres du modèle de contrôle d'accès et vérifier que les besoins d'accès sont correctement définis conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les conditions d'accès sont établies selon les fonctions du poste suivant les principes des moindres priviléges et du besoin d'en connaître.</p>	<b>Objectif</b> La définition d'un modèle de contrôle d'accès adapté à la technologie et à la philosophie de contrôle d'accès de l'entité soutient une manière cohérente et uniforme d'attribuer l'accès et réduit la possibilité d'erreurs telles que l'octroi de droits excessifs. <b>Bonne Pratique</b> Un facteur à considérer lors de la définition des besoins d'accès est le principe de séparation des tâches. Ce principe vise à prévenir la fraude et l'abus ou le vol de ressources. Par exemple, 1) répartir les fonctions critiques et les fonctions de support du système d'information entre différentes personnes et/ou fonctions, 2) établir des rôles tels que les activités de support du système d'information sont exécutées par différentes fonctions/personnes (par exemple, gestion du système, programmation, gestion des configurations, assurance qualité et tests, et sécurité du réseau), et 3) s'assurer que le personnel de sécurité administrant les fonctions de contrôle d'accès n'administre pas également les fonctions d'audit. Dans les environnements où une seule personne exécute plusieurs fonctions, telles que les opérations d'administration et de sécurité, des tâches peuvent être attribuées de sorte qu'aucune personne n'ait le contrôle de bout en bout d'un processus sans un point de contrôle indépendant. Par exemple, la responsabilité de la configuration et la responsabilité de l'approbation des modifications pourraient être attribuées à des personnes distinctes. <i>(suite à la page suivante)</i>

Exigences et Procédures de Test	Directives
	<p><b>Définitions</b></p> <p>Les éléments clés d'un modèle de contrôle d'accès comprennent :</p> <ul style="list-style-type: none"> <li>• Les ressources à protéger (les systèmes/appareils/données auxquels l'accès est nécessaire),</li> <li>• Les fonctions de travail qui ont besoin d'accéder à la ressource (par exemple, administrateur système, personnel du centre d'appels, commis de magasin), et</li> <li>• Les activités que chaque fonction doit effectuer (par exemple, lecture/écriture ou requête).</li> </ul> <p>Une fois que les fonctions de travail, les ressources et les activités par fonction sont définies, les individus peuvent se voir accorder l'accès en conséquence.</p> <p><b>Exemples</b></p> <p>Les modèles de contrôle d'accès que les entités peuvent envisager comportent le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC). Le modèle de contrôle d'accès utilisé par une entité donnée dépend de ses besoins professionnels et d'accès.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.2.2</b> L'accès est attribué aux utilisateurs, y compris les utilisateurs privilégiés, selon :</p> <ul style="list-style-type: none"> <li>• La classification du poste et de la fonction.</li> <li>• Les moindres priviléges nécessaires pour exercer les responsabilités de la tâche.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.2.2.a</b> Examiner les politiques et procédures afin de vérifier qu'elles couvrent l'attribution de l'accès aux utilisateurs conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.2.b</b> Examiner les paramètres d'accès des utilisateurs, y compris pour les utilisateurs privilégiés, et interroger le personnel responsable de la gestion afin de vérifier que les priviléges attribués sont conformes à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.2.c</b> Interroger le personnel chargé d'attribuer l'accès afin de vérifier que l'accès des utilisateurs privilégiés est attribué conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'accès aux systèmes et aux données est limité uniquement à l'accès nécessaire à l'exécution des fonctions professionnelles, tel que défini dans les rôles d'accès associés.</p>	<p><b>Objectif</b> L'attribution de moindres priviléges permet d'empêcher les utilisateurs qui ne connaissent pas suffisamment l'application de modifier de manière incorrecte ou accidentelle la configuration de l'application ou de modifier ses paramètres de sécurité. L'application des moindres priviléges permet également de minimiser l'étendue des dommages si une personne non autorisée accède à un identifiant utilisateur.</p> <p><b>Bonne Pratique</b> Les droits d'accès sont accordés à un utilisateur par affectation à une ou plusieurs fonctions. L'accès est attribué selon les fonctions d'utilisateur spécifiques et avec le périmètre minimal requis pour la tâche.</p> <p>Lors de l'attribution d'un accès privilégié, il est important d'attribuer aux individus uniquement les priviléges dont ils ont besoin pour effectuer leur travail (les « moindres priviléges »). Par exemple, l'administrateur de base de données ou l'administrateur de sauvegarde ne doit pas disposer des mêmes priviléges que l'administrateur système global.</p> <p>Une fois les besoins définis pour les fonctions utilisateur (conformément à l'exigence 7.2.1 du standard PCI DSS), il est facile d'accorder l'accès aux personnes en fonction de la classification de leur poste et de leur fonction en utilisant les rôles déjà créés.</p> <p>Les entités peuvent envisager d'utiliser la gestion des accès privilégiés (PAM), qui est une méthode pour accorder l'accès aux comptes privilégiés uniquement lorsque ces priviléges sont requis, en révoquant immédiatement cet accès une fois qu'ils ne sont plus nécessaires.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>7.2.3</b> Les privilèges requis sont approuvés par un personnel autorisé.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>7.2.3.a</b> Examiner les politiques et procédures afin de vérifier qu'elles définissent des processus d'approbation de tous les privilèges par un personnel autorisé.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les privilèges d'accès ne peuvent pas être accordés aux utilisateurs sans autorisation appropriée et documentée.</p>	<b>Objectif</b> L'approbation documentée (par exemple, par écrit ou par voie électronique) garantit que les personnes disposant d'un accès et de privilèges sont connues et autorisées par la direction, et que leur accès est nécessaire pour leur fonction.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.2.4</b> Tous les comptes et les priviléges d'accès associés, y compris les comptes tiers/fournisseurs, sont examinés comme suit :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les six mois.</li> <li>• Pour garantir que les comptes d'utilisateurs et l'accès restent appropriés selon la fonction du poste.</li> <li>• Tout accès inapproprié est traité.</li> <li>• La direction reconnaît que l'accès demeure approprié.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.2.4.a</b> Examiner les politiques et les procédures afin de vérifier qu'elles définissent des processus pour examiner tous les comptes d'utilisateurs et les priviléges d'accès associés, y compris les comptes de tiers/fournisseurs, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.4.b</b> Interroger le personnel responsable et examiner les résultats documentés des examens périodiques des comptes d'utilisateurs afin de vérifier que tous les résultats sont conformes à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attributions de priviléges de compte sont vérifiées périodiquement par la direction comme étant correctes, et toute non-conformité est corrigée.</p>	<p><b>Objectif</b></p> <p>L'examen régulier des droits d'accès permet de détecter les droits d'accès excessifs restants après le changement des responsabilités professionnelles de l'utilisateur, le changement des fonctions du système ou autres changements. Si des droits excessifs d'un utilisateur ne sont pas révoqués en temps utile, ils peuvent être exploités par des utilisateurs malveillants pour un accès non autorisé. Cet examen offre une autre possibilité de s'assurer que les comptes de tous les utilisateurs ayant terminé leurs tâches ont été supprimés (le cas échéant, au moment de la fin de leurs tâches), ainsi que de s'assurer que tout tiers qui n'a plus besoin d'accès a vu son accès suspendu.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à tous les comptes d'utilisateurs et aux priviléges d'accès associés, y compris ceux utilisés par le personnel et les tiers/fournisseurs, et les comptes utilisés pour accéder aux services cloud de tiers.</p> <p>Voir les exigences 7.2.5 et 7.2.5.1 et 8.6.1 à 8.6.3 pour les mesures de sécurité des comptes d'application et système.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Bonne Pratique</b></p> <p>Lorsqu'un utilisateur est transféré dans un nouveau rôle ou un nouveau service, les priviléges et l'accès associés à son ancien rôle ne sont généralement plus nécessaire. L'accès continu à des priviléges ou fonctions qui ne sont plus nécessaires peut introduire un risque d'abus ou d'erreurs. Par conséquent, lorsque les responsabilités changent, les processus qui revalident l'accès aident à garantir que l'accès de l'utilisateur est approprié pour les nouvelles responsabilités dudit utilisateur.</p> <p>Les entités peuvent envisager de mettre en œuvre un processus régulier et reproductible pour effectuer des examens des droits d'accès et attribuer des « propriétaires de données » qui sont responsables de la gestion et de la surveillance de l'accès aux données liées à leur fonction, et qui garantissent également que l'accès des utilisateurs reste à jour et approprié.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>À titre d'exemple, un responsable direct pourrait examiner l'accès de l'équipe tous les mois, tandis que le responsable principal examine l'accès de ses groupes tous les trimestres, tous deux mettant à jour l'accès au besoin. Le but de ces meilleures pratiques est de soutenir et de faciliter l'opération des examens au moins une fois tous les 6 mois.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.2.5</b> Tous les comptes d'applications et système et les privilèges d'accès associés sont attribués et gérés comme suit :</p> <ul style="list-style-type: none"> <li>• Basé sur les moindres privilèges nécessaires à l'opérabilité du système ou de l'application.</li> <li>• L'accès est limité aux systèmes, applications ou processus qui nécessitent spécifiquement leur utilisation.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.2.5.a</b> Examiner les politiques et les procédures afin de vérifier qu'elles définissent des processus pour gérer et attribuer les comptes d'applications et système, et les privilèges d'accès associés conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les droits d'accès accordés aux comptes d'applications et système sont limités uniquement à l'accès nécessaire au fonctionnement de cette application ou de ce système.</p>	<p><b>7.2.5.b</b> Examiner les privilèges associés aux comptes système et d'applications, et interroger le personnel responsable afin de vérifier que les comptes d'applications et système et les privilèges d'accès associés sont attribués et gérés conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Objectif</b> Il est important d'établir le niveau d'accès approprié pour les comptes d'applications ou système. Si de tels comptes sont compromis, des utilisateurs malveillants recevront le même niveau d'accès que celui accordé à l'application ou au système. Par conséquent, il est important de garantir qu'un accès limité est accordé aux comptes système et d'applications sur la même base qu'aux comptes utilisateur.</p> <p><b>Bonne Pratique</b> Les entités peuvent envisager d'établir une base de référence lors de la configuration de ces comptes d'applications et système, y compris les éléments suivants, selon le cas de l'entreprise :</p> <ul style="list-style-type: none"> <li>• S'assurer que le compte n'est pas membre d'un groupe privilégié tel que les administrateurs de domaine, les administrateurs locaux ou root.</li> <li>• La restriction des ordinateurs sur lesquels le compte peut être utilisé.</li> <li>• La restriction des heures d'utilisation.</li> <li>• La suppression de tous les paramètres supplémentaires tels que l'accès VPN et l'accès à distance.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.2.5.1</b> Tous les accès par comptes d'applications et système et les priviléges d'accès associés sont examinés comme suit :</p> <ul style="list-style-type: none"> <li>• Périodiquement, (à la fréquence définie dans l'analyse de risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1).</li> <li>• L'accès à l'application ou au système reste approprié pour la fonction exécutée.</li> <li>• Tout accès inapproprié est traité.</li> <li>• La direction reconnaît que l'accès demeure approprié.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.2.5.1.a</b> Examiner les politiques et les procédures afin de vérifier qu'elles définissent des processus pour examiner tous les comptes d'applications et système et les priviléges d'accès associés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.5.1.b</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des examens périodiques des comptes d'applications et système, et des priviléges d'accès associés afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p> <p><b>7.2.5.1.c</b> Interroger le personnel responsable et examiner les résultats documentés des examens périodiques des comptes système et d'applications, et des priviléges associés afin de vérifier que les examens se déroulent conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attributions de priviléges de comptes d'applications et système sont vérifiées périodiquement par la direction comme étant correctes, et toute non-conformité est corrigée.</p>	<p><b>Objectif</b></p> <p>L'examen régulier des droits d'accès permet de détecter les droits d'accès excessifs restants après un changement de fonctions du système ou d'autres modifications de l'application ou du système. Si des droits excessifs ne sont pas supprimés lorsqu'ils ne sont plus nécessaires, ils peuvent être exploités par des utilisateurs malveillants pour un accès non autorisé.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>7.2.6</b> Tout accès utilisateur pour envoyer aux référentiels des requêtes de données de titulaires de cartes stockées est limité comme suit :</p> <ul style="list-style-type: none"> <li>• Via des applications ou d'autres méthodes programmatiques, avec accès et actions autorisées en fonction des rôles d'utilisateur et des moindres priviléges.</li> <li>• Seuls les administrateurs responsables peuvent accéder directement ou envoyer des requêtes aux référentiels de CHD stockés.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>7.2.6.a</b> Examiner les politiques et les procédures et interroger le personnel afin de vérifier que les processus sont définis pour accorder aux utilisateurs l'accès aux référentiels de requêtes des données stockées des titulaires de cartes, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>7.2.6.b</b> Examiner les paramètres de configuration pour envoyer des requêtes aux référentiels de données de titulaires de cartes stockées afin de vérifier qu'ils sont conformes à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'accès direct aux requêtes non filtrées (ad hoc) aux référentiels de données des titulaires de cartes est interdit, à moins qu'il ne soit effectué par un administrateur autorisé.</p>	<p><b>Objectif</b> L'utilisation abusive de l'accès par requête aux référentiels de données des titulaires de cartes a été une cause régulière de violations de données. La restriction d'un tel accès aux administrateurs réduit le risque qu'un tel accès soit mal utilisé par des utilisateurs non autorisés.</p> <p><b>Définitions</b> « Méthodes programmatiques » signifie accorder l'accès par des moyens tels que des procédures stockées dans la base de données qui permettent aux utilisateurs d'effectuer des actions contrôlées sur les données d'une table, plutôt que via un accès direct et non filtré au référentiel de données par les utilisateurs finaux (à l'exception du ou des administrateurs responsables), qui ont besoin d'un accès direct à la base de données pour leurs tâches administratives).</p> <p><b>Bonne Pratique</b> Les actions utilisateur typiques incluent le déplacement, la copie et la suppression de données. Tenez également compte de l'étendue des priviléges nécessaires lors de l'octroi de l'accès. Par exemple, l'accès peut être accordé à des objets spécifiques tels que des éléments de données, des fichiers, des tables, des index, des vues et des routines stockées. L'octroi de l'accès aux référentiels de données des titulaires de cartes doit suivre le même processus que tous les autres accès accordés, ce qui signifie qu'il est basé sur des rôles, avec uniquement les priviléges attribués à chaque utilisateur, nécessaires pour exécuter ses fonctions.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique aux mesures de sécurité d'accès des utilisateurs aux référentiels de requêtes de données de titulaires de cartes stockées.</p> <p>Voir les exigences 7.2.5 et 7.2.5.1 et 8.6.1 à 8.6.3 pour les mesures de sécurité des comptes d'application et système.</p>	

Exigences et Procédures de Test		Directives
<b>7.3 L'accès aux composants et aux données système est géré via un ou plusieurs systèmes de contrôle d'accès.</b>		
<b>Exigences de L'approche Définie</b>  <b>7.3.1</b> Un ou plusieurs systèmes de contrôle d'accès sont en place qui limitent l'accès en fonction du besoin d'en connaître de l'utilisateur et couvrent tous les composants système.	<b>Procédures de Test de L'approche Définie</b>  <b>7.3.1</b> Examiner la documentation du fournisseur et les paramètres système afin de vérifier que l'accès est géré pour chaque composant système via un ou plusieurs systèmes de contrôle d'accès qui limitent l'accès en fonction du besoin d'en connaître de l'utilisateur et couvrent tous les composants système.	<b>Objectif</b> Sans mécanisme pour restreindre l'accès en fonction du besoin d'en connaître de l'utilisateur, un utilisateur peut sans le savoir se voir accorder l'accès aux données des titulaires de cartes. Les systèmes de contrôle d'accès automatisent le processus de restriction d'accès et d'attribution de priviléges.
<b>Objectif de L'approche Personnalisée</b>  Les droits d'accès et les priviléges sont gérés via des mécanismes prévus à cet effet.		
<b>Exigences de L'approche Définie</b>  <b>7.3.2</b> Le ou les systèmes de contrôle d'accès sont configurés pour appliquer les autorisations attribuées aux personnes, aux applications et aux systèmes sur la base de la classification et la fonction des tâches.	<b>Procédures de Test de L'approche Définie</b>  <b>7.3.2</b> Examiner la documentation du fournisseur et les paramètres système afin de vérifier que le ou les systèmes de contrôle d'accès sont configurés pour appliquer les autorisations attribuées aux personnes, aux applications et aux systèmes sur la base de la classification et de la fonction des tâches.	<b>Objectif</b> Restreindre l'accès privilégié à l'aide d'un système de contrôle d'accès réduit le risque d'erreurs dans l'attribution des autorisations aux personnes, aux applications et aux systèmes.
<b>Objectif de L'approche Personnalisée</b>  Les droits d'accès et les priviléges individuels de compte aux systèmes, applications et données ne sont hérités que de l'appartenance à un groupe.		

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>7.3.3</b> Le ou les systèmes de contrôle d'accès sont définis par défaut pour « refuser tout le monde ».</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>7.3.3</b> Examiner la documentation du fournisseur et les paramètres système afin de vérifier que le ou les systèmes de contrôle d'accès sont configurés par défaut pour « refuser tout le monde ».</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les droits d'accès et les priviléges sont interdits, sauf autorisation expresse.</p>	<b>Objectif</b> Un paramètre par défaut « refuser tout le monde » garantit que personne n'est autorisé à l'accès à moins qu'une règle ne soit établie pour accorder spécifiquement un tel accès. <b>Bonne Pratique</b> Il est important de vérifier la configuration par défaut des systèmes de contrôle d'accès, car certains sont définis par défaut pour « autoriser tout le monde », permettant ainsi l'accès à moins ou jusqu'à ce qu'une règle soit écrite pour le refuser spécifiquement.

## Exigence 8 : Identifier les Utilisateurs et Authentifier L'accès aux Composants Système

### Sections

- 8.1 Les processus et mécanismes d'identification des utilisateurs et d'authentification des accès aux composants système sont définis et compris.
- 8.2 L'identification des utilisateurs et les comptes associés pour les utilisateurs et les administrateurs sont strictement gérés tout au long du cycle de vie d'un compte.
- 8.3 L'authentification forte des utilisateurs et des administrateurs est implémentée et gérée.
- 8.4 L'authentification multifacteur (MFA) est mise en œuvre pour sécuriser l'accès au CDE.
- 8.5 Les systèmes d'authentification multifacteur (MFA) sont configurés de sorte à ne pas pouvoir être contournés.
- 8.6 Les comptes applicatifs, les comptes systèmes et les facteurs d'authentification associés sont gérés rigoureusement.

### Aperçu

Les deux principes fondamentaux de l'identification et de l'authentification sont 1) établir l'identité d'une personne ou d'un processus sur un système informatique, et 2) prouver ou vérifier que l'utilisateur associé à l'identité est bien celui qu'il prétend être.

L'identification d'un utilisateur ou d'un processus sur un système informatique est effectué en attribuant un identifiant à une personne (identifiant d'utilisateur) ou à un processus (identifiant système, identifiant d'application) t. Ces identifiants (également appelés « comptes ») établissent fondamentalement l'identité d'une personne ou d'un processus en attribuant un identifiant unique à chaque personne ou processus afin de distinguer un utilisateur ou un processus d'un autre. Lorsque chaque utilisateur ou processus peut être identifié de manière unique, la responsabilité des actions effectuées par cette identité est garantie. Lorsqu'une telle audibilité est en place, les actions effectuées peuvent être attribuées aux utilisateurs et processus connus et autorisés.

L'élément utilisé pour prouver ou vérifier l'identité est appelé facteur d'authentification. Les facteurs d'authentification sont 1) quelque chose que vous connaissez, tel qu'un mot de passe ou une phrase secrète ; 2) quelque chose que vous possédez, tel qu'un token physique d'authentification ou une carte à point ; ou 3) quelque chose que vous êtes, tel qu'une caractéristique biométrique.

L'identifiant et le facteur d'authentification sont considérés ensemble comme des informations d'authentification et sont utilisés pour accéder aux droits et priviléges associés à un utilisateur, une application, un système ou des comptes de service.

Ces exigences en matière d'identité et d'authentification sont basées sur les principes de sécurité acceptés par l'industrie et les meilleures pratiques pour soutenir l'écosystème de paiement. *Le document NIST Special Publication 800-63, « Directives sur l'identité numérique »,* fournit des lignes directrices relatives à l'identité numérique et aux facteurs d'authentification. Il est important de noter que les *directives du NIST sur l'identité numérique* sont destinées aux agences fédérales américaines et doivent être consultées dans leur intégralité. Bon nombre des concepts et des approches définis dans ces directives sont censés fonctionner les uns avec les autres et non comme des paramètres autonomes.

(suite à la page suivante)

**Remarque :** Sauf indication contraire dans l'exigence, ces exigences s'appliquent à **tous les comptes sur tous les composants système**, y compris, sans toutefois s'y limiter :

- Comptes de points de vente
- Comptes avec des droits administrateurs
- Comptes système et applicatifs
- Tous les comptes utilisés pour afficher ou accéder aux données des titulaires de cartes ou pour accéder à des systèmes avec les données des titulaires de cartes.

Cela inclut les comptes utilisés par les employés, les sous-traitants, les consultants, les fournisseurs internes et externes et les autres tiers (par exemple, ceux qui fournissent des services d'assistance ou de maintenance).

Certaines exigences ne sont pas destinées à s'appliquer aux comptes utilisateurs sur les terminaux des points de vente n'ayant accès qu'à un seul numéro de carte à la fois afin d'effectuer la transaction. Lorsque des éléments ne s'appliquent pas, ils sont notés directement dans l'exigence spécifique.

**Ces exigences ne s'appliquent pas aux comptes utilisés par des consommateurs (titulaires de cartes).**

Se reporter à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>8.1 Les processus et mécanismes d'identification des utilisateurs et d'authentification des accès aux composants système sont définis et compris.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 8 sont :</p> <ul style="list-style-type: none"> <li>• Documentées</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attentes, les mesures de sécurité et la surveillance des activités relatives à l'exigence 8 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 8 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b> L'exigence 8.1.1 concerne la gestion et le maintien de manière efficace des diverses politiques et procédures spécifiées dans l'exigence 8. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 8, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour être alignés avec les changements dans les processus, les technologies et les objectifs métiers. Pour cette raison, envisager de mettre à jour ces documents au fil de l'eau et pas seulement sur un cycle périodique.</p> <p><b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 8 sont documentés, attribués et compris.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités liées aux activités de l'exigence 8 sont documentées et attribuées.</p> <p><b>8.1.2.b</b> Interroger le personnel chargé d'effectuer les activités de l'exigence 8 afin de vérifier que les rôles et les responsabilités sont assignés comme documentés et qu'ils sont compris.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les responsabilités quotidiennes liées à toutes les activités de l'exigence 8 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<b>Objectif</b> Si les rôles et les responsabilités ne sont pas formellement attribués, le personnel pourrait ne pas être conscient de ses responsabilités quotidiennes et des activités critiques pourraient ne pas être effectuées. <b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués. <b>Exemples</b> Une méthode possible pour documenter les rôles et les obligations est la matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).

Exigences et Procédures de Test		Directives
<b>8.2 L'identification des utilisateurs et les comptes associés pour les utilisateurs et les administrateurs sont strictement gérés tout au long du cycle de vie d'un compte.</b>		
<b>Exigences de L'approche Définie</b>	<b>Procédures de Test de L'approche Définie</b>	<b>Objectif</b>
<b>8.2.1</b> Tous les utilisateurs reçoivent un identifiant unique avant d'être autorisé à accéder aux composants système ou aux données des titulaires de cartes.	<b>8.2.1.a</b> Interroger le personnel responsable afin de vérifier que tous les utilisateurs disposent d'un identifiant unique pour accéder aux composants système et aux données des titulaires de cartes.  <b>8.2.1.b</b> Examiner les journaux d'audit et d'autres preuves pour vérifier que l'accès aux composants système et aux données des titulaires de cartes peut être identifié de manière unique et associé à des personnes.	La capacité d'attribuer les actions effectuées sur un système informatique à une personne garantit la responsabilité et la traçabilité, et est fondamentale pour implémenter des mesures de sécurité d'accès efficaces.  En s'assurant que chaque utilisateur est identifié de manière unique, plutôt que d'utiliser un identifiant partagé entre plusieurs employés, une entreprise peut conserver la responsabilité individuelle des actions et un enregistrement efficace dans le journal d'audit par employé. En outre, cela aidera à résoudre et à contenir des problèmes en cas d'utilisation abusive ou d'intention malveillante.
<b>Objectif de L'approche Personnalisée</b>		
Toutes les actions de tous les utilisateurs sont attribuables à une personne.		
<b>Notes D'applicabilité</b>		
Cette exigence n'est pas destinée à s'appliquer aux comptes utilisateur dans les terminaux de points de vente n'ayant accès qu'à un seul numéro de carte à la fois afin d'effectuer la transaction.		

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.2.2</b> Les identifiants de groupe, partagés ou génériques, ou d'autres identifiants d'authentification partagés ne sont utilisés que lorsque cela est nécessaire, à titre exceptionnel, et sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>• L'utilisation des identifiants est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles.</li> <li>• L'utilisation est limitée au temps nécessaire à la circonstance exceptionnelle.</li> <li>• La justification métier de l'utilisation est documentée.</li> <li>• L'utilisation est explicitement approuvée par la direction.</li> <li>• L'identité de l'utilisateur est confirmée avant que l'accès au compte ne soit accordé.</li> <li>• Chaque action effectuée est attribuable à un utilisateur.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Toutes les actions effectuées par les utilisateurs avec des identifiants de groupe, partagés ou génériques, sont attribuables à une personne individuelle.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.2.2.a</b> Examiner les listes de comptes d'utilisateurs sur les composants système et la documentation applicable afin de vérifier que les identifiants d'authentification partagés ne sont utilisés que lorsque cela est nécessaire, à titre exceptionnel, et sont gérés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>8.2.2.b</b> Examiner les politiques et procédures d'authentification afin de vérifier que les processus relatifs aux identifiants d'authentification partagés sont définis de sorte qu'ils ne soient utilisés que lorsque cela est nécessaire, à titre exceptionnel, et gérés conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>8.2.2.c</b> Interroger les administrateurs système afin de vérifier que les identifiants d'authentification partagés ne sont utilisés que lorsque cela est nécessaire, à titre exceptionnel, et sont gérés conformément à tous les éléments spécifiés dans cette exigence.</p>
	<p><b>Objectif</b></p> <p>Les identifiants de groupe, partagés ou génériques (ou par défaut) sont généralement fournis avec des logiciels ou des systèmes d'exploitation, par exemple, root ou avec des priviléges associés à une fonction spécifique, telle qu'un administrateur.</p> <p>Si plusieurs utilisateurs partagent les mêmes informations d'authentification (par exemple, identifiant d'utilisateur et mot de passe), il devient impossible de retracer l'accès au système et les activités d'une personne.</p> <p>Cela empêche une entité d'attribuer la responsabilité ou d'avoir une journalisation efficace des actions d'une personne, car une action effectuée aurait pu être effectuée par toute personne du groupe connaissant l'identifiant utilisateur et les facteurs d'authentification associés.</p> <p>La possibilité d'attribuer des personnes aux actions effectuées avec un identifiant est essentielle pour garantir une responsabilité individuelle et une traçabilité (qui a effectué telle action, quelle action a été effectuée et quand cette action a été effectuée).</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence n'est pas destinée à s'appliquer aux comptes utilisateur dans les terminaux de points de vente n'ayant accès qu'à un seul numéro de carte à la fois afin d'effectuer la transaction.</p>	<p><b>Bonne Pratique</b></p> <p>Si des identifiants partagés sont utilisés pour une raison quelconque, des mesures de sécurité de gestion robustes doivent être mis en place afin de maintenir la responsabilité individuelle et la traçabilité.</p> <p><b>Exemples</b></p> <p>Des outils et des techniques peuvent faciliter à la fois la gestion et la sécurité de ces types de comptes et confirmer l'identité de l'utilisateur avant que l'accès au compte ne soit accordé. Les entités peuvent envisager des coffres de mots de passe ou d'autres mesures de sécurité gérée par le système, tels que la commande sudo.</p> <p>Exemple de circonstance exceptionnelle : utilisation d'un identifiant de secours partagé lorsque toutes les autres méthodes d'authentification ont échoué pour une utilisation d'urgence ou un accès administrateur « break glass ».</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.2.3 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les prestataires de services accédant à distance à l'environnement des clients utilisent des facteurs d'authentification différents pour chaque consommateur.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les « credentials » d'un prestataire de services utilisés pour un consommateur ne peuvent pas être utilisées pour un autre consommateur.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Cette exigence n'est pas destinée à s'appliquer aux prestataires de services accédant à leurs propres environnements de services partagés, dans lesquels plusieurs environnements clients sont hébergés.</p> <p>Si les employés du prestataire de services utilisent des facteurs d'authentification partagés pour accéder à distance à l'environnement des clients, ces facteurs doivent être différents pour chaque client et gérés conformément à l'exigence 8.2.2.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.2.3 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les politiques et procédures d'authentification et interroger le personnel afin de vérifier que les prestataires de services accédant à distance à l'environnement des clients utilisent des facteurs d'authentification différent par consommateur.</p> <p><b>Objectif</b></p> <p>Les prestataires de services disposant d'un accès à distance à l'environnement des clients utilisent généralement cet accès pour prendre en charge les systèmes de POS POI ou fournir d'autres services à distance.</p> <p>Si un prestataire de services utilise les mêmes facteurs d'authentification pour accéder à plusieurs clients, tous les clients du prestataire de services peuvent facilement être compromis si un attaquant compromet ce facteur.</p> <p>Les criminels le savent et ciblent délibérément les prestataires de services à la recherche d'un facteur d'authentification partagé qui leur donne un accès à distance à de nombreux commerçants via ce seul facteur.</p> <p><b>Exemples</b></p> <p>Des technologies comme l'authentification multifacteur qui fournissent une information d'authentification différente à chaque connexion (tel qu'un mot de passe à usage unique) pourraient également répondre à l'objectif de la présente exigence.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.2.4</b> L'ajout, la suppression et la modification des identifiants utilisateur, des facteurs d'authentification et d'autres objets identifiants sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>• Autorisés avec l'approbation appropriée.</li> <li>• Mis en œuvre avec uniquement les priviléges spécifiés sur l'approbation documentée.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.2.4</b> Examiner les autorisations documentées à travers les différentes phases du cycle de vie du compte (ajouts, modifications et suppressions) et examiner les paramètres système afin de vérifier que l'activité a été gérée conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les événements de cycle de vie pour les identifiants utilisateur et les facteurs d'authentification ne peuvent pas se produire sans autorisation appropriée.</p>	<p><b>Objectif</b></p> <p>Il est impératif que le cycle de vie d'un identifiant d'utilisateur (ajouts, suppressions et modifications) soit contrôlé afin que seuls les comptes autorisés puissent exécuter des actions, que les actions soient auditables et que les priviléges soient limités à ce qui est requis.</p> <p>Les attaquants compromettent souvent un compte existant, puis élèvent les priviléges du compte pour effectuer des actes non autorisés, ou ils peuvent créer de nouveaux identifiants pour poursuivre leur activité en arrière-plan. Il est essentiel de détecter et de réagir lorsque des identifiants d'utilisateurs sont créés ou modifiés en dehors du processus de modification normal ou sans autorisation.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique à tous les comptes utilisateur, y compris les employés, les sous-traitants, les consultants, les intérimaires et les fournisseurs tiers.</p>	

Exigences et Procédures de Test		Directives
<b>Exigences de L'approche Définie</b> <p><b>8.2.5</b> L'accès des utilisateurs dont le contrat a été résilié est immédiatement révoqué.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.2.5.a</b> Examiner les sources d'informations pour les utilisateurs dont le contrat a été résilié et examiner les listes d'accès des utilisateurs actuels (pour l'accès local et distant) afin de vérifier que les identifiants des utilisateurs dont le contrat a été résilié ont été désactivés ou supprimés des listes d'accès.</p> <p><b>8.2.5.b</b> Interroger le personnel responsable pour vérifier que tous les facteurs d'authentification physiques, tels que les cartes à puce, les jetons, etc., ont été renvoyés ou désactivés pour les utilisateurs dont le contrat a été résilié.</p>	<b>Objectif</b> Si un employé ou un tiers/fournisseur a quitté l'entreprise et a toujours accès au réseau via son compte utilisateur, un acte malveillant relatif aux données des titulaires de cartes pourrait se produire, soit par l'ancien employé, soit par un utilisateur malveillant.
<b>Objectif de L'approche Personnalisée</b> <p>Les comptes des utilisateurs dont le contrat a été résilié ne peuvent pas être utilisés.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.2.6</b> Examiner les comptes utilisateur et les informations de dernière connexion, et interroger le personnel afin de vérifier que tous les comptes utilisateur inactifs depuis 90 jours sont supprimés ou désactivés.</p>	<b>Objectif</b> Les comptes qui ne sont pas utilisés régulièrement sont souvent la cible d'attaques, car il est moins probable que des modifications, telles qu'un changement de mot de passe, soient remarquées. Ainsi, ces comptes peuvent être plus facilement exploités et utilisés pour accéder aux données des titulaires de cartes. <b>Bonne Pratique</b> Lorsqu'il peut être raisonnablement prévu qu'un compte ne sera pas utilisé pendant une période prolongée, comme un congé prolongé, le compte doit être désactivé dès le début du congé, plutôt que d'attendre les 90 jours.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.2.7</b> Les comptes utilisés par les tiers pour accéder, prendre en charge ou maintenir les composants système via un accès à distance sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>Activés uniquement pendant la période d'intervention et désactivés en dehors de la période.</li> <li>L'utilisation est surveillée pour détecter toute activité inhabituelle.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.2.7</b> Interroger le personnel, examiner la documentation relative à la gestion des comptes, et examiner les preuves afin de vérifier que les comptes d'accès à distance utilisés par les tiers sont gérés conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les accès à distance utilisés par les tiers ne peuvent pas être utilisés, sauf lorsque cela est spécifiquement autorisé et que l'utilisation est supervisée par la direction.</p>	<b>Objectif</b> Permettre à des tiers d'avoir un accès 24 heures sur 24 et 7 jours sur 7 aux systèmes et aux réseaux d'une entité en cas d'assistance augmente les chances d'accès non autorisé. Cet accès pourrait se traduire par un utilisateur non autorisé dans l'environnement du tiers ou une personne malveillante utilisant le point d'entrée externe toujours disponible dans le réseau d'une entité. Lorsque des tiers ont besoin d'un accès 24 heures sur 24, 7 jours sur 7, cela doit être documenté, justifié, surveillé et lié à des besoins spécifiques. <b>Bonne Pratique</b> Activer l'accès uniquement pendant les périodes d'intervention et le désactiver dès que cela n'est plus nécessaire permet d'éviter une mauvaise utilisation de ces connexions. En outre, il est conseillé d'attribuer à des tiers une date de début et de fin d'accès conformément à leur contrat de service. La surveillance de l'accès des tiers permet de s'assurer qu'ils n'accèdent qu'aux systèmes nécessaires et uniquement pendant les périodes approuvées. Toute activité inhabituelle utilisant des comptes tiers devrait être suivie jusqu'à sa résolution.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.2.8</b> Si une session utilisateur est inactive pendant plus de 15 minutes, l'utilisateur doit s'authentifier à nouveau pour réactiver le terminal ou la session.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.2.8</b> Examiner les paramètres de configuration du système afin de vérifier que les délais d'inactivité du système ou de la session pour les sessions utilisateur ont été définis sur 15 minutes maximum.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Une session utilisateur ne peut être utilisée que par l'utilisateur autorisé.</p>	<b>Objectif</b> Lorsque les utilisateurs ne verrouillent pas leur session et qu'ils s'éloignent de leur machine donnant un accès aux composants système ou aux données des titulaires de cartes, il existe un risque que la machine soit utilisée par d'autres en l'absence de l'utilisateur, entraînant un accès non autorisé au compte et/ou une mauvaise utilisation.
<b>Notes D'applicabilité</b> <p>Cette exigence n'est pas destinée à s'appliquer aux comptes utilisateur dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de permettre la transaction.</p> <p>Cette exigence n'est pas destinée à empêcher l'exécution d'activités légitimes lorsque la console ou l'ordinateur est sans surveillance.</p>	<b>Bonne Pratique</b> La réauthentification peut être appliquée soit au niveau du système pour protéger toutes les sessions ouvertes sur cette machine, soit au niveau de l'application. Les entités peuvent également envisager de mettre en place des mesures de sécurité en cascade afin de restreindre davantage l'accès à une session sans surveillance au fur et à mesure que le temps passe. Par exemple, l'économiseur d'écran peut s'activer au bout de 15 minutes et déconnecter l'utilisateur au bout d'une heure. Cependant, les mesures de sécurité de timeout doivent tenir compte du risque d'accès et d'exposition, ainsi que l'impact sur l'utilisateur et le but de l'accès. Si un utilisateur doit exécuter un programme à partir d'un ordinateur sans surveillance, il peut se connecter à l'ordinateur pour exécuter le programme, puis verrouillera session afin que personne d'autre ne puisse utiliser la session de l'utilisateur.

Exigences et Procédures de Test	Directives
<b>8.3 L'authentification forte des utilisateurs et des administrateurs est implémentée et gérée.</b>	
<b>Exigences de L'approche Définie</b> <p><b>8.3.1</b> Tous les accès utilisateur et administrateurs aux composants système sont authentifiés via au moins l'un des facteurs d'authentification suivants :</p> <ul style="list-style-type: none"> <li>• Quelque chose que vous connaissez, comme un mot de passe ou une phrase secrète.</li> <li>• Quelque chose que vous possédez, comme un jeton d'authentification ou une carte à puce.</li> <li>• Quelque chose que vous êtes, comme un élément biométrique.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.1.a</b> Examiner la documentation décrivant le ou les facteurs d'authentification utilisés afin de vérifier que l'accès des utilisateurs aux composants système est authentifié via au moins un facteur d'authentification spécifié dans cette exigence.</p> <p><b>8.3.1.b</b> Pour chaque type de facteur d'authentification utilisé avec chaque type de composant système, observer une authentification afin de vérifier que l'authentification fonctionne conformément avec le ou les facteurs d'authentification documentés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Un compte ne peut pas être accessible sauf avec une combinaison d'identité d'utilisateur et d'un facteur d'authentification.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence n'est pas destinée à s'appliquer aux comptes utilisateur dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de permettre la transaction.</p> <p>Cette exigence ne remplace pas les exigences d'authentification multifacteur (MFA), mais s'applique aux systèmes du périmètre qui ne sont pas soumis aux exigences du MFA.</p> <p>Un certificat numérique est une option valide pour « quelque chose que vous possédez » s'il est unique pour un utilisateur particulier.</p>	<b>Objectif</b> <p>Lorsqu'un facteur d'authentification est utilisé en complément d'identifiants uniques, un facteur d'authentification contribue à protéger les identifiants des utilisateurs contre la compromission, car l'attaquant doit connaître l'identifiant unique et compromettre le ou les facteurs d'authentification associés.</p> <p><b>Bonne Pratique</b></p> <p>Une approche commune pour une personne malveillante de compromettre un système consiste à exploiter des facteurs d'authentification faibles ou inexistantes (par exemple, des mots de passe/phrases secrètes). Exiger des facteurs d'authentification forts permet de se protéger contre cette attaque.</p> <p><b>Informations Complémentaires</b></p> <p>Consulter <a href="http://fidoalliance.org">fidoalliance.org</a> pour plus d'informations sur l'utilisation de jetons, de cartes à point ou de données biométriques comme facteurs d'authentification.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.3.2</b> Une cryptographie robuste est utilisée pour rendre tous les facteurs d'authentification illisibles pendant la transmission et le stockage sur tous les composants système.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.2.a</b> Examiner la documentation du fournisseur et les paramètres de configuration du système afin de vérifier que les facteurs d'authentification sont rendus illisibles grâce à une cryptographie robuste pendant la transmission et le stockage.</p> <p><b>8.3.2.b</b> Examiner les référentiels de facteurs d'authentification afin de vérifier qu'ils sont illisibles pendant le stockage.</p> <p><b>8.3.2.c</b> Examiner les données transmises afin de vérifier que les facteurs d'authentification sont illisibles pendant la transmission.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les facteurs d'authentification en clair ne peuvent pas être obtenus, dérivés ou réutilisés à partir de l'interception de communications ou de données stockées.</p>	<b>Objectif</b> Il est connu que les périphériques réseau et les applications transmettent des facteurs d'authentification non chiffrés et lisibles (tels que des mots de passe et des phrases secrètes) sur le réseau et/ou stockent ces valeurs sans chiffrement. En conséquence, une personne malveillante peut facilement intercepter ces informations lors de la transmission à l'aide d'un « renifleur » ou accéder directement aux facteurs d'authentification non chiffrés dans les fichiers où elles sont stockées, puis utiliser ces données pour obtenir un accès non autorisé.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.3.3</b> L'identité de l'utilisateur est vérifiée avant de modifier tout facteur d'authentification.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.3</b> Examiner les procédures de modification des facteurs d'authentification et observer le personnel de sécurité afin de vérifier que l'identité de l'utilisateur est bien vérifiée lorsqu'il demande la modification d'un facteur d'authentification.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les personnes non autorisées ne peuvent pas accéder au système en usurpant l'identité d'un utilisateur autorisé.</p>	<b>Objectif</b> Les personnes malveillantes utilisent des techniques d'« ingénierie sociale » pour usurper l'identité de l'utilisateur d'un système ; par exemple en appelant un service d'assistance et en agissant en tant qu'utilisateur légitime, afin de modifier un facteur d'authentification afin qu'elles puissent utiliser un identifiant d'utilisateur valide. Exiger un contrôle positif de l'identité d'un utilisateur réduit la probabilité de survenue de ce type d'attaque. <b>Bonne Pratique</b> Les modifications apportées aux facteurs d'authentification pour lesquels l'identité de l'utilisateur doit être vérifiée incluent, sans toutefois s'y limiter, la réinitialisation de mot de passe, l'approvisionnement de nouveaux jetons matériels ou logiciels et la génération de nouvelles clés. <b>Exemples</b> Les méthodes pour vérifier l'identité d'un utilisateur comprennent une question/réponse secrète, des informations basées sur les connaissances et le rappel de l'utilisateur à un numéro de téléphone connu et préalablement défini.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.3.4</b> Les tentatives d'authentification infructueuses sont limitées par :</p> <ul style="list-style-type: none"> <li>• Le verrouillage de l'identifiant utilisateur après 10 tentatives échouées maximum.</li> <li>• Le réglage de la durée de verrouillage à 30 minutes minimum ou jusqu'à la confirmation de l'identité de l'utilisateur.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.4.a</b> Examiner les paramètres de configuration du système afin de vérifier que les paramètres d'authentification sont définis pour exiger le verrouillage des comptes utilisateur après 10 tentatives de connexion échouées maximum.</p> <p><b>8.3.4.b</b> Examiner les paramètres de configuration du système afin de vérifier que les paramètres de mot de passe sont définis pour exiger qu'une fois le compte utilisateur verrouillé, il le reste pendant au moins 30 minutes ou jusqu'à ce que l'identité de l'utilisateur soit confirmée.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Un facteur d'authentification ne peut pas être deviné par force brute dans une attaque en ligne.</p>	<b>Objectif</b> Sans mécanismes de verrouillage de compte en place, un attaquant peut continuellement essayer de deviner un mot de passe à l'aide d'outils manuels ou automatisés (par exemple, le craquage de mot de passe) jusqu'à ce que l'attaquant réussisse et accède au compte d'un utilisateur. Si un compte est verrouillé parce que quelqu'un essaie continuellement de deviner un mot de passe, les mesures de sécurité visant à retarder la réactivation du compte verrouillé empêchent la personne malveillante de deviner le mot de passe, car elle devra attendre au moins 30 minutes que le compte soit réactivé.
<b>Notes D'applicabilité</b> <p>Cette exigence n'est pas destinée à s'appliquer aux comptes utilisateur dans les terminaux de points de vente n'ayant accès qu'à un seul numéro de carte à la fois afin de permettre la transaction.</p>	<b>Bonne Pratique</b> Avant de réactiver un compte verrouillé, l'identité de l'utilisateur doit être confirmée. Par exemple, l'administrateur ou le service d'assistance peut s'assurer que la réactivation du compte est bien effectuée par le propriétaire réel du compte, ou il peut exister des mécanismes de réinitialisation de mot de passe en libre-service que le propriétaire du compte utilise pour vérifier son identité.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.5</b> Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils sont définis et réinitialisés pour chaque utilisateur comme suit :</p> <ul style="list-style-type: none"> <li>• Définis sur une valeur unique pour chaque première utilisation et lors de la réinitialisation.</li> <li>• Doivent être modifiés immédiatement après la première utilisation.</li> </ul>	<p><b>Procédures de test de l'approche définie</b></p> <p><b>8.3.5</b> Examiner les procédures de définition et de réinitialisation des mots de passe/phrases secrètes (s'ils sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1) et observer le personnel de sécurité afin de vérifier que les mots de passe/phrases secrètes sont définis et réinitialisés conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un mot de passe/phrase secrète initial ou réinitialisé attribué à un utilisateur ne peut pas être utilisé par un utilisateur non autorisé.</p>	<p><b>Objectif</b></p> <p>Si le même mot de passe/phrase secrète est utilisé pour chaque nouvel utilisateur, un utilisateur interne, un ancien employé ou une personne malveillante pourrait le connaître ou le découvrir facilement et l'utiliser pour accéder aux comptes avant que l'utilisateur autorisé ne puisse l'utiliser.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.6</b> Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils doivent répondre au niveau de complexité minimum suivant :</p> <ul style="list-style-type: none"> <li>• Une longueur minimale de 12 caractères (ou 8 caractères si le système ne prend pas en charge les 12 caractères).</li> <li>• Contenir à la fois des caractères numériques et alphabétiques.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.3.6</b> Examiner les paramètres de configuration du système afin de vérifier que les paramètres de complexité du mot de passe/de la phrase secrète de l'utilisateur sont définis conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un mot de passe/phrase secrète deviné ne peut pas être vérifié par une attaque par force brute en ligne ou hors ligne.</p>	<p><b>Objectif</b> Des mots de passe/phrases secrètes robustes peuvent être la première ligne de défense d'un réseau, car une personne malveillante essaiera souvent en premier lieu de trouver des comptes avec des mots de passe faibles, statiques ou inexistantes. Si les mots de passe sont courts ou facilement devinables, il est relativement facile pour une personne malveillante de trouver ces comptes faibles et de compromettre un réseau sous l'identité de l'utilisateur valide</p> <p><b>Bonne Pratique</b> La robustesse du mot de passe/de la phrase secrète dépend de la complexité, de la longueur et du caractère aléatoire du mot de passe/de la phrase secrète. Les mots de passe/phrases secrètes doivent être suffisamment complexes, de sorte qu'ils soient compliqués pour un attaquant de le deviner ou de le découvrir. Les entités peuvent envisager d'augmenter la complexité en exigeant l'utilisation de caractères spéciaux et de caractères majuscules et minuscules, en plus des éléments spécifiés dans cette exigence. Une complexité supplémentaire augmente le temps requis pour les attaques par force brute hors ligne des mots de passe/phrases secrètes hachés.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence n'est pas destinée à s'appliquer :</p> <ul style="list-style-type: none"> <li>• Aux comptes d'utilisateurs dans les terminaux de points de vente n'ayant accès qu'à un seul numéro de carte à la fois afin de permettre la transaction.</li> <li>• Aux comptes d'applications ou système, qui sont régis par les exigences de la section 8.6.</li> </ul> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p> <p>Jusqu'au 31 mars 2025, les mots de passe doivent avoir une longueur minimale de 7 caractères conformément à l'exigence 8.2.3 du standard PCI DSSv3.2.1.</p>	<p>Une autre option pour augmenter la résistance des mots de passe aux attaques par déduction consiste à comparer les mots de passe/phrases secrètes à une liste de mots de passe interdits et à demander aux utilisateurs de fournir de nouveaux mots de passe pour chaque mot de passe trouvé sur la liste.</p>

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>8.3.7</b> Les utilisateurs ne sont pas autorisés à soumettre un nouveau mot de passe/phrase secrète correspondant à l'un des quatre derniers mots de passe/phrases secrètes utilisés.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.7</b> Examiner les paramètres de configuration du système afin de vérifier que les paramètres de mot de passe sont définis pour exiger que les nouveaux mots de passe/phrases secrètes ne soient pas les mêmes que les quatre mots de passe/phrases secrètes précédemment utilisés.</p>	<b>Objectif</b> Si un historique des mots de passe n'est pas conservé, l'efficacité de la modification des mots de passe est réduite, car les mots de passe précédents peuvent être réutilisés éternellement. Exiger que les mots de passe ne puissent pas être réutilisés pendant une certaine période réduit la probabilité que les mots de passe qui ont été devinés ou cassés par force brute seront réutilisés à l'avenir.
<b>Objectif de L'approche Personnalisée</b> Un mot de passe précédemment utilisé ne peut pas être utilisé pour accéder à un compte pendant au moins 12 mois.		Les mots de passe ou les phrases secrètes peuvent avoir déjà été modifiés en raison d'un soupçon de compromission ou parce que le mot de passe ou la phrase secrète ont dépassé leur période d'utilisation effective, deux raisons pour lesquelles les mots de passe précédemment utilisés ne doivent pas être réutilisés.
<b>Notes D'applicabilité</b> Cette exigence n'est pas applicable pour les comptes configurés sur les terminaux de paiement ayant accès à un seul numéro de carte bancaire à la fois.		
<b>Exigences de L'approche Définie</b> <p><b>8.3.8</b> Les politiques et procédures d'authentification sont documentées et communiquées à tous les utilisateurs, notamment :</p> <ul style="list-style-type: none"> <li>Des conseils sur le choix de facteurs d'authentification robustes.</li> <li>Des conseils sur la façon dont les utilisateurs doivent protéger leurs facteurs d'authentification.</li> <li>Des instructions pour ne pas réutiliser les mots de passe/phrases secrètes précédemment utilisés.</li> <li>Des instructions pour modifier les mots de passe/phrases secrètes en cas de soupçon ou en sachant que les mots de passe/phrases secrètes ont été compromis et comment signaler l'incident.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.3.8.a</b> Examiner les procédures et interroger le personnel afin de vérifier que les politiques et procédures d'authentification sont distribuées à tous les utilisateurs.</p> <p><b>8.3.8.b</b> Examiner les politiques et procédures d'authentification qui sont distribuées aux utilisateurs et vérifier qu'elles incluent les éléments spécifiés dans cette exigence.</p> <p><b>8.3.8.c</b> Interroger les utilisateurs afin de vérifier qu'ils connaissent bien les politiques et procédures d'authentification.</p>	<b>Objectif</b> La communication des politiques et procédures d'authentification à tous les utilisateurs les aide à comprendre et à respecter les politiques. <b>Bonne Pratique</b> Des conseils sur le choix 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 ou d'informations sur l'utilisateur, telles que l'identité de l'utilisateur, les noms des membres de sa famille, sa date de naissance, etc. Des conseils pour protéger les facteurs d'authentification peuvent inclure de ne pas écrire les mots de passe ou les enregistrer dans des fichiers non sécurisés, et d'être attentif aux personnes malveillantes qui peuvent essayer d'exploiter leurs mots de passe (par exemple, en appelant un employé et en lui demandant son mot

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les utilisateurs connaissent l'utilisation correcte des facteurs d'authentification et peuvent accéder à une assistance et à des conseils en cas de besoin.</p>	<p>de passe en prétextant la résolution d'un problème).</p> <p>Alternativement, les entités peuvent mettre en œuvre des processus pour confirmer que les mots de passe respectent la politique relative aux mots de passe ; par exemple, en comparant les choix de mot de passe à une liste de mots de passe inacceptables et en demandant aux utilisateurs de choisir un nouveau mot de passe s'il fait partie de la liste. Demander aux utilisateurs de modifier leur mot de passe s'il y a une chance qu'il ne soit plus sûr, peut empêcher les utilisateurs malveillants d'utiliser un mot de passe légitime pour obtenir un accès non autorisé.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.9</b> Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès utilisateur (c'est-à-dire dans le cas d'authentification à un seul facteur), alors soit :</p> <ul style="list-style-type: none"> <li>• Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours, <b>OU</b></li> <li>• La posture de sécurité des comptes est analysée de manière dynamique et l'accès aux ressources est réalisé en temps-réel et est déterminé automatiquement en conséquence.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.3.9</b> Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès utilisateur, inspecter les paramètres de configuration du système afin de vérifier que les mots de passe/phrases secrètes sont gérés conformément à UN des éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b> L'accès aux composants système dans le périmètre qui ne sont pas dans le CDE peut être fourni à l'aide d'un seul facteur d'authentification, tel qu'un mot de passe/une phrase secrète, un jeton ou une carte à puce, ou un attribut biométrique. Lorsque des mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour un tel accès, des mesures de sécurité supplémentaires sont nécessaires afin de protéger l'intégrité du mot de passe/de la phrase secrète.</p> <p><b>Bonne Pratique</b> Les mots de passe/phrases secrètes valides pendant une longue période sans modification donnent aux personnes malveillantes plus de temps pour casser le mot de passe/la phrase secrète. La modification périodique des mots de passe offre moins de temps à une personne malveillante pour déchiffrer un mot de passe/une phrase secrète et moins de temps pour utiliser un mot de passe compromis.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un mot de passe/phrase secrète compromis non détecté ne peut pas être utilisé indéfiniment.</p>	<p>L'utilisation d'un mot de passe/phrase secrète comme seul facteur d'authentification fournit un point de défaillance unique en cas de compromission. Par conséquent, dans ces mises en œuvre, des mesures de sécurité sont nécessaires pour minimiser la durée pendant laquelle une activité malveillante pourrait se produire via un mot de passe/une phrase secrète compromis.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique pas aux composants du système dans le champ de l'évaluation où l'MFA est utilisée.</p> <p>Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction.</p> <p>Cette exigence ne s'applique pas aux comptes clients des prestataires de services mais s'applique aux comptes du personnel des prestataires de services.</p>	<p>L'analyse dynamique de l'état de sécurité d'un compte est une autre option qui permet une détection et une réponse plus rapides pour traiter les informations d'identification potentiellement compromises.</p> <p>Une telle analyse prend un certain nombre de points de données, qui peuvent inclure l'intégrité de l'appareil, l'emplacement, les heures d'accès et les ressources consultées pour déterminer en temps réel si un compte peut se voir accorder l'accès à une ressource demandée.</p> <p>De cette façon, l'accès peut être refusé et les comptes bloqués si l'on soupçonne que les informations d'authentification ont été compromises.</p> <p><b>Informations Complémentaires</b></p> <p>Pour plus d'informations sur l'utilisation de l'analyse dynamique pour gérer l'accès des utilisateurs aux ressources, voir NIST SP 800-207 Zero Trust Architecture.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.10 Exigences supplémentaires pour les prestataires de services uniquement :</b> Si des mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès des utilisateurs consommateur aux données des titulaires de cartes (c'est-à-dire dans toute mise en œuvre d'authentification à facteur unique), des conseils sont fournis aux utilisateurs clients, notamment :</p> <ul style="list-style-type: none"> <li>Des conseils aux clients pour modifier périodiquement leurs mots de passe/phrases secrète d'utilisateur.</li> <li>Des conseils sur quand et dans quelles circonstances les mots de passe/phrases secrètes sont modifiés.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.3.10 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Si des mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès des utilisateurs consommateur aux données des titulaires de cartes, examiner les instructions fournies aux utilisateurs consommateur afin de vérifier qu'elles incluent tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les mots de passe/phrases secrètes pour les clients des prestataires de services ne peuvent pas être utilisés indéfiniment.</p>	
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité audité est un prestataire de services.</p> <p>Cette exigence ne s'applique pas aux comptes des utilisateurs consommateur accédant à leurs propres informations de carte de paiement.</p> <p>Cette exigence pour les prestataires de services sera remplacée par l'exigence 8.3.10.1 une fois que 8.3.10.1 entrera en vigueur.</p>	<p><b>Objectif</b></p> <p>L'utilisation d'un mot de passe/phrase secrète comme seul facteur d'authentification fournit un point de défaillance unique en cas de compromission. Par conséquent, dans ces mises en œuvre, des mesures de sécurité sont nécessaires pour minimiser la durée pendant laquelle une activité malveillante pourrait se produire via un mot de passe/une phrase secrète compromis.</p> <p><b>Bonne Pratique</b></p> <p>Les mots de passe/phrases secrètes valides pendant une longue période sans modification donnent aux personnes malveillantes plus de temps pour casser le mot de passe/la phrase secrète. La modification périodique des mots de passe offre moins de temps à une personne malveillante pour déchiffrer un mot de passe/une phrase secrète et moins de temps pour utiliser un mot de passe compromis.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.10.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès aux utilisateurs consommateur (c'est-à-dire dans toute mise en œuvre d'authentification à un seul facteur), alors soit :</p> <ul style="list-style-type: none"> <li>• Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours, <b>OU</b></li> <li>• La posture de sécurité des comptes est analysée de manière dynamique et l'accès en temps réel aux ressources est automatiquement déterminé en conséquence.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les mots de passe/phrases secrètes pour les clients des prestataires de services ne peuvent pas être utilisés indéfiniment.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité audité est un prestataire de services.</p> <p>Cette exigence ne s'applique pas aux comptes des utilisateurs consommateur accédant à leurs propres informations de carte de paiement.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p> <p>Jusqu'à ce que cette exigence entre en vigueur le 31 mars 2025, les prestataires de services peuvent satisfaire à l'exigence 8.3.10 ou 8.3.10.1.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.3.10.1 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès aux utilisateurs consommateur, inspecter les paramètres de configuration du système afin de vérifier que les mots de passe/phrases secrètes sont gérés conformément à UN des éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>L'utilisation d'un mot de passe/phrase secrète comme seul facteur d'authentification fournit un point de défaillance unique en cas de compromission. Par conséquent, dans ces mises en œuvre, des mesures de sécurité sont nécessaires pour minimiser la durée pendant laquelle une activité malveillante pourrait se produire via un mot de passe/une phrase secrète compromis.</p> <p><b>Bonne Pratique</b></p> <p>Les mots de passe/phrases secrètes valides pendant une longue période sans modification donnent aux personnes malveillantes plus de temps pour casser le mot de passe/la phrase secrète. La modification périodique des mots de passe offre moins de temps à une personne malveillante pour déchiffrer un mot de passe/une phrase secrète et moins de temps pour utiliser un mot de passe compromis.</p> <p>L'analyse dynamique de la posture de sécurité d'un compte est une autre option qui permet une détection et une réponse plus rapides pour traiter les crédentiels potentiellement compromis. Une telle analyse prend un certain nombre de points de données, qui peuvent inclure l'intégrité de l'appareil, l'emplacement, les heures d'accès et les ressources consultées afin de déterminer en temps réel si un compte peut se voir accorder l'accès à une ressource demandée. De cette façon, l'accès peut être refusé et les comptes bloqués si l'on soupçonne que les crédentiels du compte ont été compromis.</p> <p><b>Informations Complémentaires</b></p> <p>Pour plus d'informations sur l'utilisation de l'analyse dynamique pour gérer l'accès des utilisateurs aux ressources, se reporter à <i>NIST SP 800-207 Zero Trust Architecture</i>.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.3.11</b> Lorsque des facteurs d'authentification tels que des tokens physiques ou logiques, des cartes à point ou des certificats sont utilisés :</p> <ul style="list-style-type: none"> <li>• Les facteurs sont attribués à un utilisateur individuel et ne sont pas partagés entre plusieurs utilisateurs.</li> <li>• Les mesures physiques et/ou logiques garantissent que seul l'utilisateur prévu peut utiliser ce facteur pour obtenir l'accès.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.3.11.a</b> Examiner les politiques et procédures d'authentification afin de vérifier que les procédures d'utilisation des facteurs d'authentification tels que les tokens physiques, les cartes à point et les certificats sont définies et comportent tous les éléments spécifiés dans cette exigence.</p> <p><b>8.3.11.b</b> Interroger le personnel de sécurité afin de vérifier que les facteurs d'authentification sont attribués à un utilisateur individuel et ne sont pas partagés entre plusieurs utilisateurs.</p> <p><b>8.3.11.c</b> Examiner les paramètres de configuration du système et/ou observer les mesures de sécurité physiques, le cas échéant, afin de vérifier que les mesures de sécurité sont mises en œuvre pour garantir que seul l'utilisateur prévu peut utiliser ce facteur pour obtenir l'accès.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un facteur d'authentification ne peut être utilisé par personne d'autre que l'utilisateur auquel il est attribué.</p>	<p><b>Objectif</b> Si plusieurs utilisateurs peuvent utiliser des facteurs d'authentification tels que des tokens physiques ou logiques, des cartes à point et des certificats, il peut être impossible d'identifier la personne à l'aide du mécanisme d'authentification.</p> <p><b>Bonne Pratique</b> Le fait d'avoir des mesures de sécurité physiques et/ou logiques (par exemple, un code PIN, des données biométriques ou un mot de passe) pour authentifier de manière unique l'utilisateur du compte empêchera les utilisateurs non autorisés d'accéder au compte utilisateur via l'utilisation d'un facteur d'authentification partagé.</p>

Exigences et Procédures de Test	Directives
<b>8.4 L'authentification multifacteur (MFA) est mise en œuvre pour sécuriser l'accès au CDE.</b>	
<b>Exigences de L'approche Définie</b> <p><b>8.4.1</b> Le MFA est mis en œuvre pour tous les accès non-console dans le CDE pour le personnel avec des accès d'administration.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.4.1.a</b> Examiner les configurations réseau et/ou système afin de vérifier que l'authentification MFA est obligatoire pour toutes les opérations non-console dans le CDE pour le personnel disposant d'un accès d'administration.</p> <p><b>8.4.1.b</b> Observer les administrateurs se connecter au CDE et vérifier que l'authentification MFA est exigée.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les accès d'administration au CDE ne peuvent pas être obtenus p en utilisant un seul facteur d'authentification.</p>	<b>Objectif</b> Exiger plus d'un type de facteur d'authentification réduit la probabilité qu'un attaquant puisse accéder à un système en se faisant passer pour un utilisateur légitime, car l'attaquant devra pouvoir compromettre plusieurs facteurs d'authentification. Cela est particulièrement vrai dans les environnements où traditionnellement, le seul facteur d'authentification utilisé était quelque chose qu'un utilisateur connaît, tel qu'un mot de passe ou une phrase secrète. <b>Bonne Pratique</b> La mise en œuvre de la MFA pour l'accès administratif hors console aux composants système dans le périmètre qui ne font pas partie du CDE aidera à empêcher les utilisateurs non autorisés d'utiliser un seul facteur pour accéder et compromettre les composants système dans le périmètre. <b>Définitions</b> L'utilisation d'un facteur d'authentification deux fois (par exemple, l'utilisation de deux mots de passe distincts) n'est pas considérée comme une authentification multifacteur.
<b>Notes D'applicabilité</b> <p>L'exigence du MFA pour l'accès d'administration non-console s'applique à tout le personnel avec des priviléges élevés ou accrues accédant au CDE via une connexion non-console, c'est-à-dire via un accès logique survenant sur une interface réseau plutôt que via une connexion physique directe.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.4.2</b> L'authentification MFA est mise en œuvre pour tous les accès hors console au CDE.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.4.2.a</b> Examiner les configurations réseau et/ou système afin de vérifier que l'authentification MFA est mise en œuvre pour tous les accès hors console au CDE.</p> <p><b>8.4.2.b</b> Observer les administrateurs se connecter au CDE et vérifier que l'authentification MFA est exigée.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'accès au CDE ne peut pas être obtenu par l'utilisation d'un seul facteur d'authentification.</p>	<p><b>Objectif</b> Exiger plus d'un type de facteur d'authentification réduit la probabilité qu'un attaquant puisse accéder à un système en se faisant passer pour un utilisateur légitime, car l'attaquant devra pouvoir compromettre plusieurs facteurs d'authentification. Cela est particulièrement vrai dans les environnements où traditionnellement, le seul facteur d'authentification utilisé était quelque chose qu'un utilisateur connaît, tel qu'un mot de passe ou une phrase secrète.</p> <p><b>Définitions</b> L'utilisation d'un facteur d'authentification deux fois (par exemple, l'utilisation de deux mots de passe distincts) n'est pas considérée comme une authentification multifacteur.</p> <p>Se reporter à l'Annexe G pour la définition de « l'authentification résistant à l'hameçonnage »</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique pas :</p> <ul style="list-style-type: none"> <li>• Aux comptes applicatifs ou système exécutant des fonctions automatisées.</li> <li>• Aux comptes utilisateur dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin d'effectuer une seule transaction</li> <li>• Aux comptes utilisateur qui uniquement authentifiés via des facteurs d'authentification résistant à l'hameçonnage</li> </ul> <p>L'authentification MFA est requise pour les deux types d'accès spécifiés dans les exigences 8.4.2 et 8.4.3. Par conséquent, l'application du MFA à un type d'accès ne remplace pas la nécessité d'appliquer une autre instance du MFA à l'autre type d'accès.</p> <p>(suite à la page suivante)</p>	

Exigences et Procédures de Test	Directives
<p>Si une personne se connecte d'abord au réseau de l'entité via un accès à distance, puis initie ultérieurement une connexion au CDE à partir du réseau, conformément à cette exigence, ladite personne s'authentifiera à l'aide du MFA à deux reprises, une fois lors de la connexion via un accès à distance au réseau de l'entité et une fois lors de la connexion du réseau de l'entité au CDE.</p> <p>Les exigences de l'authentification MFA s'appliquent à tous les types de composants système, y compris le cloud, les systèmes hébergés et les applications sur site, les dispositifs de sécurité réseau, les postes de travail, les serveurs et les points de terminaison, et comportent l'accès direct aux réseaux ou systèmes d'une entité ainsi qu'un accès Web à une application ou à une fonction.</p> <p>L'authentification MFA pour l'accès au CDE peut être mise en œuvre au niveau du réseau ou du système/application ; elle n'a pas à être appliquée aux deux niveaux. Par exemple, si l'authentification MFA est utilisée lorsqu'un utilisateur se connecte au réseau CDE, il n'est pas nécessaire de l'utiliser lorsque l'utilisateur se connecte à chaque système ou application au sein du CDE.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>8.4.3</b> L'authentification MFA est mise en œuvre pour tous les accès distants provenant de l'extérieur du réseau de l'entité qui pourraient accéder ou avoir une incidence sur le CDE.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.4.3.a</b> Examiner les configurations réseau et/ou système pour les serveurs et systèmes d'accès à distance afin de vérifier que l'authentification MFA est requise conforme à tous les éléments spécifiés dans cette exigence.</p> <p><b>8.4.3.b</b> Observer le personnel (par exemple, les utilisateurs et les administrateurs) et les tiers se connectant à distance au réseau et vérifier que l'authentification à plusieurs facteurs est requise.</p>
<b>Objectif de L'approche Personnalisée</b> <p>L'accès à distance au réseau de l'entité ne peut pas être obtenu en utilisant un seul facteur d'authentification.</p> <p>(suite à la page suivante)</p>	<b>Objectif</b> Exiger plus d'un type de facteur d'authentification réduit la probabilité qu'un attaquant puisse accéder à un système en se faisant passer pour un utilisateur légitime, car l'attaquant devra pouvoir compromettre plusieurs facteurs d'authentification. Cela est particulièrement vrai dans les environnements où traditionnellement, le seul facteur d'authentification utilisé était quelque chose qu'un utilisateur connaît, tel qu'un mot de passe ou une phrase secrète. <b>Définitions</b> L'authentification multifacteur (MFA) exige qu'un individu présente au moins deux des trois facteurs d'authentification spécifiés dans l'exigence 8.3.1 avant que l'accès ne soit accordé. L'utilisation d'un facteur d'authentification deux fois (par exemple, l'utilisation de deux mots de passe distincts) n'est pas considérée comme une authentification multifacteur.

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>L'exigence de l'authentification MFA pour l'accès à distance provenant de l'extérieur du réseau de l'entité s'applique à tous les comptes utilisateur pouvant accéder au réseau à distance, lorsque cet accès à distance conduit ou pourrait conduire à l'accès au CDE.</p> <p>Cela inclut tous les accès à distance par le personnel (utilisateurs et administrateurs) et par des tiers (y compris, sans toutefois s'y limiter, les vendeurs, les fournisseurs, les prestataires de services et les clients).</p> <p>Si l'accès à distance concerne une partie du réseau de l'entité qui est correctement segmentée du CDE, de sorte que les utilisateurs distants ne peuvent pas accéder ou avoir un impact sur le CDE, l'authentification MFA pour l'accès à distance à cette partie du réseau n'est pas requise.</p> <p>Cependant, l'authentification MFA est requise pour tout accès distant aux réseaux ayant accès au CDE et est recommandée pour tous les accès distants aux réseaux de l'entité.</p> <p>Les exigences de l'authentification MFA s'appliquent à tous les types de composants système, y compris le cloud, les systèmes hébergés et les applications sur site, les dispositifs de sécurité réseau, les postes de travail, les serveurs et les points de terminaison, et comportent l'accès direct aux réseaux ou systèmes d'une entité ainsi qu'un accès Web à une application ou à une fonction.</p>	

Exigences et Procédures de Test	Directives
<b>8.5 Les systèmes d'authentification multifacteurs (MFA) sont configurés de sorte à ne pas pouvoir être contournés.</b>	
<b>Exigences de L'approche Définie</b> <p><b>8.5.1</b> Les systèmes MFA sont mis en œuvre comme suit :</p> <ul style="list-style-type: none"> <li>• Le système MFA n'est pas sensible aux attaques par rejeu.</li> <li>• Les systèmes MFA ne peuvent pas être contournés par aucun utilisateur, y compris les administrateurs, à moins que cela ne soit spécifiquement documenté et autorisé par la direction à titre exceptionnel, pour une période limitée.</li> <li>• Au moins deux types différents de facteurs d'authentification sont utilisés.</li> <li>• La réussite de tous les facteurs d'authentification est obligatoire avant que l'accès ne soit accordé.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.5.1.a</b> Examiner la documentation du système du fournisseur afin de vérifier que le système MFA n'est pas susceptible d'être attaqué par rejeu.</p> <p><b>8.5.1.b</b> Examiner les configurations système pour la mise en œuvre du MFA afin de vérifier qu'elle est configurée conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>8.5.1.c</b> Interroger le personnel responsable et observer les processus afin de vérifier que toute demande de contournement du MFA est spécifiquement documentée et autorisée par la direction à titre exceptionnel, pour une période de temps limitée.</p> <p><b>8.5.1.d</b> Observer le personnel se connectant aux composants du système dans le CDE afin de vérifier que l'accès n'est accordé qu'une fois tous les facteurs d'authentification réussis.</p> <p><b>8.5.1.e</b> Observer le personnel se connectant à distance depuis l'extérieur du réseau de l'entité afin de vérifier que l'accès est accordé uniquement après que tous les facteurs d'authentification ont abouti.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les systèmes MFA résistent aux attaques et contrôlent strictement toutes les dérogations administratives.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</p>	<b>Objectif</b> Les systèmes MFA mal configuré peuvent être contournés par des attaques. Cette exigence concerne donc la configuration du ou des systèmes d'authentification MFA qui fournissent le MFA pour les utilisateurs accédant aux composants du système dans le CDE. <b>Définitions</b> L'utilisation d'un type de facteurs d'authentification deux fois (par exemple, l'utilisation de deux mots de passe distincts) n'est pas considérée comme une authentification multifacteur. Une attaque par rejeu se produit lorsqu'un attaquant intercepte une transmission valide de données, puis renvoie ou redirige cette communication à des fins malveillantes. Dans les implémentations MFA, les attaques par rejeu sont généralement utilisées pour obtenir un accès non autorisé en exploitant des informations d'identification légitimes. <b>Exemples</b> Voici des exemples de méthodes permettant de vous protéger contre les attaques par rejeu : <ul style="list-style-type: none"> <li>• Identifiants de session uniques et clés de session</li> <li>• Horodatages</li> <li>• Mots de passe ou codes d'accès à usage unique, basés sur le temps</li> <li>• Mécanismes anti-rejeu qui détectent et rejettent les tentatives d'authentification en double.</li> </ul> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p><b>Informations Complémentaires</b> Pour plus d'informations sur les systèmes et fonctionnalités du MFA, se reporter à ce qui suit : <i>Complément d'informations du PCI SSC : Multi-Factor Authentication.</i> Foire aux questions (FAQ) du PCI SSC sur ce sujet.</p>

Exigences et Procédures de Test	Directives
<b>8.6 Les comptes applicatifs, les comptes systèmes et les facteurs d'authentification associés est gérés rigoureusement.</b>	
<b>Exigences de L'approche Définie</b> <p><b>8.6.1</b> Si les comptes utilisés par les systèmes ou les applications peuvent être utilisés pour la connexion interactive, ils sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>• L'utilisation interactive est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles.</li> <li>• L'utilisation interactive est limitée au temps nécessaire à la circonstance exceptionnelle.</li> <li>• La justification métier de l'utilisation interactive est documentée.</li> <li>• L'utilisation interactive est explicitement approuvée par la direction.</li> <li>• L'identité de l'utilisateur individuel est confirmée avant que l'accès au compte ne soit accordé.</li> <li>• Chaque action entreprise est attribuable à un utilisateur individuel.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>8.6.1</b> Examiner les comptes applicatifs et système qui peuvent être utilisés de manière interactive et interroger les administrateurs afin de vérifier que les comptes applicatifs et système sont gérés conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Lorsqu'elles sont utilisées de manière interactive, toutes les actions avec des comptes désignés comme comptes système ou applicatifs sont autorisées et attribuables à une personne.</p>	
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> <p>Comme les comptes utilisateur individuels, les comptes système et applicatifs nécessitent une responsabilité et une gestion stricte pour s'assurer qu'ils sont utilisés uniquement aux fins prévues et qu'ils ne sont pas mal utilisés. Les attaquants compromettent souvent les comptes système ou applicatifs pour accéder aux données des titulaires de cartes.</p> <p><b>Bonne Pratique</b></p> <p>Dans la mesure du possible, configurer les comptes système et applicatifs pour interdire la connexion interactive afin d'empêcher les personnes non autorisées de se connecter et d'utiliser le compte avec ses priviléges système associés, et de limiter les machines et appareils sur lesquels le compte peut être utilisé.</p> <p><b>Définitions</b></p> <p>La connexion interactive est la possibilité pour une personne de se connecter à un compte système ou d'applications de la même manière qu'un compte utilisateur normal. L'utilisation des comptes système et applicatifs de cette manière signifie qu'il n'y a pas de responsabilité et de traçabilité des actions entreprises par l'utilisateur. Se reporter à l'Annexe G pour la définition du thème « Comptes applicatifs et système »</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.6.2</b> Les mots de passe/phrases secrètes pour tous les comptes applicatifs et système qui peuvent être utilisés pour la connexion interactive ne sont pas codés en dur dans les scripts, les fichiers de configuration/de propriété ou le code source sur mesure et personnalisé.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.6.2.a</b> Interroger le personnel et examiner les procédures de développement du système afin de vérifier que les processus sont définis pour les comptes applicatifs et système qui peuvent être utilisés pour la connexion interactive, en spécifiant que les mots de passe/phrases secrètes ne sont pas codés en dur dans les scripts, les fichiers de configuration ou de propriété, ou le code source sur mesure et personnalisé.</p> <p><b>8.6.2.b</b> Examiner les scripts, les fichiers de configuration/de propriété et le code source sur mesure et personnalisé pour les comptes applicatifs et système pouvant être utilisés pour une connexion interactive, afin de vérifier que les mots de passe/phrases secrètes pour ces comptes ne sont pas présents.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les mots de passe/phrases secrètes utilisés par les comptes applicatifs et système ne peuvent pas être utilisés par du personnel non autorisé.</p>	<p><b>Objectif</b> Ne pas protéger correctement les mots de passe/phrases secrètes utilisés par les comptes applicatifs et système, en particulier si ces comptes peuvent être utilisés pour une connexion interactive, augmente le risque et la réussite d'une utilisation non autorisée de ces comptes privilégiés.</p> <p><b>Bonne Pratique</b> La modification de ces valeurs en raison d'une divulgation soupçonnée ou confirmée peut être particulièrement difficile à mettre en œuvre. Les outils peuvent faciliter à la fois la gestion et la sécurité des facteurs d'authentification pour les comptes d'applications et système. Par exemple, pensez aux coffres de mots de passe ou à d'autres mesures de sécurité gérée par le système.</p>
<p><b>Notes D'applicabilité</b></p> <p>Les mots de passe/phrases secrètes stockés doivent être chiffrés conformément à l'exigence 8.3.2 du standard PCI DSS.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>8.6.3</b> Les mots de passe/phrases secrètes pour tous les comptes applicatifs et système sont protégés contre les abus comme suit :</p> <ul style="list-style-type: none"> <li>• Les mots de passe/phrases secrètes sont modifiés périodiquement (à la fréquence définie dans l'analyse de risques ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1) et en cas de soupçon ou de confirmation de compromission.</li> <li>• Les mots de passe/phrases secrètes sont construits avec une complexité suffisante adaptée à la fréquence à laquelle l'entité modifie les mots de passe/phrases secrètes.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>8.6.3.a</b> Examiner les politiques et procédures afin de vérifier que des procédures sont définies pour protéger les mots de passe/phrases secrètes pour les comptes applicatifs ou système contre les abus conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>8.6.3.b</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des modifications et la complexité des mots de passe/phrases secrètes pour les comptes applicatifs et système afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1 et aborde :</p> <ul style="list-style-type: none"> <li>• La fréquence définie pour les modifications périodiques des mots de passe/phrases secrètes de l'application et du système.</li> <li>• La complexité définie pour les mots de passe/phrases secrètes et la pertinence de la complexité par rapport à la fréquence des modifications.</li> </ul> <p><b>8.6.3.c</b> Interroger le personnel responsable et examiner les paramètres de configuration du système afin de vérifier que les mots de passe/phrases secrètes de toute application et de tout compte système sont protégés contre les abus conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les mots de passe/phrases secrètes utilisés par les comptes d'applications et système ne peuvent pas être utilisés indéfiniment et sont structurés pour résister aux attaques par force brute et par perçage.</p>	
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Objectif</b> Les systèmes et les comptes applicatifs présentent un risque de sécurité plus inhérent que les comptes d'utilisateurs, car ils s'exécutent souvent dans un contexte de sécurité élevé, avec un accès aux systèmes qui ne sont généralement pas accordés aux comptes utilisateur, tels que l'accès programmatique aux bases de données, etc. Par conséquent, une attention particulière doit être accordée à la protection des mots de passe/phrases secrètes utilisés pour les comptes d'applications et système.</p> <p><b>Bonne Pratique</b> Les entités doivent prendre en compte les facteurs de risque suivants lorsqu'elles déterminent la manière de protéger les mots de passe/phrases secrètes des applications et système contre les abus :</p> <ul style="list-style-type: none"> <li>• Le niveau de sécurité du stockage des mots de passe/phrases secrètes (par exemple, s'ils sont stockés dans un coffre de mots de passe).</li> <li>• Roulement du personnel.</li> <li>• Le nombre de personnes ayant accès au facteur d'authentification.</li> <li>• Si le compte peut être utilisé pour une connexion interactive.</li> <li>• Si la posture de sécurité des comptes est analysée dynamiquement et si l'accès en temps réel aux ressources est automatiquement déterminé en conséquence (voir l'exigence 8.3.9).</li> </ul> <p>Tous ces éléments affectent le niveau de risque pour les comptes applicatifs et système et peuvent avoir une incidence sur la sécurité des systèmes auxquels accèdent les comptes système et applicatifs.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p>Les entités doivent corréler la fréquence des modifications choisie pour les mots de passe/phrases secrètes applicatifs et système avec la complexité choisie pour ces mots de passe/phrases secrètes - c'est-à-dire que la complexité doit être plus rigoureuse lorsque les mots de passe/phrases secrètes sont modifiés peu fréquemment et peut être moins rigoureuse lorsqu'ils sont modifiés plus fréquemment. Par exemple, une fréquence de modification plus longue est plus justifiable lorsque la complexité des mots de passe/phrases secrètes est définie sur 36 caractères alphanumériques avec des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.</p> <p>Les meilleures pratiques consistent à prendre en compte les modifications de mots de passe au moins une fois par an, une longueur de mot de passe/phrase secrète d'au moins 15 caractères et la complexité des mots de passe/phrases secrètes de caractères alphanumériques, avec des lettres majuscules et minuscules et des caractères spéciaux.</p> <p><b>Informations Complémentaires</b></p> <p>Pour plus d'informations sur la variabilité et l'équivalence de la force du mot de passe pour les mots de passe/phrases secrètes de différents formats, consultez les standards de l'industrie (par exemple, la version actuelle du <i>NIST SP 800-63 Digital Identity Guidelines</i>).</p>

## **Exigence 9 : Limiter L'accès Physique aux Données des Titulaires de Cartes**

### **Sections**

- 9.1** Les processus et mécanismes de restriction de l'accès physique aux données des titulaires de cartes sont définis et compris.
- 9.2** Les mesures de sécurité d'accès physiques gèrent l'entrée dans les installations et les systèmes contenant les données des titulaires de cartes.
- 9.3** L'accès physique du personnel et des visiteurs est autorisé et géré.
- 9.4** Les supports contenant les données des titulaires de carte sont stockés, consultés, distribués et détruits de manière sécurisée.
- 9.5** Les dispositifs de point d'interaction (POI) sont protégés contre l'altération et la substitution non autorisée.

### **Aperçu**

Tout accès physique aux données des titulaires de cartes ou aux systèmes qui stockent, traitent ou transmettent les données des titulaires de cartes offre la possibilité à des personnes d'accéder et/ou de supprimer des systèmes ou des copies papier contenant des données de titulaires de cartes ; par conséquent, l'accès physique doit être limité de manière appropriée.

Il y a trois domaines différents mentionnés dans l'exigence 9 :

1. Les exigences qui se reportent spécifiquement aux zones sensibles sont destinées à s'appliquer uniquement à ces zones. Chaque entité doit identifier les zones sensibles de ses environnements pour garantir que les contrôles physiques appropriés sont mis en œuvre.
2. Les exigences qui se reportent spécifiquement à l'environnement de données des titulaires de cartes (CDE) sont destinées à s'appliquer à l'ensemble du CDE, y compris toutes les zones sensibles résidant au sein du CDE.
3. Les exigences qui se reportent spécifiquement à l'installation font référence aux types de mesures qui peuvent être gérés plus largement à la limite physique d'un local commercial (tel qu'un bâtiment) dans lequel résident les CDE et les zones sensibles. Ces mesures de sécurité existent souvent en dehors d'un CDE ou d'une zone sensible, par exemple un poste de garde qui identifie, badge et enregistre les visiteurs. Le terme « installation » est utilisé pour reconnaître que ces mesures de sécurité peuvent exister à différents endroits dans une installation, par exemple, à l'entrée d'un bâtiment ou à une entrée interne d'un centre de données ou d'un espace de bureau.

Se reporter à [l'Annexe G](#) pour les définitions de « médias », « personnel », « zones sensibles », « visiteurs » et d'autres termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>9.1 Les processus et mécanismes de restriction de l'accès physique aux données des titulaires de cartes sont définis et compris.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 9 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 9 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les attentes, les mesures de sécurité et la surveillance relatives à l'exigence 9 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<p><b>Objectif</b> L'exigence 9.1.1 concerne la gestion efficace et le maintien des diverses politiques et procédures spécifiées dans toute l'exigence 9. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 9, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique.</p> <p><b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.</p> <p>Les politiques et procédures, y compris les mises à jour, sont activement communiquées à tout le personnel concerné et sont justifiées par des procédures opérationnelles décrivant la manière d'effectuer les activités.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 9 sont documentés, attribués et compris.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 9 sont documentées et attribuées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 9 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>9.1.2.b</b> Interroger le personnel chargé d'exécuter les activités de l'exigence 9 afin de vérifier que les rôles et les responsabilités sont assignés comme documentés et qu'ils sont compris.</p> <p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués. Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable auditable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>9.2 Les mesures de sécurité d'accès physiques gèrent l'entrée dans les installations et les systèmes contenant les données des titulaires de cartes.</b>	
<b>Exigences de L'approche Définie</b> <p><b>9.2.1</b> Des mesures de sécurité d'accès aux installations appropriés sont en place pour limiter l'accès physique aux systèmes du CDE.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.2.1</b> Observer les mesures de sécurité dans les zones d'entrée et interroger le personnel responsable afin de vérifier que des mesures de sécurité de sécurité physique sont en place pour limiter l'accès aux systèmes du CDE.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les composants système dans le CDE ne sont pas physiquement accessibles par du personnel non autorisé.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique pas aux emplacements accessibles au public par les consommateurs (titulaires de carte).</p>	<b>Objectif</b> <p>Sans contrôle d'accès physique, des personnes non autorisées pourraient potentiellement accéder au CDE et aux informations sensibles, ou pourraient modifier les configurations du système, introduire des vulnérabilités dans le réseau, ou détruire ou voler des équipements. Par conséquent, le but de cette exigence est que l'accès physique au CDE soit contrôlé via des mesures de sécurité de sécurité physiques tels que des lecteurs de badges ou d'autres mécanismes tels que des serrures et des clés.</p> <b>Bonne Pratique</b> <p>Quel que soit le mécanisme qui répond à cette exigence, il doit être suffisant pour l'entreprise de vérifier que seul du personnel autorisé a accès.</p> <b>Exemples</b> <p>Les mesures de sécurité dans les zones d'entrée aux installations comprennent des mesures de sécurité de sécurité physique dans chaque salle informatique, centre de données et autres zones physiques avec des systèmes dans le CDE. Il peut également inclure des lecteurs de badges ou d'autres dispositifs qui gèrent les mesures de sécurité d'accès physiques, tels qu'une serrure et une clé avec une liste à jour de toutes les personnes détenant les clés.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.2.1.1</b> L'accès physique individuel aux zones sensibles au sein du CDE est surveillé à l'aide de caméras vidéo ou de mécanismes de contrôle d'accès physique (ou les deux), des manières suivantes :</p> <ul style="list-style-type: none"> <li>• Les points d'entrée et de sortie des zones sensibles du CDE sont surveillés.</li> <li>• Les dispositifs ou mécanismes de surveillance sont protégés contre l'altération ou la désactivation.</li> <li>• Les données recueillies sont examinées et corrélées avec d'autres entrées.</li> <li>• Les données recueillies sont conservées pendant au moins trois mois, sauf restriction légale contraire.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.2.1.1.a</b> Observer les emplacements où a lieu l'accès physique individuel aux zones sensibles du CDE afin de vérifier que des caméras vidéo ou des mécanismes de contrôle d'accès physique (ou les deux) sont en place pour surveiller les points d'entrée et de sortie.</p> <p><b>9.2.1.1.b</b> Observer les emplacements où a lieu l'accès physique individuel aux zones sensibles du CDE afin de vérifier que des caméras vidéo ou des mécanismes de contrôle d'accès physique (ou les deux) sont protégés contre l'altération ou la désactivation.</p> <p><b>9.2.1.1.c</b> Observer les mécanismes de contrôle d'accès physique et/ou examiner les caméras vidéo et interroger le personnel responsable afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• Les données recueillies à partir des caméras vidéo et/ou des mécanismes de contrôle d'accès physique sont examinées et corrélées avec d'autres entrées.</li> <li>• Les données recueillies sont conservées pendant au moins trois mois.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des enregistrements fiables et vérifiables sont conservés pour chaque entrée et sortie physiques des zones sensibles.</p>	<p><b>Objectif</b></p> <p>Le maintien des détails des personnes entrantes et sortantes des zones sensibles peut aider aux enquêtes sur les violations physiques en identifiant les personnes qui ont physiquement accédé aux zones sensibles, ainsi que les heures auxquelles elles sont entrées et sorties.</p> <p><b>Bonne Pratique</b></p> <p>Quel que soit le mécanisme qui satisfait à cette exigence, il doit surveiller efficacement tous les points d'entrée et de sortie des zones sensibles. Les criminels qui tentent d'accéder physiquement à des zones sensibles essaieront souvent de désactiver ou de contourner les mesures de sécurité de surveillance. Pour protéger ces mesures de sécurité contre les altérations, des caméras vidéo peuvent être positionnées de manière à ce qu'elles soient hors de périmètre et/ou être surveillées pour détecter les altérations. De même, les mécanismes de contrôle d'accès physique pourraient être surveillés où avoir des protections physiques installées pour les empêcher d'être endommagés ou désactivés par des personnes malveillantes.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.2.2</b> Des mesures de sécurité physiques et/ou logiques sont mis en œuvre pour limiter l'utilisation des prises réseaux accessibles au public au sein de l'installation.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les appareils non autorisés ne peuvent pas se connecter au réseau de l'entité à partir des zones publiques de l'installation.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.2.2</b> Interroger le personnel responsable et observer les emplacements des prises réseaux accessibles au public afin de vérifier que des mesures de sécurité physiques et/ou logiques sont en place pour limiter l'accès aux prises réseaux accessibles au public au sein de l'installation.</p>

Exigences et Procédures de Test	Directives	
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.2.3</b> L'accès physique aux points d'accès sans fil, aux passerelles, au matériel de mise en réseau/de communication et aux lignes de télécommunication au sein de l'installation est limité.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>L'équipement réseau n'est pas accessible physiquement au personnel non autorisé.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.2.3</b> Interroger le personnel responsable et observer l'emplacement du matériel et des câbles afin de vérifier que l'accès physique aux points d'accès sans fil, aux passerelles, au matériel de réseau/de communication et aux lignes de télécommunication au sein de l'installation est limité.</p>	<p><b>Objectif</b></p> <p>Sans une sécurité physique appropriée régissant l'accès aux composants et appareils sans fil, et aux équipements et lignes de réseau informatique et de télécommunications, des utilisateurs malveillants pourraient accéder aux ressources réseau de l'entité. De plus, ils pourraient connecter leurs propres appareils au réseau pour obtenir un accès non autorisé au CDE ou aux systèmes connectés au CDE.</p> <p>De plus, la sécurisation du matériel de mise en réseau et de communication empêche les utilisateurs malveillants d'intercepter le trafic réseau ou de connecter physiquement leurs propres appareils aux ressources du réseau câblé.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.2.4</b> L'accès aux consoles dans les zones sensibles est limité par un système de verrouillage lorsqu'elles ne sont pas utilisées.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les consoles physiques dans les zones sensibles ne peuvent pas être utilisées par du personnel non autorisé.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.2.4</b> Observer la tentative d'un administrateur système de se connecter aux consoles dans les zones sensibles et vérifier qu'elles sont « verrouillées » afin d'empêcher toute utilisation non autorisée.</p>	<p><b>Objectif</b></p> <p>Le verrouillage des écrans de connexion à la console empêche les personnes non autorisées d'accéder à des informations sensibles, de modifier les configurations du système, d'introduire des vulnérabilités dans le réseau ou de détruire des enregistrements.</p>

Exigences et Procédures de Test	Directives
<b>9.3 L'accès physique du personnel et des visiteurs est autorisé et géré.</b>	
<b>Exigences de L'approche Définie</b> <p><b>9.3.1</b> Des procédures sont mises en œuvre pour autoriser et gérer l'accès physique du personnel au CDE, notamment :</p> <ul style="list-style-type: none"> <li>• Identification du personnel.</li> <li>• L'exigence de gérer les modifications d'accès physique d'une personne.</li> <li>• Révoquer ou mettre fin à l'identification du personnel.</li> <li>• Limiter l'accès au processus ou au système d'identification au personnel autorisé.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.3.1.a</b> Examiner les procédures documentées afin de vérifier que les procédures d'autorisation et de gestion de l'accès physique du personnel au CDE sont définies conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>9.3.1.b</b> Observer les méthodes d'identification, telles que les badges d'identification, et observer les processus afin de vérifier que le personnel du CDE est clairement identifié</p> <p><b>9.3.1.c</b> Observer les processus afin de vérifier que l'accès au processus d'identification, tel qu'un système de badge, est limité au personnel autorisé.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les conditions d'accès au CDE physique sont définies et appliquées pour identifier et autoriser le personnel.</p>	<b>Objectif</b> L'établissement de procédures pour accorder, gérer et supprimer l'accès lorsqu'il n'est plus nécessaire, garantit que les personnes non autorisées sont empêchées d'accéder aux zones contenant les données des titulaires de cartes. De plus, il est important de limiter l'accès au système de badges et au matériel de badgeage afin d'empêcher le personnel non autorisé de créer ses propres badges et/ou d'établir ses propres règles d'accès. <b>Bonne Pratique</b> Il est important d'identifier visuellement le personnel qui est physiquement présent et s'il s'agit d'un visiteur ou d'un employé. <b>Définitions</b> Se reporter à l'Annexe G pour la définition de « personnel » <b>Exemples</b> Une façon d'identifier le personnel est de leur attribuer des badges.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.3.1.1</b> L'accès physique aux zones sensibles au sein du CDE pour le personnel est contrôlé comme suit :</p> <ul style="list-style-type: none"> <li>• L'accès est autorisé et basé sur la fonction individuelle du poste.</li> <li>• L'accès est révoqué immédiatement après la résiliation du contrat de travail.</li> <li>• Tous les mécanismes d'accès physiques, tels que les clés, les cartes d'accès, etc., sont retournés ou désactivés lors de la résiliation du contrat.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.3.1.1.a</b> Observer le personnel dans les zones sensibles du CDE, interroger le personnel responsable et examiner les listes de contrôle d'accès physique afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• L'accès à la zone sensible est autorisé.</li> <li>• L'accès est requis pour la fonction métier de l'individu.</li> </ul> <p><b>9.3.1.1.b</b> Observer les processus et interroger le personnel afin de vérifier que l'accès de tout le personnel est révoqué immédiatement après la résiliation du contrat.</p> <p><b>9.3.1.1.c</b> Pour le personnel ayant quitté l'entreprise, examiner les listes de contrôle d'accès physique et interroger le personnel responsable afin de vérifier que tous les mécanismes d'accès physique (tels que les clés, les cartes d'accès, etc.) ont été restitués ou désactivés.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les zones sensibles ne sont pas accessibles au personnel non autorisé.</p>	<p><b>Objectif</b> Le contrôle de l'accès physique aux zones sensibles permet de garantir que seul le personnel autorisé ayant un besoin métier légitime peut y avoir accès.</p> <p><b>Bonne Pratique</b> Dans la mesure du possible, les entreprises doivent disposer de politiques et de procédures garantissant qu'avant que le personnel ne quitte l'entreprise, tous les mécanismes d'accès physique soient rendus ou désactivés dès que possible après leur départ. Cela garantira que le personnel ne pourra pas accéder physiquement aux zones sensibles une fois son emploi terminé.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.3.2</b> Des procédures sont mises en œuvre afin d'autoriser et gérer l'accès des visiteurs au CDE, notamment :</p> <ul style="list-style-type: none"> <li>• Les visiteurs sont autorisés avant d'entrer.</li> <li>• Les visiteurs sont escortés en tout temps.</li> <li>• Les visiteurs sont clairement identifiés et reçoivent un badge ou autre moyen les identifiants, ayant un délai d'expiration.</li> <li>• Les badges de visiteur ou autre moyen d'identification distinguent visiblement les visiteurs du personnel.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.3.2.a</b> Examiner les procédures documentées et interroger le personnel afin de vérifier que des procédures sont définies pour autoriser et gérer l'accès des visiteurs au CDE conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>9.3.2.b</b> Observer les processus lorsque des visiteurs sont présents dans le CDE et interroger le personnel afin de vérifier que les visiteurs sont :           <ul style="list-style-type: none"> <li>• Autorisés avant d'entrer au CDE.</li> <li>• Escortés en tout temps à l'intérieur du CDE.</li> </ul> </p> <p><b>9.3.2.c</b> Observer l'utilisation de badges des visiteurs ou autre moyen d'identification afin de vérifier que le badge ou autre moyen d'identification ne permet pas un accès sans escorte au CDE.</p> <p><b>9.3.2.d</b> Observer les visiteurs dans le CDE afin de vérifier que :           <ul style="list-style-type: none"> <li>• Des badges de visiteurs ou autre moyen d'identification sont utilisés pour tous les visiteurs.</li> <li>• Les badges de visiteur ou autre moyen d'identification distinguent visiblement les visiteurs du personnel.</li> </ul> </p> <p><b>9.3.2.e</b> Examiner les badges des visiteurs ou autres pièces d'identité et observer les preuves dans le système de badges afin de vérifier que les badges des visiteurs ou autres moyens d'identification ont expiré.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les exigences relatives à l'accès des visiteurs au CDE sont définies et appliquées. Les visiteurs ne peuvent pas dépasser tout accès physique autorisé lorsqu'ils sont dans le CDE.</p>	<p><b>Objectif</b> Les mesures de sécurité des visiteurs sont importantes pour réduire la capacité des personnes non autorisées et malveillantes à accéder aux installations et potentiellement aux données des titulaires de cartes.</p> <p>Les mesures de sécurité des visiteurs garantissent que les visiteurs sont identifiables en tant que visiteurs afin que le personnel puisse surveiller leurs activités et que leur accès soit limité à la durée de leur visite légitime.</p> <p><b>Définitions</b> Se reporter à l'Annexe G pour la définition de « visiteur »</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.3.3</b> Les badges ou les pièces d'identité des visiteurs sont remis ou désactivés avant que les visiteurs ne quittent l'établissement ou à la date d'expiration.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>L'identification des visiteurs ou les badges ne peuvent pas être réutilisés après expiration.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.3.3</b> Observer les visiteurs quittant l'établissement et interroger le personnel afin de vérifier que les badges de visiteurs ou autre pièce d'identité sont remis ou désactivés avant que les visiteurs ne quittent l'établissement ou à la date d'expiration, au départ ou à l'expiration.</p> <p><b>Objectif</b></p> <p>Veiller à ce que les badges des visiteurs soient rendus ou désactivés à l'expiration ou à la fin de la visite, empêche les personnes malveillantes d'utiliser un laissez-passer préalablement autorisé pour accéder physiquement au bâtiment une fois la visite terminée.</p>
<b>Exigences de L'approche Définie</b> <p><b>9.3.4</b> Les journaux de visiteurs sont utilisés pour conserver un enregistrement physique de l'activité des visiteurs à la fois au sein de l'installation et dans les zones sensibles, y compris :</p> <ul style="list-style-type: none"> <li>• Le nom du visiteur et l'organisation représentée.</li> <li>• La date et l'heure de la visite.</li> <li>• Le nom du personnel autorisant l'accès physique.</li> <li>• Conserver le journal pendant au moins trois mois, sauf restriction légale contraire.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Des enregistrements de l'accès des visiteurs qui permettent l'identification des personnes sont conservés.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.3.4.a</b> Examiner les journaux des visiteurs et interroger le personnel responsable afin de vérifier que des journaux de visiteurs est utilisé pour enregistrer l'accès physique à la fois à l'installation et aux zones sensibles.</p> <p><b>9.3.4.b</b> Examiner les journaux des visiteurs et vérifier qu'ils contiennent :</p> <ul style="list-style-type: none"> <li>• Le nom du visiteur et l'organisation représentée.</li> <li>• Le personnel autorisant l'accès physique.</li> <li>• Date et heure de la visite.</li> </ul> <p><b>9.3.4.c</b> Examiner les emplacements de stockage des journaux des visiteurs et interroger le personnel responsable afin de vérifier que le journal est conservé pendant au moins trois mois, sauf indication contraire par la loi.</p> <p><b>Objectif</b></p> <p>Un journal des visiteurs documentant un minimum d'informations sur le visiteur est facile et peu coûteux à maintenir. Il aidera à identifier l'historique d'accès physique à un bâtiment ou à une pièce et l'accès potentiel aux données des titulaires de cartes.</p> <p><b>Bonne Pratique</b></p> <p>Lors de l'enregistrement de la date et de l'heure de la visite, l'inclusion des heures d'entrée et de sortie est considérée comme une Bonne Pratique, car elle fournit des informations de suivi utiles et garantit qu'un visiteur est parti à la fin de la journée. Il est également bon de vérifier que l'identifiant d'un visiteur (permis de conduire, etc.) correspond au nom qu'il a inscrit dans le journal des visiteurs.</p>

Exigences et Procédures de Test		Directives
<b>9.4 Les supports contenant les données des titulaires de carte sont stockés, consultés, distribués et détruits de manière sécurisée.</b>		
<b>Exigences de L'approche Définie</b>  <b>9.4.1</b> Tous les supports contenant les données des titulaires de cartes sont physiquement sécurisés.	<b>Procédures de Test de L'approche Définie</b>  <b>9.4.1.</b> Examiner la documentation afin de vérifier que les procédures définies pour la protection des données des titulaires de cartes comportent des mesures pour sécuriser physiquement tous les supports	<b>Objectif</b> Les mesures de sécurité de sécurité physique des supports sont destinées à empêcher les personnes non autorisées d'accéder aux données des titulaires de cartes sur n'importe quel support. Les données des titulaires de cartes sont susceptibles d'être visualisées, copiées ou numérisées sans autorisation si elles ne sont pas protégées alors qu'elles se trouvent sur un support amovible ou portable, imprimées ou laissées sur le bureau d'un employé.
<b>Objectif de L'approche Personnalisée</b>  Les supports contenant les données de titulaires de cartes ne sont pas accessibles au personnel non autorisé.		
<b>Exigences de L'approche Définie</b>  <b>9.4.1.1</b> Les sauvegardes hors ligne des supports contenant les données des titulaires de cartes sont stockées dans un emplacement sécurisé.	<b>Procédures de Test de L'approche Définie</b>  <b>9.4.1.1.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour sécuriser physiquement les sauvegardes hors ligne des supports contenant les données des titulaires de cartes dans un emplacement sécurisé.  <b>9.4.1.1.b</b> Examiner les journaux ou toute autre documentation et interroger le personnel responsable de l'emplacement de stockage afin de vérifier que les sauvegardes hors ligne des supports contenant les données des titulaires de cartes sont stockées dans un emplacement sécurisé.	<b>Objectif</b> Si elles sont stockées dans une installation non sécurisée, les sauvegardes contenant les données des titulaires de cartes peuvent facilement être perdues, volées ou copiées à des fins malveillantes.  <b>Bonne Pratique</b> Pour un stockage sécurisé des supports de sauvegarde, une Bonne Pratique consiste à stocker les supports dans une installation hors site, telle qu'un site alternatif ou de sauvegarde ou dans les locaux d'un prestataire tiers de service de stockage.
<b>Objectif de L'approche Personnalisée</b>  Les sauvegardes hors ligne ne sont pas accessibles au personnel non autorisé.		

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>9.4.1.2</b> La sécurité des emplacements de sauvegarde hors ligne des supports contenant les données des titulaires de cartes est examinée au moins une fois tous les 12 mois.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.1.2.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour examiner la sécurité du ou des emplacements de sauvegarde hors ligne des supports avec les données des titulaires de cartes au moins une fois tous les 12 mois.</p>	<b>Objectif</b> La réalisation d'examens réguliers de l'installation de stockage permet à l'entreprise de résoudre rapidement les problèmes de sécurité identifiés, en minimisant les risques potentiels. Il est important que l'entité soit consciente de la sécurité de la zone dans laquelle les supports sont stockés.
<b>Objectif de L'approche Personnalisée</b> <p>Les mesures de sécurité de sécurité protégeant les sauvegardes hors ligne sont vérifiées périodiquement par inspection.</p>	<p><b>9.4.1.2.b</b> Examiner les procédures documentées, les journaux ou toute autre documentation, et interroger le personnel responsable du ou des emplacements de stockage afin de vérifier que la sécurité de l'emplacement du stockage est examinée au moins une fois tous les 12 mois.</p>	
<b>Exigences de L'approche Définie</b> <p><b>9.4.2</b> Tous les supports contenant des données de titulaires de cartes sont classés en fonction de la sensibilité des données.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.2.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour classer les supports avec les données des titulaires de cartes en fonction de la sensibilité des données.</p>	<b>Objectif</b> Les supports non identifiés comme confidentiels peuvent ne pas être protégés de manière adéquate ou peuvent être perdus ou volés. <b>Bonne Pratique</b> Il est important que les supports soient identifiés de manière à ce que leur statut de classification soit apparent. Cela ne signifie pas pour autant que les médias doivent avoir un label « confidentiel ».
<b>Objectif de L'approche Personnalisée</b> <p>Les médias sont classés et protégés de manière appropriée.</p>	<p><b>9.4.2.b</b> Examiner les journaux liés aux supports ou toute autre documentation afin de vérifier que tous les médias sont classés en fonction de la sensibilité des données.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.4.3</b> Les supports avec les données des titulaires de cartes envoyées à l'extérieur de l'installation sont sécurisés comme suit :</p> <ul style="list-style-type: none"> <li>• Les supports envoyés à l'extérieur de l'installation sont documentés.</li> <li>• Les supports sont envoyés par courrier sécurisé ou par un autre mode de livraison pouvant être suivi avec précision.</li> <li>• La documentation de suivi des supports hors site inclue des détails sur l'emplacement.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les supports sont sécurisés et suivis lorsqu'ils sont transportés hors de l'installation.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.4.3.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour sécuriser les supports envoyés à l'extérieur de l'installation conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>9.4.3.b</b> Interroger le personnel et examiner les dossiers afin de vérifier que tous les supports envoyés à l'extérieur de l'installation sont documentés et envoyés par courrier sécurisé ou par une autre méthode de livraison pouvant être suivie.</p> <p><b>9.4.3.c</b> Examiner la documentation de suivi des supports hors site, pour tous les supports, afin de vérifier que les détails de suivi sont documentés.</p> <p><b>Objectif</b>            Les supports peuvent être perdus ou volés s'ils sont envoyés via une méthode n'assurant pas le suivi telle que le courrier postal ordinaire. L'utilisation de coursiers sécurisés pour livrer tout support contenant des données de titulaires de cartes permet aux entreprises d'utiliser leurs systèmes de suivi pour maintenir l'inventaire et l'emplacement des expéditions.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.4.4</b> La direction approuve tous les supports avec des données de titulaires de cartes qui sont déplacés hors de l'installation (y compris lorsque les supports sont distribués à des personnes individuelles).</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.4.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour garantir que les supports déplacés hors de l'installation sont approuvés par la direction.</p> <p><b>9.4.4.b</b> Examiner la documentation de suivi des supports hors site et interroger le personnel responsable afin de vérifier qu'une autorisation de la direction est obtenue pour tous les supports déplacés hors de l'installation (y compris les supports distribués à des personnes individuelles).</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les médias ne peuvent pas quitter une installation sans l'approbation du personnel responsable.</p>	<b>Objectif</b> Sans un processus ferme pour garantir que tous les mouvements des supports sont approuvés avant que les médias ne soient retirés des zones sécurisées, les supports ne seraient pas suivis ou protégés de manière appropriée, et leur emplacement serait inconnu, ce qui entraînerait la perte ou le vol desdits supports.
<b>Notes D'applicabilité</b> <p>Les personnes qui approuvent les mouvements des supports devraient avoir le niveau hiérarchique approprié pour accorder cette approbation. Cependant, il n'est pas spécifiquement exigé que ces personnes aient l'indication « responsable » dans leur titre.</p>	
<b>Exigences de L'approche Définie</b> <p><b>9.4.5</b> Un inventaire de tous les supports électroniques contenant les données des titulaires de cartes est conservé.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.5.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour maintenir un inventaire des médias électroniques.</p> <p><b>9.4.5.b</b> Examiner les journaux l'inventaire des médias électroniques et interroger le personnel responsable afin de vérifier que l'inventaire est maintenu à jour.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Des inventaires précis des supports électroniques stockés sont conservés.</p>	<b>Objectif</b> Sans méthodes d'inventaire et mesures de sécurité de stockage minutieux, les supports électroniques volés ou manquants pourraient passer inaperçus pendant une durée indéterminée.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.4.5.1</b> Les inventaires des supports électroniques avec les données des titulaires de cartes sont réalisés au moins une fois tous les 12 mois.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.5.1.a</b> Examiner la documentation afin de vérifier que des procédures sont définies pour effectuer des inventaires des supports électroniques avec les données des titulaires de cartes au moins une fois tous les 12 mois.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les inventaires des supports sont vérifiés périodiquement.</p>	<p><b>9.4.5.1.b</b> Examiner les journaux d'inventaire des médias électroniques et interroger le personnel afin de vérifier que les inventaires des supports électroniques sont effectués au moins une fois tous les 12 mois.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.4.6</b> Les documents papier contenant les données des titulaires de cartes sont détruits lorsqu'ils ne sont plus nécessaires pour des raisons métiers ou juridiques, comme suit :</p> <ul style="list-style-type: none"> <li>• Les matériaux sont déchiquetés, incinérés ou réduits en pâte afin que les données des titulaires de cartes ne puissent pas être reconstituées.</li> <li>• Les documents sont stockés dans des conteneurs de stockage sécurisés avant destruction.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.4.6.a</b> Examiner la politique de destruction des supports afin de vérifier que des procédures sont définies pour détruire les supports papier contenant les données des titulaires de cartes lorsqu'ils ne sont plus nécessaires pour des raisons métiers ou juridiques, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>9.4.6.b</b> Observer les processus et interroger le personnel pour vérifier que les documents papier sont déchiquetés, incinérés ou réduits en pâte de telle sorte que les données des titulaires de cartes ne puissent pas être reconstituées.</p> <p><b>9.4.6.c</b> Observer les conteneurs de stockage utilisés pour les documents contenant des informations à détruire afin de vérifier que les conteneurs sont sécurisés.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les données des titulaires de cartes ne peuvent pas être récupérées à partir d'un support détruit ou en attente de destruction.</p>	<p><b>Objectif</b> Si des mesures ne sont pas prises pour détruire les informations contenues sur les supports papier avant leur élimination, des personnes malveillantes peuvent récupérer des informations à partir des supports éliminés, ce qui entraîne une compromission desdites données. Par exemple, des personnes malveillantes peuvent utiliser une technique connue sous le nom de « Fouille des poubelles », où ils fouillent dans les poubelles et les corbeilles de recyclage à la recherche de documents papier contenant des informations qu'ils peuvent utiliser pour lancer une attaque.</p> <p>La sécurisation des conteneurs de stockage utilisés pour les documents qui vont être détruits empêche la capture d'informations sensibles pendant la collecte des documents.</p> <p><b>Bonne Pratique</b> Envisager des conteneurs « à déchiqueter » avec un verrou qui empêche l'accès à leur contenu ou qui empêche physiquement l'accès à l'intérieur du conteneur.</p> <p><b>Informations Complémentaires</b> <i>Publication spéciale 800-88 du NIST, Révision 1 : Directives pour l'effacement des supports de stockage.</i></p>
<p><b>Notes D'applicabilité</b></p> <p>Ces exigences relatives à la destruction du support lorsque ce support n'est plus nécessaire pour des raisons métiers ou juridiques sont distinctes de l'exigence 3.2.1 du standard PCI DSS, qui vise à supprimer en toute sécurité les données des titulaires de cartes lorsque celles-ci ne sont plus nécessaires conformément aux politiques de conservation des données des titulaires de carte de l'entité.</p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.4.7</b> Les supports électroniques contenant les données de titulaires de cartes sont détruits lorsqu'ils ne sont plus nécessaires pour des raisons métier ou juridiques via l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Les supports électroniques sont détruits.</li> <li>• Les données des titulaires de cartes sont rendues irrécupérables de sorte qu'elles ne peuvent pas être reconstituées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.4.7.a</b> Examiner la politique de destruction des supports afin de vérifier que des procédures sont définies pour détruire les supports électroniques lorsqu'ils ne sont plus nécessaires pour des raisons métier ou juridiques, conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>9.4.7.b</b> Observer le processus de destruction des supports et interroger le personnel responsable afin de vérifier que les supports électroniques contenant les données des titulaires de cartes sont détruits via l'une des méthodes spécifiées dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les données des titulaires des cartes ne peuvent pas être récupérées à partir d'un support qui a été effacé ou détruit.</p>	<b>Objectif</b> Si des mesures ne sont pas prises pour détruire les informations contenues sur les supports électroniques lorsqu'elles ne sont plus nécessaires, des personnes malveillantes peuvent récupérer des informations à partir des supports mis au rebut, entraînant une compromission des données. Par exemple, des personnes malveillantes peuvent utiliser une technique connue sous le nom de « Fouille des poubelles », où ils fouillent dans les poubelles et les corbeilles de recyclage à la recherche d'informations qu'ils peuvent utiliser pour lancer une attaque.
<b>Notes D'applicabilité</b> <p>Ces exigences relatives à la destruction du support lorsque ce support n'est plus nécessaire pour des raisons métier ou juridiques sont distinctes de l'exigence 3.2.1 du standard PCI DSS, qui vise à supprimer en toute sécurité les données des titulaires de cartes lorsque celles-ci ne sont plus nécessaires conformément aux politiques de conservation des données des titulaires de carte de l'entité.</p>	<b>Bonne Pratique</b> La fonction de suppression de la plupart des systèmes d'exploitation permet de récupérer les données supprimées. Par conséquent, une fonction ou une application de suppression sécurisée dédiée doit être utilisée pour rendre les données irrécupérables. <p><b>Exemples</b></p> <p>Les méthodes de destruction sécurisée des supports électroniques comprennent l'effacement sécurisé conformément aux standards acceptés par l'industrie pour la suppression sécurisée, la démagnétisation ou la destruction physique (telle que le broyage ou le déchiquetage des disques durs).</p> <p><b>Informations Complémentaires</b>  <i>Publication spéciale 800-88 du NIST, Revision 1: Guidelines for Media Sanitization.</i></p>

Exigences et Procédures de Test	Directives
<b>9.5 Les dispositifs de point d'interaction (POI) sont protégés contre l'altération et la substitution non autorisée.</b>	
<b>Exigences de L'approche Définie</b> <p><b>9.5.1</b> Les appareils POI qui capturent les données de la carte de paiement via une interaction physique directe avec le facteur de forme de la carte de paiement sont protégés contre l'altération et la substitution non autorisée, notamment :</p> <ul style="list-style-type: none"> <li>• Maintenir une liste des périphériques POI.</li> <li>• Inspecter périodiquement les appareils POI pour rechercher des altérations ou des substitutions non autorisées.</li> <li>• Former le personnel à être conscient des comportements suspects et à signaler toute altération ou substitution non autorisée d'appareils.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.5.1</b> Examiner les politiques et procédures documentées afin de vérifier que des processus sont définis et incluent tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>L'entité a défini des procédures pour protéger et gérer les dispositifs de point d'interaction. Les attentes, les mesures de sécurité et la surveillance de la gestion et de la protection des appareils POI sont définis et respectés par le personnel concerné.</p>	<b>Objectif</b> <p>Les criminels tentent de voler les données des cartes de paiement en volant et/ou en manipulant des appareils et des terminaux de lecture de cartes. Les criminels essaieront de voler des appareils afin qu'ils puissent apprendre à les compromettre, et ils essaient souvent de remplacer les appareils légitimes par des appareils frauduleux qui leur envoient des données de carte de paiement chaque fois qu'une carte est insérée.</p> <p>Ils essaieront également d'ajouter des composants « de skimming » à l'extérieur des appareils, qui sont conçus pour capturer les données de carte de paiement avant qu'elles n'entrent dans l'appareil, par exemple, en attachant un lecteur de carte supplémentaire au-dessus du lecteur de carte légitime afin que les données de paiement de la carte soient capturées deux fois : une fois par le composant du criminel, et l'autre par le composant légitime de l'appareil.</p> <p>De cette façon, les transactions peuvent toujours être effectuées sans interruption pendant que le criminel « skim » les données de la carte de paiement au cours du processus.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Ces exigences s'appliquent aux appareils POI déployés utilisés dans les transactions par carte (c'est-à-dire un facteur de forme de carte de paiement tel qu'une carte qui est glissée, tapée ou insérée).</p> <p>Cette exigence ne s'applique pas aux :</p> <ul style="list-style-type: none"> <li>• Composants utilisés uniquement pour la saisie manuelle des clés de PAN</li> <li>• Appareils commerciaux disponibles sur le marché (COTS) (par exemple, les smartphones ou les tablettes), qui sont des appareils mobiles appartenant à des commerçants conçus pour la distribution sur le marché de masse.</li> </ul>	<p><b>Bonne Pratique</b></p> <p>Les entités peuvent envisager de mettre en œuvre une protection contre la falsification et la substitution non autorisée pour :</p> <ul style="list-style-type: none"> <li>• Les composants utilisés uniquement pour la saisie manuelle de la clé du PAN</li> <li>• Appareils commerciaux prêts à l'emploi (COTS) (par exemple, smartphones ou tablettes), qui sont des appareils mobiles appartenant à des commerçants et conçus pour une distribution sur le marché de masse.</li> </ul> <p><b>Informations Complémentaires</b></p> <p>D'autres bonnes pratiques en matière de prévention du skimming sont disponibles sur le site Web du PCI SSC.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.5.1.1</b> Une liste à jour des appareils POI est maintenue, y compris :</p> <ul style="list-style-type: none"> <li>• La marque et le modèle de l'appareil.</li> <li>• L'emplacement de l'appareil.</li> <li>• Numéro de série de l'appareil ou autres méthodes d'identification uniques.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.5.1.1.a</b> Examiner la liste des appareils POI afin de vérifier qu'elle comprend tous les éléments spécifiés dans cette exigence.</p> <p><b>9.5.1.1.b</b> Observer les appareils POI et les emplacements des appareils et comparez-les aux appareils de la liste afin de vérifier que la liste est exacte et à jour.</p> <p><b>9.5.1.1.c</b> Interroger le personnel afin de vérifier que la liste des appareils POI est mise à jour lorsque des appareils sont ajoutés, déplacés, mis hors service, etc.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'identité et l'emplacement des appareils POI sont documentés et connus à tout moment.</p>	<p><b>Objectif</b></p> <p>Tenir à jour une liste des appareils POI aide une entreprise à savoir où les appareils sont censés se trouver et à identifier rapidement si un appareil est manquant ou perdu.</p> <p><b>Bonne Pratique</b></p> <p>La méthode de maintien d'une liste de dispositifs peut être automatisée (par exemple, un système de gestion des appareils) ou manuelle (par exemple, documentée dans des enregistrements électroniques ou papier). Pour les dispositifs routiers, l'emplacement peut inclure le nom du personnel auquel le dispositif est attribué.</p> <p><b>Exemples</b></p> <p>Les méthodes pour conserver les emplacements des appareils comprennent l'identification de l'adresse du site ou de l'installation où se trouve l'appareil.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>9.5.1.2</b> Les surfaces des appareils POI sont inspectées périodiquement afin de détecter les altérations et les substitutions non autorisées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>9.5.1.2.a</b> Examiner les procédures documentées afin de vérifier que les processus sont définis pour les inspections périodiques des surfaces des appareils POI afin de détecter les altérations et les substitutions non autorisées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les appareils de point d'interaction ne peuvent pas être altérés, remplacés sans autorisation, ou avoir des accessoires de skimming installées sans détection en temps opportun.</p>	<p><b>Objectif</b> Des inspections régulières des appareils aideront les entreprises à détecter plus rapidement les altérations via des preuves externes (par exemple, l'ajout d'un skimmer de carte) ou le remplacement d'un appareil, minimisant ainsi l'impact potentiel de l'utilisation d'appareils frauduleux.</p> <p><b>Bonne Pratique</b> Les méthodes d'inspection périodique comprennent la vérification du numéro de série ou d'autres caractéristiques de l'appareil et la comparaison des informations avec la liste des appareils POI afin de vérifier que l'appareil n'a pas été remplacé par un appareil frauduleux.</p> <p><b>Exemples</b> Le type d'inspection dépendra de l'appareil. Par exemple, des photographies d'appareils connus pour être sécurisés peuvent être utilisées pour comparer l'apparence actuelle d'un appareil avec son apparence d'origine pour voir s'il a changé. Une autre option peut être d'utiliser un marqueur sécurisé, tel qu'un marqueur à lumière UV, pour marquer les surfaces et les ouvertures de l'appareil afin que toute altération ou remplacement soit apparents. Les criminels remplacent souvent le boîtier extérieur d'un appareil pour dissimuler leur altération, et ces méthodes peuvent aider à détecter de telles activités. Les fournisseurs d'appareils peuvent également fournir des conseils de sécurité et des guides pratiques pour aider à déterminer si l'appareil a fait l'objet d'une altération.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Les signes indiquant qu'un appareil ont pu être altéré ou remplacé comprennent :</p> <ul style="list-style-type: none"> <li>• Des accessoires inattendus ou des câbles branchés sur l'appareil,</li> <li>• Des étiquettes de sécurité manquantes ou modifiées,</li> <li>• Un boîtier cassé, de couleur différente, ou</li> <li>• Des modifications du numéro de série ou d'autres marquages externes.</li> </ul>
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.5.1.2.1</b> La fréquence des inspections périodiques des appareils POI et le type d'inspections effectuées sont définis dans l'analyse de risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.5.1.2.1.a</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des inspections périodiques des appareils POI et le type d'inspections effectuées afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les appareils POI sont inspectés à une fréquence qui tient compte des risques de l'entité.</p>	<p><b>9.5.1.2.1.b</b> Examiner les résultats documentés des inspections périodiques des appareils et interroger le personnel afin de vérifier que la fréquence et le type d'inspections des appareils POI effectuées correspondent à ce qui est défini dans l'analyse de risques ciblée de l'entité menée dans le cadre de la présente exigence.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Objectif</b> Les entités sont les mieux placées pour déterminer la fréquence des inspections des appareils POI en fonction de l'environnement dans lequel l'appareil fonctionne.</p> <p><b>Bonne Pratique</b> La fréquence des inspections dépendra de facteurs tels que l'emplacement d'un appareil et si l'appareil est surveillé ou non. Par exemple, les appareils laissés dans des espaces publics sans la supervision du personnel de l'entreprise peuvent faire l'objet d'inspections plus fréquentes que les appareils conservés dans des zones sécurisées ou supervisés lorsqu'ils sont accessibles au public. En outre, de nombreux fournisseurs de POI incluent des conseils dans la documentation de leurs utilisateurs sur la fréquence à laquelle les appareils POI doivent être vérifiés et les raisons de le faire - les entités doivent consulter la documentation de leurs fournisseurs et intégrer ces recommandations dans leurs inspections périodiques.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>9.5.1.3</b> Une formation est dispensée au personnel des environnements POI pour qu'il soit au courant des pratiques d'altération ou de remplacement des appareils POI, et comprend :</p> <ul style="list-style-type: none"> <li>• Vérifier l'identité de toute personne tierce prétendant être du personnel de réparation ou de maintenance, avant de leur accorder l'accès pour modifier ou dépanner les appareils.</li> <li>• Des procédures pour garantir que les appareils ne sont pas installés, remplacés ou retournés sans vérification.</li> <li>• Être conscient des comportements suspects entourant les appareils.</li> <li>• Signaler les comportements suspects et les indications d'altération ou de substitution de l'appareil au personnel approprié.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>9.5.1.3.a</b> Examiner les supports de formation pour le personnel dans les environnements de POI afin de vérifier qu'ils comportent tous les éléments spécifiés dans cette exigence.</p> <p><b>9.5.1.3.b</b> Interroger le personnel dans les environnements de POI afin de vérifier que tous les membres ont reçu une formation et qu'ils connaissent les procédures pour tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le personnel connaît les types d'attaques contre les appareils POI, les contre-mesures techniques et procédurales de l'entité, et peut accéder à une assistance et à des conseils si nécessaire.</p>	<p><b>Objectif</b> Les criminels se font souvent passer pour du personnel de maintenance autorisé pour accéder aux appareils POI.</p> <p><b>Bonne Pratique</b> La formation du personnel doit inclure le fait d'être attentif et d'interroger toute personne qui se présente pour effectuer la maintenance des POI pour s'assurer qu'elle est autorisée et qu'elle dispose d'un bon de travail valide, y compris les agents, le personnel de maintenance ou de réparation, les techniciens, les prestataires de services ou d'autres tiers. Toutes les tierces parties demandant l'accès aux appareils doivent toujours être vérifiées avant de recevoir l'accès ; par exemple, en vérifiant auprès de la direction ou en téléphonant à la société de maintenance des points d'intérêt, telle que le prestataire ou acquéreur, pour vérification. De nombreux criminels essaieront de tromper le personnel en s'habillant déguisés comme des agents (par exemple, en portant des boîtes à outils et en portant des vêtements de travail), et pourraient également connaître l'emplacement des appareils, le personnel doit donc être formé pour toujours suivre les procédures.</p> <p>Une autre astuce utilisée par les criminels consiste à envoyer un « nouveau » appareil POI avec des instructions pour l'échanger avec un appareil légitime et « rendre » le nouvel appareil légitime. Les criminels peuvent même fournir des frais de retour à l'adresse indiquée. Par conséquent, le personnel doit toujours vérifier auprès de son responsable ou de son fournisseur que l'appareil est légitime et provient d'une source fiable avant de l'installer ou de l'utiliser à des fins professionnelles.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p><b>Exemples</b> Les comportements suspects dont le personnel doit être informé incluent les tentatives de personnes inconnues de débrancher ou d'ouvrir des appareils.</p> <p>S'assurer que le personnel connaît les mécanismes de signalement des comportements suspects et à qui signaler un tel comportement (par exemple, un chef hiérarchique ou un responsable de la sécurité) contribuera à réduire la probabilité et l'impact potentiel d'un appareil altéré ou remplacé.</p>

## Surveiller et Tester Régulièrement les Réseaux

### ***Exigence 10 : Enregistrer et Surveiller tous les Accès aux Composants Système et aux Données des Titulaires de Cartes***

#### Sections

- 10.1** Les processus et mécanismes d'enregistrement et de surveillance de tous les accès aux composants système et aux données des titulaires de cartes sont définis et compris.
- 10.2** Les journaux d'audit sont mis en œuvre pour prendre en charge la détection des anomalies et des activités suspectes, ainsi que l'analyse forensique des événements.
- 10.3** Les journaux d'audit sont protégés contre la destruction et les modifications non autorisées.
- 10.4** Les journaux d'audit sont examinés pour identifier les anomalies ou les activités suspectes.
- 10.5** L'historique des journaux d'audit est conservé et disponible pour analyse.
- 10.6** Les mécanismes de synchronisation temporelle prennent en charge des paramètres de temps cohérents sur tous les systèmes.
- 10.7** Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement.

#### Aperçu

Les mécanismes de journalisation et la capacité de suivre les activités des utilisateurs sont essentiels pour prévenir, détecter ou minimiser l'impact d'une compromission des données. La présence de journaux sur tous les composants système et dans l'environnement de données des titulaires de cartes (CDE) permet un suivi, une alerte et une analyse approfondis en cas de problème. Déterminer la cause d'une compromission est difficile, voire impossible, sans les journaux d'activité du système.

Cette exigence s'applique aux activités des utilisateurs, y compris celles des employés, des sous-traitants, des consultants et des fournisseurs internes et externes, et d'autres tiers (par exemple, ceux qui fournissent des services d'assistance ou de maintenance).

Ces exigences ne s'appliquent pas à l'activité d'utilisateur des consommateurs (titulaires de cartes).

Se reporter à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>10.1 Les processus et mécanismes d'enregistrement et de surveillance de tous les accès aux composants système et aux données des titulaires de cartes sont définis et compris.</b>	
<b>Exigences de L'approche Définie</b> <p><b>10.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 10 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles identifiées dans l'exigence 10 sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les attentes, les mesures de sécurité et la surveillance des activités de réunion dans l'exigence 10 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>	<b>Objectif</b> L'exigence 10.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 10. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 10, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées. <b>Bonne Pratique</b> Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents dès que possible après un changement et pas seulement sur un cycle périodique. <b>Définitions</b> Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat escompté de manière cohérente et conformément aux objectifs de la politique.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 10 sont documentés, attribués et compris.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 10 sont attribuées. Le personnel est responsable du bon fonctionnement continu desdites exigences.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.1.2.a</b> Examiner la documentation pour vérifier que les descriptions des rôles et des responsabilités pour l'exécution des activités de l'exigence 10 sont documentées et attribuées.</p> <p><b>10.1.2.b</b> Interroger le personnel chargé d'exécuter les activités de l'exigence 10 afin de vérifier que les rôles et les responsabilités sont assignés comme documentés et qu'ils sont compris.</p> <p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel peut ne pas être conscient de ses responsabilités quotidiennes et les activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents distincts. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, auditable consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<p><b>10.2 Les journaux d'audit sont mis en œuvre pour prendre en charge la détection des anomalies et des activités suspectes, ainsi que l'analyse criminelle des événements.</b></p>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.2.1</b> Les journaux d'audit sont activés et actifs pour tous les composants système et les données des titulaires de cartes.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.2.1</b> Interroger l'administrateur système et examiner les configurations système afin de vérifier que les journaux d'audit sont activés et actifs pour tous les composants système.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les enregistrements de toutes les activités affectant les composants système et les données des titulaires de cartes sont capturés.</p>	<p><b>Objectif</b></p> <p>Un journal doit exister pour tous les composants système. Les journaux d'audit envoient des alertes à l'administrateur système, fournissent des données à d'autres mécanismes de surveillance, tels que les systèmes de détection d'intrusion (IDS) et les outils de systèmes d'informations de sécurité et de surveillance des événements (SIEM), et fournissent un historique pour les enquêtes après incident.</p> <p>La journalisation et l'analyse des événements liés à la sécurité permettent à une entreprise d'identifier et de tracer les activités potentiellement malveillantes.</p> <p><b>Bonne Pratique</b></p> <p>Lorsqu'une entité considère les informations à enregistrer dans ses journaux, il est important de se rappeler que les informations stockées dans les journaux d'audit sont sensibles et doivent être protégées conformément aux exigences de ce standard. Il faut veiller à ne stocker que les informations essentielles dans les journaux d'audit afin de minimiser les risques.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.2.1.1</b> Les journaux d'audit capturent tous les accès des utilisateurs individuels aux données des titulaires de cartes.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les enregistrements de tous les accès des utilisateurs individuels aux données des titulaires de cartes sont capturés.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.2.1.1</b> Examiner les configurations des journaux d'audit et les données des journaux afin de vérifier que tous les accès des utilisateurs individuels aux données des titulaires de cartes sont enregistrés.</p> <p><b>Objectif</b> Il est essentiel d'avoir un processus ou un système qui relie l'accès des utilisateurs aux composants système auxquels ils accèdent. Des personnes malveillantes pourraient obtenir la connaissance d'un compte d'utilisateur ayant accès aux systèmes du CDE, ou ils pourraient créer un nouveau compte non autorisé pour accéder aux données des titulaires de cartes.</p> <p><b>Bonne Pratique</b> Un enregistrement de tous les accès individuels aux données des titulaires de cartes peut identifier les comptes qui peuvent avoir été compromis ou utilisés à des fins malveillantes.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.2.1.2</b> Les journaux d'audit capturent toutes les actions effectuées par toute personne disposant d'un accès d'administration, y compris toute utilisation interactive des comptes d'applications ou système.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les enregistrements de toutes les actions effectuées par des personnes disposant de priviléges élevés sont capturés.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.2.1.2</b> Examiner les configurations des journaux d'audit et les données des journaux afin de vérifier que toutes les actions entreprises par toute personne disposant d'un accès d'administration, y compris toute utilisation interactive des comptes d'applications ou système, sont enregistrées.</p> <p><b>Objectif</b> Les comptes avec des priviléges d'accès accrus, tels que le compte « administrateur » ou « root », ont le potentiel d'avoir un impact significatif sur la sécurité ou la fonctionnalité opérationnelle d'un système. Sans un journal des activités effectuées, une entreprise ne peut pas retracer les problèmes résultant d'une erreur administrative ou d'un abus de privilège jusqu'à l'action et le compte spécifiques.</p> <p><b>Définitions</b> Les fonctions ou activités considérées comme d'administration sont au-delà de celles exécutées par les utilisateurs réguliers dans le cadre des fonctions métier de routine. Se reporter à l'Annexe G pour la définition de « Accès administratif »</p>

Exigences et Procédures de Test	Directives	
<b>Exigences de L'approche Définie</b> <p><b>10.2.1.3</b> Les journaux d'audit capturent tous les accès aux journaux d'audit.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.2.1.3</b> Examiner les configurations des journaux d'audit et les données des journaux afin de vérifier que l'accès à tous les journaux d'audit est capturé.</p>	<b>Objectif</b> Les utilisateurs malveillants tentent souvent de modifier les journaux d'audit pour masquer leurs actions. Un enregistrement d'accès permet à une entreprise de retracer toute incohérence ou altération potentielle des journaux jusqu'à un compte individuel. Le fait que les journaux identifient les modifications, les ajouts et les suppressions dans les journaux d'audit peut aider à retracer les étapes effectuées par du personnel non autorisé.
<b>Objectif de L'approche Personnalisée</b> Les enregistrements de tous les accès aux journaux d'audit sont capturés.	<b>Procédures de Test de L'approche Définie</b> <p><b>10.2.1.4</b> Examiner les configurations des journaux d'audit et les données des journaux afin de vérifier que les tentatives d'accès logique non valides sont capturées.</p>	<b>Objectif</b> Les personnes malveillantes effectueront souvent plusieurs tentatives d'accès aux systèmes ciblés. Plusieurs tentatives de connexion non valides peuvent être une indication des tentatives d'un utilisateur non autorisé d'accéder par « force brute » ou de deviner un mot de passe.
<b>Exigences de L'approche Définie</b> <p><b>10.2.1.5</b> Les journaux d'audit capturent toutes les modifications apportées à l'identification et aux identifiants d'authentification, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• La création de nouveaux comptes.</li> <li>• L'élévation des priviléges.</li> <li>• Toutes les modifications, ajouts ou suppressions de comptes avec accès administrateur.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.2.1.5</b> Examiner les configurations des journaux d'audit et les données des journaux afin de vérifier que les modifications apportées aux informations d'identification et d'authentification sont capturées conformément à tous les éléments spécifiés dans cette exigence.</p>	<b>Objectif</b> La journalisation des modifications apportées aux informations d'authentification (y compris l'élévation des priviléges, les ajouts et les suppressions de comptes avec accès administratif) fournit une preuve résiduelle des activités. Des utilisateurs malveillants peuvent tenter de manipuler les informations d'authentification pour les contourner ou usurper l'identité d'un compte valide.
<b>Objectif de L'approche Personnalisée</b> Les enregistrements de toutes les modifications apportées à l'identification et aux informations d'authentification sont capturés.		

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.2.1.6</b> Les journaux d'audit capturent les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Toutes les initialisations des nouveaux journaux d'audit, et</li> <li>• Tous les démarrages, arrêts ou pauses des journaux d'audit existants.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.2.1.6</b> Examiner les configurations des journaux d'audit et les données de journalisation afin de vérifier que tous les éléments spécifiés dans cette exigence sont capturés.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les enregistrements de toutes les modifications apportées à l'état d'activité des journaux d'audit sont capturés.</p>	<b>Objectif</b> La désactivation ou la suspension des journaux d'audit avant d'effectuer des activités illégales est une pratique courante chez les utilisateurs malveillants qui souhaitent éviter la détection. L'initialisation des journaux d'audit peut indiquer qu'un utilisateur a désactivé la fonction de journalisation pour masquer ses actions.
<b>Exigences de L'approche Définie</b> <p><b>10.2.1.7</b> Les journaux d'audit capturent toutes les créations et suppressions d'objets au niveau du système.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.2.1.7</b> Examiner les configurations des journaux d'audit et les données de journalisation afin de vérifier que la création et la suppression d'objets au niveau du système sont capturées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les enregistrements des modifications qui indiquent qu'un système a été modifié par rapport à sa fonctionnalité prévue sont capturés.</p>	<b>Objectif</b> Les logiciels malveillants, tels que les programmes malveillants, créent ou remplacent souvent des objets au niveau du système sur le système cible afin de contrôler une fonction ou une opération particulière sur ce système. En enregistrant quand des objets au niveau du système sont créés ou supprimés, il sera plus facile de déterminer si de telles modifications ont été autorisées.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.2.2</b> Les journaux d'audit enregistrent les détails suivants pour chaque événement auditabile :</p> <ul style="list-style-type: none"> <li>• Identification de l'utilisateur.</li> <li>• Type d'événement.</li> <li>• Date et heure.</li> <li>• Indication de réussite et d'échec.</li> <li>• Origine de l'événement.</li> <li>• Identité ou nom des données, composant système, ressource ou service touchés (par exemple, nom et protocole).</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.2.2</b> Interroger le personnel et examiner les configurations des journaux d'audit et les données de journalisation afin de vérifier que tous les éléments spécifiés dans cette exigence sont inclus dans les entrées des journaux pour chaque événement auditabile (de 10.2.1.1 à 10.2.1.7).</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des données suffisantes pour pouvoir identifier les tentatives réussies et échouées et qui, quoi, quand, où et comment pour chaque événement répertorié dans l'exigence 10.2.1 sont capturés.</p>	<p><b>Objectif</b></p> <p>En enregistrant ces détails pour les événements auditables de 10.2.1.1 à 10.2.1.7, une compromission potentielle peut être rapidement identifiée, avec suffisamment de détails pour faciliter le suivi des activités suspectes.</p>

Exigences et Procédures de Test		Directives
<b>10.3 Les journaux d'audit sont protégés contre la destruction et les modifications non autorisées.</b>		
<b>Exigences de L'approche Définie</b>  <b>10.3.1</b> L'accès en lecture aux fichiers journaux d'audit est limité aux personnes ayant un besoin lié à leur poste.	<b>Procédures de Test de L'approche Définie</b>  <b>10.3.1</b> Interroger les administrateurs système et examiner les configurations et les priviléges du système afin de vérifier que seules les personnes ayant un besoin lié à leur poste ont un accès en lecture aux fichiers journaux d'audit.	<b>Objectif</b> Les fichiers journaux d'audit contiennent des informations sensibles et l'accès en lecture aux fichiers journaux doit être limité uniquement aux personnes ayant un besoin professionnel valable. Cet accès inclut les fichiers journaux d'audit sur les systèmes d'origine ainsi que partout ailleurs où ils sont stockés.  <b>Bonne Pratique</b> Une protection adéquate des journaux d'audit comprend un contrôle d'accès strict qui limite l'accès aux journaux en fonction du « besoin d'en connaître » uniquement et l'utilisation d'une ségrégation physique ou réseau pour rendre les journaux plus difficiles à trouver et à modifier.
<b>Objectif de L'approche Personnalisée</b>  Les enregistrements d'activité stockés ne sont pas accessibles au personnel non autorisé.		
<b>Exigences de L'approche Définie</b>  <b>10.3.2</b> Les fichiers journaux d'audit sont protégés pour empêcher les modifications par des personnes.	<b>Procédures de Test de L'approche Définie</b>  <b>10.3.2</b> Examiner les configurations et les priviléges du système et interroger les administrateurs système afin de vérifier que les fichiers journaux d'audit actuels sont protégés contre les modifications par des personnes via des mécanismes de contrôle d'accès, une ségrégation physique et/ou une ségrégation réseau.	<b>Objectif</b> Souvent, une personne malveillante qui a pénétré le réseau essaiera de modifier les journaux d'audit pour masquer son activité. Sans une protection adéquate des journaux d'audit, leur complétude, leur exactitude et leur intégrité ne peuvent être garanties, et les journaux d'audit peuvent devenir inutiles en tant qu'outil d'enquête après une compromission. Par conséquent, les journaux d'audit doivent être protégés sur les systèmes d'origine ainsi que partout ailleurs où ils sont stockés.  <b>Bonne Pratique</b> Les entités doivent tenter d'empêcher les journaux d'être exposés dans des emplacements accessibles au public.
<b>Objectif de L'approche Personnalisée</b>  Les enregistrements d'activité stockés ne peuvent pas être modifiés par le personnel.		

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.3.3</b> Les fichiers Journaux d'audit, y compris ceux des technologies exposées en externes, sont rapidement sauvegardés sur un ou des serveurs de journaux internes sécurisés et centraux ou sur d'autres supports difficiles à modifier.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les enregistrements d'activité stockés sont sécurisés et conservés dans un emplacement central pour empêcher toute modification non autorisée.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.3.3</b> Examiner les configurations de sauvegarde ou les fichiers journaux afin de vérifier que les fichiers journaux d'audit actuels, y compris ceux des technologies externes, sont rapidement sauvegardés sur un ou plusieurs serveurs de journaux internes sécurisés ou sur d'autres supports qui sont difficiles à modifier.</p>
<p><b>Exigences de l'approche définie</b></p> <p><b>10.3.4</b> Des mécanismes de surveillance de l'intégrité des fichiers ou de détection des modifications sont utilisés sur les journaux d'audit afin de garantir que les données de journalisation existantes ne peuvent pas être modifiées sans générer d'alertes.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les enregistrements d'activités stockés ne peuvent pas être modifiés sans qu'une alerte ne soit générée.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.3.4</b> Examiner les paramètres système, les fichiers surveillés et les résultats des activités de surveillance afin de vérifier la présence d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications sur les journaux d'audit.</p>

Exigences et Procédures de Test	Directives
<b>10.4 Les journaux d'audit sont examinés pour identifier les anomalies ou les activités suspectes.</b>	
<b>Exigences de L'approche Définie</b> <p><b>10.4.1</b> Les journaux d'audit suivants sont examinés au moins une fois par jour :</p> <ul style="list-style-type: none"> <li>• Tous les événements de sécurité.</li> <li>• Les journaux de tous les composants système qui stockent, traitent ou transmettent des CHD et/ou des SAD.</li> <li>• Les journaux de tous les composants système critiques.</li> <li>• Les journaux de tous les serveurs et composants système qui exécutent des fonctions de sécurité (par exemple, mesures de sécurité réseau, systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), serveurs d'authentification).</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.4.1.a</b> Examiner les politiques et procédures de sécurité afin de vérifier que des processus sont définis pour examiner tous les éléments spécifiés dans cette exigence au moins une fois par jour.</p> <p><b>10.4.1.b</b> Observer les processus et interroger le personnel afin de vérifier que tous les éléments spécifiés dans cette exigence sont examinés au moins une fois par jour</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les activités potentiellement suspectes ou anormales sont rapidement identifiées pour minimiser l'impact.</p>	<b>Objectif</b> <p>De nombreuses violations surviennent des mois avant d'être détectées. Des examens réguliers des journaux signifient que les incidents peuvent être rapidement identifiés et résolus de manière proactive.</p> <p><b>Bonne Pratique</b></p> <p>La vérification quotidienne des journaux (7 jours par semaine, 365 jours par an, jours fériés compris) minimise le temps et l'exposition à une violation potentielle. Les outils de collecte, d'analyse et d'alerte des journaux, les systèmes centralisés de gestion des journaux, les analyseurs d'événements de journaux et les solutions de gestion des informations de sécurité et des événements (SIEM) sont des exemples d'outils automatisés qui peuvent être utilisés pour répondre à la présente exigence.</p> <p>Un examen quotidien des événements de sécurité, par exemple, des notifications ou des alertes qui identifient des activités suspectes ou anormales, ainsi que des journaux des composants système critiques et des journaux des systèmes exécutant des fonctions de sécurité, tels que les pare-feu, IDS/IPS, la surveillance de l'intégrité des fichiers (FIM) systèmes, etc., est nécessaire pour identifier les problèmes potentiels.</p> <p>La détermination d'un « événement de sécurité » variera pour chaque entreprise et peut prendre en compte le type de technologie, l'emplacement et la fonction de l'appareil. Les entreprises peuvent également souhaiter maintenir une base de trafic « normal » pour aider à identifier les comportements anormaux.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Une entité qui utilise des prestataires de services tiers pour effectuer des services d'examen des journaux est chargée de fournir un contexte sur l'environnement de l'entité aux prestataires de services, afin qu'elle comprenne l'environnement de l'entité, dispose d'une base de trafic « normal » pour l'entité et puisse détecter les problèmes de sécurité potentiels et fournir des exceptions précises et des notifications d'anomalies.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.4.1.1</b> Des mécanismes automatisés sont utilisés pour effectuer des examens des journaux d'audit.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les activités potentiellement suspectes ou anormales sont identifiées via un mécanisme reproductible et uniforme.</p> <p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.4.1.1</b> Examiner les mécanismes d'examen des journaux et interroger le personnel afin de vérifier que des mécanismes automatisés sont utilisés pour effectuer des examens de journaux.</p> <p><b>Objectif</b></p> <p>Les examens manuels des journaux sont difficiles à effectuer, même pour un ou deux systèmes, en raison de la quantité de données de journalisation générées. Cependant, l'utilisation d'outils de collecte, d'analyse et d'alerte de journaux, de systèmes centralisés de gestion de journaux, d'analyseurs d'événements de journaux et de solutions de gestion des informations de sécurité et des événements (SIEM) peut aider à faciliter le processus en identifiant les événements de journaux qui doivent être examinés.</p> <p><b>Bonne Pratique</b></p> <p>L'établissement d'une base de référence des modèles d'activité d'audit normaux est essentiel à l'efficacité d'un mécanisme automatisé d'examen des journaux. L'analyse des nouvelles activités d'audit par rapport à la référence établie peut améliorer considérablement l'identification des activités suspectes ou anormales.</p> <p>L'entité doit maintenir les outils de journalisation alignés sur tout changement dans leur environnement en révisant périodiquement les paramètres des outils et en mettant à jour les paramètres pour refléter toute modification.</p> <p><b>Informations complémentaires</b></p> <p>Se reporter au complément d'informations : <i>Surveillance Efficace Quotidienne des Journaux</i> pour plus d'instructions</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.4.2</b> Les journaux de tous les autres composants système (ceux non spécifiés dans l'exigence 10.4.1) sont examinés périodiquement.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.4.2.a</b> Examiner les politiques et procédures de sécurité afin de vérifier que des processus sont définis pour examiner périodiquement les journaux de tous les autres composants système.</p> <p><b>10.4.2.b</b> Examiner les résultats documentés des examens des journaux et interroger le personnel afin de vérifier que les examens des journaux sont effectués périodiquement.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les activités potentiellement suspectes ou anormales pour d'autres composants système (non incluses dans l'exigence 10.4.1) sont examinées conformément au risque identifié de l'entité.</p>	<b>Objectif</b> L'examen périodique des journaux de tous les autres composants système (non spécifiés dans l'exigence 10.4.1) permet d'identifier les indications de problèmes potentiels ou de tentatives d'accès aux systèmes critiques via des systèmes moins critiques.
<b>Notes D'applicabilité</b> <p>Cette exigence s'applique à tous les autres composants système dans le périmètre non inclus dans l'exigence 10.4.1.</p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.4.2.1</b> La fréquence des examens périodiques des journaux pour tous les autres composants système (non définis dans l'exigence 10.4.1) est définie dans l'analyse de risques ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.4.2.1.a</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence des examens périodiques des journaux pour tous les autres composants système (non définis dans l'exigence 10.4.1) afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés à l'exigence 12.3.1.</p> <p><b>10.4.2.1.b</b> Examiner les résultats documentés des examens périodiques des journaux de tous les autres composants système (non définis dans l'exigence 10.4.1) et interroger le personnel afin de vérifier que les examens des journaux sont effectués à la fréquence spécifiée dans l'analyse de risques ciblée de l'entité effectuée pour cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les examens des journaux pour les composants système à faible risque sont effectuées à une fréquence qui tient compte du risque de l'entité.</p>	<b>Objectif</b> Les entités peuvent déterminer la période optimale pour examiner ces journaux en fonction de critères tels que la complexité de l'environnement de chaque entité, le nombre de types de systèmes qui doivent être évalués et les fonctions de ces systèmes.
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.4.3</b> Les exceptions et anomalies identifiées au cours du processus d'examen sont traitées.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.4.3.a</b> Examiner les politiques et procédures de sécurité afin de vérifier que les processus sont définis pour traiter les exceptions et les anomalies identifiées au cours du processus d'examen.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les activités suspectes ou anormales sont traitées.</p>	<p><b>Objectif</b> Si les exceptions et les anomalies identifiées au cours du processus d'examen des journaux ne font pas l'objet d'une enquête, l'entité peut ne pas être au courant des activités non autorisées et potentiellement malveillantes se produisant au sein de son réseau.</p> <p><b>Bonne Pratique</b> Les entités doivent réfléchir à la manière de traiter les éléments suivants lors de l'élaboration de leurs processus de définition et de gestion des exceptions et des anomalies :</p> <ul style="list-style-type: none"> <li>• Comment les activités d'examen des journaux sont enregistrées,</li> <li>• Comment classer et hiérarchiser les exceptions et anomalies,</li> <li>• Quelles procédures devraient être en place pour signaler et faire remonter les exceptions et les anomalies, et</li> <li>• Qui est responsable de l'enquête et de toute tâche de correction.</li> </ul>

Exigences et Procédures de Test	Directives	
<b>10.5 L'historique des journaux d'audit est conservé et disponible pour analyse.</b>		
<b>Exigences de L'approche Définie</b> <p><b>10.5.1</b> Conserver l'historique des journaux d'audit pendant au moins 12 mois, avec au moins les trois mois les plus récents immédiatement disponibles pour analyse.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.5.1.a</b> Examiner la documentation afin de vérifier que les éléments suivants sont définis :</p> <ul style="list-style-type: none"> <li>• Des politiques de conservation des journaux d'audit.</li> <li>• Des procédures de conservation de l'historique du journal d'audit pendant au moins 12 mois, avec au moins les trois mois les plus récents immédiatement disponibles en ligne.</li> </ul> <p><b>10.5.1.b</b> Examiner les configurations de l'historique des journaux d'audit, interroger le personnel et examiner les journaux d'audit afin de vérifier que l'historique des journaux d'audit est conservé pendant au moins 12 mois.</p> <p><b>10.5.1.c</b> Interroger le personnel et observer les processus afin de vérifier qu'au moins l'historique des journaux d'audit des trois derniers mois est immédiatement disponible pour analyse.</p>	<b>Objectif</b> Il est nécessaire de conserver l'historique des journaux d'audit pendant au moins 12 mois, car les compromissions passent souvent inaperçues pendant de longues périodes. Le stockage centralisé de l'historique des journaux permet aux enquêteurs de mieux déterminer la durée pendant laquelle une violation potentielle s'est produite et le ou les systèmes possibles touchés. En disposant de trois mois de journaux immédiatement disponibles, une entité peut rapidement identifier et minimiser l'impact d'une violation des données.
<b>Objectif de L'approche Personnalisée</b> L'historique des enregistrements d'activités sont disponibles immédiatement pour appuyer la réponse aux incidents et sont conservés pendant au moins 12 mois.		<b>Exemples</b> Les méthodes qui permettent aux journaux d'être immédiatement disponibles incluent le stockage des journaux en ligne, l'archivage des journaux ou la restauration rapide des journaux à partir de sauvegardes.

Exigences et Procédures de Test	Directives
<b>10.6 Les mécanismes de synchronisation temporelle prennent en charge des paramètres de temps cohérents sur tous les systèmes.</b>	
<b>Exigences de L'approche Définie</b>	<b>Procédures de Test de L'approche Définie</b>
<b>10.6.1</b> Les horloges système et l'heure sont synchronisées à l'aide de la technologie de synchronisation date/heure.	<b>10.6.1</b> Examiner les paramètres de configuration du système afin de vérifier que la technologie de synchronisation date/heure est mise en œuvre et maintenue à jour.
<b>Objectif de L'approche Personnalisée</b>	La date/heure commune est établie dans tous les systèmes.
<b>Notes D'applicabilité</b>	Le maintien à jour de la technologie de synchronisation date/heure comporte la gestion des vulnérabilités et la mise à jour de la technologie conformément aux exigences 6.3.1 et 6.3.3 du standard PCI DSS.
	<b>Objectif</b> La technologie de synchronisation date/heure est utilisée pour synchroniser les horloges sur plusieurs systèmes. Lorsque les horloges ne sont pas correctement synchronisées, il peut être difficile, voire impossible, de comparer les fichiers journaux de différents systèmes et d'établir une séquence exacte d'événements, ce qui est crucial pour l'analyse criminalistique suite à une violation. Pour les équipes de criminalistique après incident, la précision et la cohérence date/heure sur tous les systèmes et la date/heure de chaque activité sont essentiels pour déterminer comment les systèmes ont été compromis.
	<b>Exemples</b> Le Network Time Protocol (NTP) est un exemple de technologie de synchronisation date/heure.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.6.2</b> Les systèmes sont configurés pour l'heure correcte et cohérente comme suit :</p> <ul style="list-style-type: none"> <li>• Un ou plusieurs serveurs de temps désignés utilisés.</li> <li>• Seul le ou seuls les serveurs de temps centraux désignés reçoit l'heure de sources externes.</li> <li>• L'heure reçue de sources externes est basée sur le temps atomique international ou le temps universel coordonné (UTC).</li> <li>• Le ou les serveurs de temps désignés n'acceptent les mises à jour de la date/heure que de sources externes spécifiques acceptées par l'industrie.</li> <li>• Lorsqu'il y a plus d'un serveur de temps désigné, les serveurs de temps s'échangent les uns avec les autres pour garder l'heure exacte.</li> <li>• Les systèmes internes ne reçoivent des informations de date/heure que du ou des serveurs de temps centraux désignés.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.6.2</b> Examiner les paramètres de configuration du système pour acquérir, distribuer et stocker l'heure correcte afin de vérifier que les paramètres sont configurés conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'heure sur tous les systèmes est précise et uniforme.</p>	<p><b>Objectif</b> L'utilisation de serveurs de temps réputés est un élément essentiel du processus de synchronisation date/heure. L'acceptation des mises à jour de l'heure à partir de sources externes spécifiques et acceptées par l'industrie permet d'empêcher une personne malveillante de modifier les paramètres date/heure sur les systèmes.</p> <p><b>Bonne Pratique</b> Une autre option pour empêcher l'utilisation non autorisée des serveurs de temps internes consiste à chiffrer les mises à jour avec une clé symétrique et à créer des listes de contrôle d'accès qui spécifient les adresses IP des machines clientes qui seront fournies avec les mises à jour de la date/heure.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.6.3</b> Les paramètres et les données de synchronisation date/heure sont protégés comme suit :</p> <ul style="list-style-type: none"> <li>• L'accès aux données date/heure est limité au personnel ayant un besoin professionnel.</li> <li>• Toute modification des paramètres horaires sur les systèmes critiques est enregistrée, surveillée et examinée.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.6.3.a</b> Examiner les configurations système et les paramètres de synchronisation date/heure afin de vérifier que l'accès aux données horaires est limité au personnel ayant un besoin professionnel.</p> <p><b>10.6.3.b</b> Examiner les configurations système et les paramètres et journaux de synchronisation date/heure et observer les processus afin de vérifier que toute modification périphérique aux paramètres horaires sur les systèmes critiques est enregistrée, surveillée et examinée.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les paramètres horaires du système ne peuvent pas être modifiés par du personnel non autorisé.</p>	<b>Objectif</b> Les attaquants tenteront de modifier les configurations de la date/heure pour masquer leur activité. Par conséquent, limiter la possibilité de changer ou de modifier les configurations de synchronisation date/heure ou de l'heure système aux administrateurs réduira la probabilité qu'un attaquant réussisse à modifier les configurations date/heure.

Exigences et Procédures de Test	Directives
10.7 Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement.	
<b>Exigences de L'approche Définie</b> <p><b>10.7.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances des systèmes de mesures de sécurité critiques suivants :</p> <ul style="list-style-type: none"> <li>• Les mesures de sécurité réseau</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Les solutions anti-programmes malveillants</li> <li>• Les mesures d'accès physiques</li> <li>• Les mesures d'accès logiques</li> <li>• Les mécanismes de journalisation des audits</li> <li>• Les mesures de segmentation (le cas échéant)</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.7.1.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner la documentation afin de vérifier que les processus sont définis pour la détection et la résolution rapides des défaillances des systèmes de mesures de sécurité critiques, y compris, sans toutefois s'y limiter, la défaillance de tous les éléments spécifiés dans cette exigence.</p> <p><b>10.7.1.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Observer les processus de détection et d'alerte et interroger le personnel afin de vérifier que les défaillances des systèmes de mesures de sécurité critiques sont détectées et signalées, et que la défaillance d'une mesure de sécurité critique entraîne la génération d'une alerte.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les défaillances des systèmes de mesures de sécurité critiques sont rapidement identifiées et traitées.</p>	<b>Objectif</b> <p>Sans processus formels pour détecter et alerter lorsque les mesures de sécurité de sécurité critiques échouent, les défaillances peuvent passer inaperçues pendant de longues périodes et donner aux attaquants suffisamment de temps pour compromettre les composants système et voler les données de carte du CDE.</p> <p><b>Bonne Pratique</b>  <p>Les types spécifiques de pannes peuvent varier selon la fonction du composant système de l'appareil et de la technologie utilisée. Les défaillances typiques incluent un système cessant d'exécuter sa fonction de sécurité ou ne fonctionnant pas de la manière prévue, tel un pare-feu effaçant toutes ses règles ou se déconnectant.</p> </p>
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Cette exigence sera remplacée par l'exigence 10.7.2 à partir du 31 mars 2025.</p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>10.7.2</b> Les défaillances des systèmes de mesures de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances des systèmes de mesures de sécurité critiques suivants :</p> <ul style="list-style-type: none"> <li>• Les mesures de sécurité réseau</li> <li>• IDS/IPS</li> <li>• Les mécanismes de détection des modifications</li> <li>• Les solutions anti-programmes malveillants</li> <li>• Les mesures d'accès physiques</li> <li>• Les mesures d'accès logiques</li> <li>• Les mécanismes de journalisation des audits</li> <li>• Les mesures de segmentation (le cas échéant)</li> <li>• Les mécanismes d'examen des Journaux d'audit</li> <li>• Des outils automatisés de test de la sécurité (le cas échéant)</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>10.7.2.a</b> Examiner la documentation afin de vérifier que les processus sont définis pour la détection et la résolution rapides des défaillances des systèmes de mesures de sécurité critiques, y compris, sans toutefois s'y limiter, la défaillance de tous les éléments spécifiés dans cette exigence.</p> <p><b>10.7.2.b</b> Observer les processus de détection et d'alerte et interroger le personnel afin de vérifier que les défaillances des systèmes de mesures de sécurité critiques sont détectées et signalées, et que la défaillance d'une mesure de sécurité critique entraîne la génération d'une alerte.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les défaillances des systèmes de mesures de sécurité critiques sont rapidement identifiées et traitées.</p>	<b>Objectif</b> Sans processus formels pour détecter et alerter lorsque les mesures de sécurité de sécurité critiques échouent, les défaillances peuvent passer inaperçues pendant de longues périodes et donner aux attaquants suffisamment de temps pour compromettre les composants système et voler les données de carte du CDE. <b>Bonne Pratique</b> Les types spécifiques de pannes peuvent varier selon la fonction du composant système de l'appareil et de la technologie utilisée. Cependant, les défaillances typiques incluent un système qui n'exécute plus sa fonction de sécurité ou ne fonctionne pas comme prévu, par exemple, un pare-feu effaçant ses règles ou se déconnectant.
<b>Notes D'applicabilité</b> <p><i>Cette exigence s'applique à toutes les entités, y compris les prestataires de services, et remplacera l'exigence 10.7.1 à compter du 31 mars 2025. Elle comprend deux systèmes supplémentaires de mesures de sécurité critiques qui ne figurent pas dans l'exigence 10.7.1.</i></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>10.7.3</b> Les défaillances de tout système de mesures de sécurité critique sont traitées rapidement, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Restauration des fonctions de sécurité.</li> <li>• Identifier et documenter la durée (date et heure du début à la fin) de la défaillance de sécurité.</li> <li>• Identifier et documenter la ou les causes de la défaillance et documenter les mesures correctives nécessaires.</li> <li>• Identifier et résoudre tous les problèmes de sécurité survenus lors de la défaillance.</li> <li>• Déterminer si d'autres mesures sont nécessaires à la suite de la défaillance de sécurité.</li> <li>• Mettre en œuvre des mesures afin d'éviter que la cause de la défaillance ne se reproduise.</li> <li>• Reprendre la surveillance des mesures de sécurité.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>10.7.3.a</b> Examiner la documentation et interroger le personnel afin de vérifier que les processus sont définis et mis en œuvre pour répondre à une défaillance de tout système de mesures de sécurité critique, et incluent au moins tous les éléments spécifiés dans cette exigence.</p> <p><b>10.7.3.b</b> Examiner les enregistrements afin de vérifier que les défaillances des systèmes de mesures de sécurité critiques sont documentées pour inclure :</p> <ul style="list-style-type: none"> <li>• L'identification de la ou des causes de la défaillance.</li> <li>• La durée (date et heure de début et de fin) de la défaillance de sécurité.</li> <li>• Les détails des correctifs nécessaires pour traiter la cause profonde.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les défaillances des systèmes de mesures de sécurité critiques sont analysées, contenues et résolues, et les mesures de sécurité de sécurité sont restaurées pour minimiser l'impact. Les problèmes de sécurité qui en résultent sont traités et des mesures sont prises afin d'éviter qu'elles ne se reproduisent.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>Si les alertes de défaillances des systèmes de mesures de sécurité critiques ne sont pas traitées rapidement et efficacement, les attaquants peuvent utiliser ce temps pour insérer des logiciels malveillants, prendre le contrôle d'un système ou voler des données dans l'environnement de l'entité.</p> <p><b>Bonne Pratique</b></p> <p>Des preuves documentées (par exemple, des enregistrements au sein d'un système de gestion des problèmes) doivent fournir un justificatif indiquant que des processus et des procédures sont en place pour répondre aux défaillances de sécurité. De plus, le personnel doit être conscient de ses responsabilités en cas de défaillance. Les actions et les réponses à l'échec doivent être consignées dans les preuves documentées.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique uniquement lorsque l'entité évaluée est un prestataire de services, jusqu'au 31 Mars 2025, après quoi cette exigence s'appliquera à toutes les entités.</p> <p><i>Il s'agit d'une exigence actuelle v3.2.1 qui s'applique uniquement aux prestataires de services. Cependant, cette exigence est une Bonne Pratique pour toutes les autres entités jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	

## **Exigence 11 : Tester Régulièrement la Sécurité des Systèmes et des Réseaux**

### **Sections**

- 11.1** Les processus et mécanismes pour tester régulièrement la sécurité des systèmes et des réseaux sont définis et compris.
- 11.2** Les points d'accès sans fil sont identifiés et surveillés, et les points d'accès sans fil non autorisés sont traités.
- 11.3** Les vulnérabilités externes et internes sont régulièrement identifiées, priorisées et traitées.
- 11.4** Des tests d'intrusion externes et internes sont effectués régulièrement, les vulnérabilités exploitables et les faiblesses de sécurité sont corrigées.
- 11.5** Les intrusions réseau et les modifications imprévues de fichiers sont détectées et traitées.
- 11.6** Les modifications non autorisées sur les pages de paiement sont détectées et traitées.

### **Aperçu**

Des vulnérabilités sont découvertes en permanence par des individus malveillants et des chercheurs, et aussi introduites par de nouveaux logiciels. Les composants système, les processus et les logiciels faits sur mesure et personnalisés doivent être testés fréquemment afin de garantir que les mesures de sécurité de sécurité continuent de refléter un environnement en évolution.

Se reporter à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test		Directives
<b>11.1 Les processus et mécanismes pour tester régulièrement la sécurité des systèmes et des réseaux sont définis et compris.</b>		
<b>Exigences de L'approche Définie</b> <p><b>11.1.1</b> Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 11 sont :</p> <ul style="list-style-type: none"> <li>• Documentées.</li> <li>• Tenues à jour.</li> <li>• Utilisées.</li> <li>• Connues de toutes les parties concernées.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>11.1.1</b> Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles sont gérées conformément à tous les éléments spécifiés dans cette exigence.</p>	<b>Objectif</b> <p>L'exigence 11.1.1 concerne la gestion et le maintien efficaces des diverses politiques et procédures spécifiées dans toute l'exigence 11. S'il est important de définir les politiques ou procédures spécifiques décrites dans l'exigence 11, il est tout aussi important de s'assurer qu'elles sont correctement documentées, maintenues et diffusées.</p> <p><b>Bonne Pratique</b></p> <p>Il est important de mettre à jour les politiques et les procédures au besoin pour faire face aux changements dans les processus, les technologies et les objectifs métier. Pour cette raison, envisager de mettre à jour ces documents, non seulement, de manière périodique mais aussi dès que possible après un changement.</p> <p><b>Définitions</b></p> <p>Les politiques de sécurité définissent les objectifs et les principes de sécurité de l'entité. Les procédures opérationnelles décrivent la façon d'exécuter les activités et définissent les mesures de sécurité, les méthodes et les processus qui sont suivis pour atteindre le résultat désiré de manière cohérente et conformément aux objectifs de la politique.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les attentes, les mesures de sécurité et la surveillance des activités pour répondre à l'exigence 11 sont définis et respectés par le personnel concerné. Toutes les activités de soutien sont reproductibles, appliquées de manière cohérente et conformes à l'intention de la direction.</p>		

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>11.1.2</b> Les rôles et les responsabilités liées aux activités de l'exigence 11 sont documentés, attribués et compris.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>11.1.2.a</b> Examiner la documentation pour vérifier que la description des rôles et des responsabilités pour l'exécution des activités de l'exigence 11 sont documentées et attribuées.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les responsabilités quotidiennes pour l'exécution de toutes les activités de l'exigence 11 sont attribuées. Le personnel est responsable du bon fonctionnement continu ces exigences.</p>	<p><b>Objectif</b> Si les rôles et les responsabilités ne sont pas officiellement attribués, le personnel pourrait ne pas être conscient de ses responsabilités quotidiennes et des activités critiques peuvent ne pas avoir lieu.</p> <p><b>Bonne Pratique</b> Les rôles et les responsabilités peuvent être documentés dans des politiques et procédures, ou conservés dans des documents séparés. Dans le cadre de la communication des rôles et des responsabilités, les entités peuvent envisager de demander au personnel de reconnaître leur acceptation et leur compréhension des rôles et responsabilités qui leur sont attribués.</p> <p><b>Exemples</b> Une méthode pour documenter les rôles et les obligations est une matrice d'attribution des responsabilités qui indique qui est responsable, redevable, consulté et informé (également appelée matrice RACI).</p>

Exigences et Procédures de Test	Directives
<b>11.2 Les points d'accès sans fil sont identifiés et surveillés, et les points d'accès sans fil non autorisés sont traités.</b>	
<b>Exigences de L'approche Définie</b> <p><b>11.2.1</b> Les points d'accès sans fil autorisés et non autorisés sont gérés de la manière suivante :</p> <ul style="list-style-type: none"> <li>La présence de points d'accès sans fil (Wi-Fi) est testée,</li> <li>Tous les points d'accès sans fil autorisés et non autorisés sont détectés et identifiés,</li> <li>Les tests, la détection et l'identification sont effectués au moins une fois tous les trois mois.</li> <li>Si une surveillance automatisée est utilisée, le personnel doit être averti via la génération d'alertes.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>11.2.1.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour gérer les points d'accès sans fil autorisés et non autorisés avec tous les éléments spécifiés dans cette exigence.</p> <p><b>11.2.1.b</b> Examiner la ou les méthodologies utilisées et la documentation qui en découle, et interroger le personnel afin de vérifier que les processus sont définis pour détecter et identifier les points d'accès sans fil autorisés et non autorisés conformément à tous les éléments spécifiés dans la cette exigence.</p> <p><b>11.2.1.c</b> Examiner le résultat des évaluations du réseau sans fil et interroger le personnel afin de vérifier que les évaluations du réseau sans fil ont été menées conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>11.2.1.d</b> Si la surveillance automatisée est utilisée, examiner les paramètres de configuration afin de vérifier que la configuration générera des alertes pour aviser le personnel.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les points d'accès sans fil non autorisés sont identifiés et traités périodiquement.</p>	<b>Objectif</b> <p>La mise en œuvre et/ou l'exploitation de la technologie sans fil au sein d'un réseau sont des voies habituelles permettant aux utilisateurs malveillants d'accéder sans autorisation au réseau et aux données des titulaires de cartes. Des dispositifs sans fil non autorisés peuvent être masqués ou connectés à un ordinateur ou à un autre composant système. Ces appareils peuvent également être connectés directement à un port réseau, à un périphérique réseau tel qu'un commutateur ou un routeur, ou insérés en tant que carte d'interface sans fil au sein d'un composant système.</p> <p>Même si une entreprise a une politique interdisant l'utilisation de technologies sans fil, un appareil ou un réseau sans fil non autorisé pourrait être installé à l'insu de l'entreprise, permettant à un attaquant d'accéder au réseau aisément et « de manière invisible ». La détection et l'élimination de ces points d'accès non autorisés réduisent la durée et la probabilité que ces périphériques soient exploités en vue d'une attaque.</p> <p><b>Bonne Pratique</b></p> <p>La taille et la complexité d'un environnement dicteront les outils et processus appropriés à utiliser afin de fournir une garantie suffisante qu'un point d'accès sans fil malveillant n'a pas été installé dans l'environnement.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>L'exigence s'applique même lorsqu'il existe une politique interdisant l'utilisation de la technologie sans fil.</p> <p>Les méthodes utilisées pour satisfaire à cette exigence doivent être suffisantes pour détecter et identifier à la fois les appareils autorisés et non autorisés, y compris les appareils non autorisés qui se connectent à des appareils eux-mêmes autorisés.</p>	<p>Par exemple, l'exécution d'une inspection physique détaillée d'un seul kiosque de vente au détail autonome dans un centre commercial, dans lequel tous les composants de communication sont contenus dans des boîtiers inviolables, peut être suffisante pour garantir qu'un point d'accès sans fil malveillant n'a pas été raccordé ou installé.</p> <p>Cependant, dans un environnement avec plusieurs points d'accès (tel que dans un grand magasin de détail, un centre d'appels, une salle de serveurs ou un centre de données), une inspection physique détaillée peut s'avérer difficile. Dans ce cas, plusieurs méthodes peuvent être combinées, telles que la réalisation d'inspections physiques du système en conjonction avec les résultats d'un analyseur de réseau sans fil.</p> <p><b>Définitions</b></p> <p>Ceci est également appelé détection des points d'accès non autorisés.</p> <p><b>Exemples</b></p> <p>Les méthodes pouvant être utilisées incluent, sans toutefois s'y limiter, les analyses de réseau sans fil, les inspections physiques/logiques des composants et de l'infrastructure du système, le contrôle d'accès au réseau (NAC) ou le système IDS/IPS pour réseau sans fil. Les systèmes NAC et IDS/IPS sans fil sont des exemples d'outils de surveillance automatisés.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.2.2</b> Un inventaire des points d'accès sans fil autorisés est conservé, y compris une justification métier documentée.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les points d'accès sans fil non autorisés ne sont pas confondus avec les points d'accès sans fil autorisés.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.2.2</b> Examiner la documentation afin de vérifier qu'un inventaire des points d'accès sans fil autorisés est maintenu et qu'une justification métier est documentée pour tous les points d'accès sans fil autorisés.</p>

Exigences et Procédures de Test	Directives
<b>11.3 Les vulnérabilités externes et internes sont régulièrement identifiées, priorisées et traitées.</b>	
<b>Exigences de L'approche Définie</b> <p><b>11.3.1</b> Les scans de vulnérabilités internes sont effectuées comme suit :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les trois mois.</li> <li>• Les vulnérabilités qui sont soit à haut risque soit critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues.</li> <li>• Des rescans sont effectués pour confirmer que toutes les vulnérabilités à haut risque et critiques, comme indiqué ci-dessus, ont été résolues.</li> <li>• L'outil de scan est tenu à jour avec les dernières informations sur les vulnérabilités.</li> <li>• Les scans sont effectués par du personnel qualifié et l'indépendance organisationnelle du testeur existe.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>11.3.1.a</b> Examiner le résultat des rapports de scans internes des 12 derniers mois afin de vérifier que les scans internes ont eu lieu au moins une fois tous les trois mois au cours de la période de 12 mois la plus récente.</p> <p><b>11.3.1.b</b> Examiner les résultats du rapport de scans internes de chaque scan et scan de vérification exécutés au cours des 12 derniers mois afin de vérifier que les vulnérabilités à haut risque et toutes les vulnérabilités critiques (définies dans l'exigence 6.3.1 du standard PCI DSS) sont résolues.</p> <p><b>11.3.1.c</b> Examiner les configurations de l'outil de scan et interroger le personnel afin de vérifier que l'outil d'analyse est tenu à jour avec les dernières définitions des vulnérabilités.</p> <p><b>11.3.1.d</b> Interroger le personnel responsable afin de vérifier que le scan a été effectué par une ou plusieurs ressources internes qualifiées ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe.</p>
<b>Objectif de L'approche Personnalisée</b> <p>La posture de sécurité de tous les composants système est vérifiée périodiquement à l'aide d'outils automatisés conçus pour détecter les vulnérabilités opérant à l'intérieur du réseau. Les vulnérabilités détectées sont évaluées et rectifiées sur la base d'un cadre formel d'évaluation des risques.</p>	<b>Objectif</b> L'identification et la résolution des vulnérabilités réduisent rapidement la probabilité qu'une vulnérabilité soit exploitée et la compromission potentielle d'un composant système ou des données des titulaires de cartes. Des scans de vulnérabilité menées au moins tous les trois mois permettent cette détection et cette identification. <b>Bonne Pratique</b> Les vulnérabilités posant le plus grand risque pour l'environnement (par exemple, classées élevées ou critiques conformément à l'exigence 6.3.1) doivent être résolues avec la plus haute priorité. Les vulnérabilités identifiées lors des analyses de vulnérabilité internes doivent faire partie d'un processus de gestion des vulnérabilités qui inclut plusieurs sources de vulnérabilité, comme spécifié dans l'exigence 6.3.1. Plusieurs rapports de scans peuvent être combinés pour le processus de test trimestriel afin de montrer que tous les systèmes ont été scannés et que toutes les vulnérabilités applicables ont été corrigées dans le cadre du cycle trimestriel d'analyse des vulnérabilités. Cependant, une documentation supplémentaire peut être requise afin de vérifier que les vulnérabilités non corrigées sont en cours de résolution. Bien que des scans soient obligatoires au moins une fois tous les trois mois, des scans plus fréquents sont recommandés en fonction de la complexité du réseau, de la fréquence des modifications et des types d'appareils, de logiciels et de systèmes d'exploitation utilisés. <i>(suite à la page suivante)</i>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Il n'est pas demandé d'utiliser un QSA ou un ASV pour effectuer des scans de vulnérabilité internes. Les scans de vulnérabilités internes peuvent être effectués par du personnel interne qualifié qui est raisonnablement indépendant du ou des composants système analysés (par exemple, un administrateur réseau ne devrait pas être responsable des scans du réseau), ou une entité peut choisir d'avoir des analyses de vulnérabilités internes effectuées par une société spécialisée dans le scan des vulnérabilités.</p>	<p><b>Définitions</b></p> <p>Un scan des vulnérabilités est une combinaison d'outils, de techniques et/ou de méthodes automatisés exécutés sur des périphériques et des serveurs externes et internes, conçue pour exposer les vulnérabilités potentielles dans les applications, les systèmes d'exploitation et les périphériques réseau qui pourraient être trouvés et exploités par des personnes malveillantes.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.3.1.1</b> Toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme vulnérabilités à haut risque ou vulnérabilités critiques (conformément aux classements de risque de vulnérabilité de l'entité définis à l'exigence 6.3.1) sont gérées comme suit :</p> <ul style="list-style-type: none"> <li>• Traitées sur la base du risque défini dans l'analyse de risque ciblée de l'entité, qui est effectuée selon tous les éléments spécifiés dans l'exigence 12.3.1.</li> <li>• Des scans de vérification sont effectués si besoin.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.3.1.1.a</b> Examiner l'analyse de risque ciblée de l'entité qui définit le risque pour traiter toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme vulnérabilités à haut risque ou vulnérabilités critiques selon les classements du risque des vulnérabilités de l'entité à l'exigence 6.3.1) afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés à l'exigence 12.3.1.</p> <p><b>11.3.1.1.b</b> Interroger le personnel responsable et examiner les résultats du rapport de scan interne ou d'autres documents afin de vérifier que toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme vulnérabilités à haut risque ou vulnérabilités critiques selon le classement du risque des vulnérabilités de l'entité à l'exigence 6.3.1) sont traitées en fonction du risque défini dans l'analyse de risque ciblée de l'entité, et que le processus de scan comprend des scans de vérification si besoin pour confirmer que les vulnérabilités ont été corrigées.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les vulnérabilités classées plus faibles (risque inférieur à éléver ou critique) sont traitées à une fréquence conforme au risque de l'entité.</p>	
<p><b>Notes D'applicabilité</b></p> <p>Le délai pour traiter les vulnérabilités à faible risque est soumis aux résultats d'une analyse de risques conformément à l'exigence 12.3.1 qui comprend (au minimum) l'identification des actifs protégés, des menaces et de la probabilité qu'une menace soit réalisée et/ou de son impact si elle est réalisée.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.3.1.2</b> Les scans de vulnérabilité internes sont effectués via un scan authentifié comme suit :</p> <ul style="list-style-type: none"> <li>• Les systèmes qui ne peuvent pas accepter les « credentials » pour le scan authentifié sont documentés.</li> <li>• Des privilèges suffisants sont utilisés pour les systèmes qui acceptent les « credentials » pour le scan.</li> <li>• Si les comptes utilisés pour le scan authentifié peuvent être utilisés pour la connexion interactive, ils sont gérés conformément à l'exigence 8.2.2.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.3.1.2.a</b> Examiner les configurations de l'outil de scan afin de vérifier que le scan authentifié est utilisé pour les scans internes, avec des privilèges suffisants, pour les systèmes qui acceptent les informations d'identification pour le scan.</p> <p><b>11.3.1.2.b</b> Examiner les résultats du rapport de scan et interroger le personnel afin de vérifier que les scans authentifiés sont effectués.</p> <p><b>11.3.1.2.c</b> Si les comptes utilisés pour le scan authentifié peuvent être utilisés pour une connexion interactive, examiner les comptes et interroger le personnel afin de vérifier que les comptes sont gérés conformément à tous les éléments spécifiés dans l'exigence 8.2.2.</p> <p><b>11.3.1.2.d</b> Examiner la documentation afin de vérifier que les systèmes qui ne sont pas en mesure d'accepter les « credentials » pour le scan authentifié sont définis.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les outils automatisés utilisés pour détecter les vulnérabilités peuvent détecter les vulnérabilités locales à chaque système, qui ne sont pas visibles à distance.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>Le scan authentifié fournit un meilleur aperçu du paysage des vulnérabilités d'une entité, car il peut détecter des vulnérabilités que les scans non authentifiés ne peuvent pas détecter. Les attaques peuvent exploiter des vulnérabilités dont une entité n'a pas connaissance, car certaines vulnérabilités ne seront détectées qu'avec un scan authentifié.</p> <p>Le scan authentifié peut fournir d'autres informations importantes sur les vulnérabilités d'une entreprise.</p> <p><b>Bonne Pratique</b></p> <p>Les informations d'identification utilisées pour ces scans doivent être considérées comme hautement sensibles. Elles doivent être protégées et contrôlées en tant que telles, conformément aux exigences 7 et 8 du standard PCI DSS (à l'exception des exigences relatives à l'authentification à plusieurs facteurs et aux comptes d'applications et système).</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Les outils de scan authentifiés peuvent être basés sur l'hôte ou sur le réseau.</p> <p>Les privilèges « suffisants » sont ceux qui sont nécessaires pour accéder aux ressources système afin qu'un scan approfondi puisse être effectué pour détecter les vulnérabilités connues.</p> <p>Cette exigence ne s'applique pas aux composants système qui ne peuvent pas accepter les informations d'identification pour le scan. Des exemples de systèmes qui peuvent ne pas accepter les informations d'identification pour le scan comportent certains appareils réseau et de sécurité, les serveurs principaux et les conteneurs.</p> <p>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.3.1.3</b> Les scans de vulnérabilités internes sont effectués après toute modification importante comme suit :</p> <ul style="list-style-type: none"> <li>• Les vulnérabilités qui sont soit à haut risque, soit critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues.</li> <li>• Des scans de vérification sont effectués au besoin.</li> <li>• Les scans sont effectués par du personnel qualifié et l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.3.1.3.a</b> Examiner la documentation de contrôle des modifications et les rapports de scans internes afin de vérifier que les composants système ont été analysés après toute modification importante.</p> <p><b>11.3.1.3.b</b> Interroger le personnel et examiner les rapports de scans et de scans de vérification internes afin de vérifier que les analyses internes ont été effectuées après des modifications importantes et que toutes les vulnérabilités à haut risque et toutes les vulnérabilités critiques (définies dans l'exigence PCI DSS 6.3.1) ont été résolues.</p> <p><b>11.3.1.3.c</b> Interroger le personnel afin de vérifier que les scans internes sont effectués par une ou des ressources internes qualifiées ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>La posture de sécurité de tous les composants système est vérifiée à la suite de modifications importantes apportées au réseau ou aux systèmes, à l'aide d'outils automatisés conçus pour détecter les vulnérabilités opérant à l'intérieur du réseau. Les vulnérabilités détectées sont évaluées et corrigées sur la base d'un cadre formel d'évaluation des risques.</p>	
<p><b>Notes D'applicabilité</b></p> <p>Le scan de vulnérabilités internes authentifiés conformément à l'exigence 11.3.1.2 n'est pas nécessaire pour les analyses effectuées après des modifications importantes.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.3.2</b> Les scans de vulnérabilités externes sont effectués comme suit :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les trois mois.</li> <li>• Par un fournisseur de scan de vulnérabilités agréé PCI SSC (ASV).</li> <li>• Les vulnérabilités sont résolues et les exigences du guide du programme de l'ASV pour un scan réussi sont respectées.</li> <li>• Des scans de vérification sont effectués si besoin pour confirmer que les vulnérabilités sont résolues conformément aux exigences du guide du programme de l'ASV pour un scan réussi.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.3.2.a</b> Examiner les rapports de scans de l'ASV des 12 derniers mois afin de vérifier que les scans de vulnérabilité externes ont eu lieu au moins une fois tous les trois mois au cours de la période de 12 mois la plus récente.</p> <p><b>11.3.2.b</b> Examiner le rapport de scans de l'ASV de chaque scan et scans de vérification exécutés au cours des 12 derniers mois afin de vérifier que les vulnérabilités sont résolues et que les exigences du guide du programme de l'ASV pour un scan réussi sont respectées.</p> <p><b>11.3.2.c</b> Examiner les rapports de scans de l'ASV afin de vérifier que les scans ont été effectués par un fournisseur de scans de vulnérabilité agréé PCI SSC (ASV).</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'approche personnalisée n'est pas applicable à cette exigence</p>	<p><b>Objectif</b> Les attaquants recherchent régulièrement des serveurs externes non « patchés » ou vulnérables, qui peuvent être exploités pour lancer une attaque dirigée. Les entreprises doivent s'assurer que ces appareils externes sont régulièrement scans afin de détecter les faiblesses et que les vulnérabilités soient corrigées ou résolues pour protéger l'entité.</p> <p>Étant donné que les réseaux externes courent un plus grand risque de compromission, les scans de vulnérabilités externes doivent être effectués au moins une fois tous les trois mois par un fournisseur de scan de vulnérabilités agréé PCI SSC (ASV).</p> <p><b>Bonne Pratique</b> Bien que des scans soient requis au moins une fois tous les trois mois, des scans plus fréquents sont recommandés en fonction de la complexité du réseau, de la fréquence des modifications et des types d'appareils, de logiciels et de systèmes d'exploitation utilisés.</p>
<p><b>Notes D'applicabilité</b></p> <p>Pour l'évaluation initiale au standard PCI DSS pour cette exigence, il n'est pas nécessaire que quatre scans réussis soient effectués dans les 12 mois si l'auditeur vérifie que : 1) le résultat du scan le plus récent était un scan réussi, 2) l'entité a des politiques et des procédures documentées exigeant un scan au moins une fois tous les trois mois, et 3) les vulnérabilités trouvées dans les résultats du scan ont été corrigées comme indiqué dans une ou plusieurs nouvelles analyses.</p> <p>(suite à la page suivante)</p>	<p>Les vulnérabilités identifiées lors des analyses de vulnérabilité externes doivent faire partie d'un processus de gestion des vulnérabilités qui inclut plusieurs sources de vulnérabilité, comme spécifié dans l'exigence 6.3.1.</p> <p>Plusieurs rapports de scans peuvent être combinés pour montrer que tous les systèmes ont été analysés et que toutes les vulnérabilités applicables ont été résolues dans le cadre du cycle trimestriel de scans des vulnérabilités. Cependant, une documentation supplémentaire peut être requise afin de vérifier que les vulnérabilités non corrigées sont en cours de résolution.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p>Cependant, pour les années suivantes après l'évaluation initiale du standard PCI DSS, des scans réussis au moins tous les trois mois doivent avoir eu lieu.</p> <p>Les outils de scan de l'ASV peuvent scanner une vaste gamme de types de réseaux et de topologies. Tous les détails concernant l'environnement cible (par exemple, les équilibriseurs de charge, les fournisseurs tiers, les Fournisseurs d'Accès Internet, les configurations spécifiques, les protocoles utilisés, les interférences d'analyse) doivent être réglés entre l'ASV et l'entité.</p> <p>Se référer au <i>guide du programme de l'ASV</i> publié sur le site Web du PCI SSC afin de connaître les responsabilités du consommateur de l'analyse, la préparation de l'analyse, etc.</p>	<p><b>Informations complémentaires</b> Consulter le <i>Guide du programme ASV</i> sur le site Web du PCI SSC</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.3.2.1</b> Les scans de vulnérabilités externes sont effectués après toute modification importante comme suit :</p> <ul style="list-style-type: none"> <li>• Les vulnérabilités trouvées avec un CVSS égal à 4.0 ou plus sont résolues.</li> <li>• Des scans de vérification sont effectués si besoin.</li> <li>• Les scans sont effectués par du personnel qualifié et l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.3.2.1.a</b> Examiner la documentation de contrôle des changements et les rapports de scans externes afin de vérifier que les composants système ont été analysés après toute modification importante.</p> <p><b>11.3.2.1.b</b> Interroger le personnel et examiner les rapports de scans et de rescans externes afin de vérifier que les scans externes ont été effectués après des modifications importantes et que les vulnérabilités trouvées avec un CVSS égal à 4.0 ou plus ont été résolues.</p> <p><b>11.3.2.1.c</b> Interroger le personnel afin de vérifier que les scans externes sont effectués par une ou des ressources internes qualifiée(s) ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>La posture de sécurité de tous les composants système est vérifiée à la suite de modifications importantes du réseau ou des systèmes, à l'aide d'outils conçus pour détecter les vulnérabilités opérant depuis l'extérieur du réseau. Les vulnérabilités détectées sont évaluées et rectifiées sur la base d'un cadre formel d'évaluation des risques.</p>	<p><b>Objectif</b> Le scan de vulnérabilités d'un environnement après toute modification importante garantit que les modifications ont été effectuées de manière appropriée, de sorte que la sécurité de l'environnement n'a pas été compromise en raison de la modification.</p> <p><b>Bonne Pratique</b> Les entités doivent inclure la nécessité d'effectuer des scans de vulnérabilités après des modifications importantes dans le cadre du processus de modification et avant que la modification ne soit considérée comme terminée. Tous les composants systèmes touchés par la modification devront être analysés.</p>

Exigences et Procédures de Test	Directives
<b>11.4 Des tests d'intrusion externes et internes sont effectués régulièrement, et les vulnérabilités exploitables et les faiblesses de sécurité sont corrigées.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.1</b> Une méthodologie de test d'intrusion est définie, documentée et mise en œuvre par l'entité, et comprend :</p> <ul style="list-style-type: none"> <li>• Des approches de test d'intrusion acceptées par l'industrie.</li> <li>• Une couverture de l'ensemble du périmètre du CDE et des systèmes critiques.</li> <li>• Des tests à la fois à l'intérieur et à l'extérieur du réseau.</li> <li>• Des tests pour valider les mesures de segmentation et de réduction du périmètre.</li> <li>• Des tests d'intrusion de la couche application pour identifier, au minimum, les vulnérabilités répertoriées dans l'exigence 6.2.4.</li> <li>• Des tests d'intrusion de la couche réseau qui englobent tous les composants prenant en charge les fonctions réseau ainsi que les systèmes d'exploitation.</li> <li>• L'examen et la prise en compte des menaces et des vulnérabilités rencontrées au cours des 12 derniers mois.</li> <li>• Une approche documentée pour évaluer et traiter le risque posé par les vulnérabilités exploitables et les faiblesses de sécurité détectées lors des tests d'intrusion.</li> <li>• La conservation des résultats des tests d'intrusion et des activités de correction pendant au moins 12 mois.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.1</b> Examiner la documentation et interroger le personnel afin de vérifier que la méthodologie des tests d'intrusion définie, documentée et mise en œuvre par l'entité comprend tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>Les attaquants passent beaucoup de temps à rechercher des vulnérabilités externes et internes à exploiter pour accéder aux données des titulaires de cartes, pour ensuite exfiltrer ces données. En tant que telles, les entités doivent tester leurs réseaux de manière approfondie, tout comme le ferait un attaquant. Ce test permet à l'entité d'identifier et de corriger les faiblesses qui pourraient être exploitées pour compromettre le réseau et les données de l'entité, puis de prendre les mesures appropriées pour protéger le réseau et les composants système contre de telles attaques.</p> <p><b>Bonne Pratique</b></p> <p>Les techniques de test d'intrusion différeront en fonction des besoins et de la structure d'une entreprise et devraient être adaptées à l'environnement testé. Par exemple, les tests à données aléatoires (fuzzing), d'injection et falsification de données peuvent être appropriés. Le type, la profondeur et la complexité des tests dépendront de l'environnement spécifique et des besoins de l'entreprise.</p> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Une méthodologie formelle est définie pour des tests techniques approfondis qui tentent d'exploiter les vulnérabilités et les faiblesses de sécurité via des méthodes d'attaque simulées par un attaquant manuel compétent.</p> <p><b>Notes D'applicabilité</b></p> <p>Les tests à l'intérieur du réseau (ou « tests d'intrusion internes ») signifient des tests à la fois à l'intérieur du CDE et vers le CDE à partir de réseaux internes fiables et non fiables.</p> <p>Les tests depuis l'extérieur du réseau (ou test de pénétration « externe ») signifie tester le périmètre externe exposé des réseaux de confiance et des systèmes critiques connectés ou accessibles aux infrastructures de réseau public.</p>	<p><b>Définitions</b></p> <p>Les tests d'intrusion simulent une situation d'attaque réelle dans le but d'identifier jusqu'où un attaquant pourrait s'introduire dans un environnement, en fonction des différentes quantités d'informations fournies au testeur. Cela permet à une entité de mieux comprendre son exposition potentielle et de développer une stratégie pour se défendre contre les attaques. Un test d'intrusion diffère d'une analyse de vulnérabilité, car un test d'intrusion est un processus actif qui inclut généralement l'exploitation des vulnérabilités identifiées. Le scan de vulnérabilités seul n'est pas un test d'intrusion, et un test d'intrusion n'est pas non plus adéquat si l'objectif est uniquement d'essayer d'exploiter les vulnérabilités trouvées dans une analyse de vulnérabilité. La réalisation d'une analyse de vulnérabilité peut être l'une des premières étapes, mais ce n'est pas la seule étape qu'un testeur d'intrusion effectuera pour planifier la stratégie de test. Même si une analyse de vulnérabilités ne détecte pas les vulnérabilités connues, le testeur d'intrusion obtiendra souvent suffisamment de connaissances sur le système pour identifier d'éventuelles failles de sécurité.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Les tests d'intrusion sont un processus hautement manuel. Bien que certains outils automatisés puissent être utilisés, le testeur utilise sa connaissance des systèmes pour accéder à un environnement. Souvent, le testeur enchaîne plusieurs types d'exploitations dans le but de percer les couches de défenses. Par exemple, si le testeur trouve un moyen d'accéder à un serveur d'applications, le testeur utilisera alors le serveur compromis comme point pour lancer une nouvelle attaque basée sur les ressources auxquelles le serveur a accès. De cette façon, un testeur peut simuler les techniques utilisées par un attaquant pour identifier les zones de faiblesse potentielles dans l'environnement. Le test des méthodes de surveillance et de détection de la sécurité, par exemple pour confirmer l'efficacité des mécanismes de journalisation et de surveillance de l'intégrité des fichiers, doit également être envisagé.</p> <p><b>Informations Complémentaires</b></p> <p>Se référer au <i>Complément d'informations : Information Supplement: Penetration Testing Guidance</i> pour des conseils supplémentaires.</p> <p>Des approches de test d'intrusion acceptées par l'industrie comportent :</p> <p><i>The Open Source Security Testing Methodology and Manual (OSSTMM)</i></p> <p><i>Open Web Application Security Project (OWASP) penetration testing programs.</i></p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.2</b> Un test d'intrusion interne est effectué :</p> <ul style="list-style-type: none"> <li>• Selon la méthodologie définie par l'entité,</li> <li>• Au moins une fois tous les 12 mois.</li> <li>• Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application</li> <li>• Par une ressource interne qualifiée ou un tiers externe qualifié</li> <li>• L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les défenses internes du système sont vérifiées par des tests techniques conformément à la méthodologie définie par l'entité aussi souvent que nécessaire afin de faire face aux attaques et menaces nouvelles et évolutives, et de garantir que des modifications importantes n'introduisent pas de vulnérabilités inconnues.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.2.a</b> Examiner la périmètre des travaux et les résultats du test d'intrusion interne le plus récent afin de vérifier que les tests d'intrusion sont effectués conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>11.4.2.b</b> Interroger le personnel afin de vérifier que le test d'intrusion interne a été effectué par une ressource interne qualifiée ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</p> <p><b>Objectif</b></p> <p>Les tests d'intrusion internes ont deux objectifs. D'abord, tout comme un test d'intrusion externe, il découvre des vulnérabilités et des erreurs de configuration qui pourraient être utilisées par un attaquant qui a réussi à obtenir un certain degré d'accès au réseau interne, que ce soit parce que l'attaquant est un utilisateur autorisé menant des activités non autorisées, ou un attaquant externe qui avait réussi à pénétrer dans le périmètre de l'entité.</p> <p>Deuxièmement, les tests d'intrusion internes aident également les entités à découvrir où leur processus de contrôle des modifications a échoué en détectant des systèmes auparavant inconnus. De plus, il vérifie l'état de la plupart des mesures de sécurité opérant au sein du CDE.</p> <p>Un test d'intrusion n'est pas vraiment un « test » car le résultat d'un test d'intrusion n'est pas quelque chose qui peut être classé comme une « réussite » ou un « échec ». Le meilleur résultat d'un test est un catalogue de vulnérabilités et de mauvaises configurations qu'une entité ne connaissait pas et que le testeur d'intrusion a trouvées avant qu'un attaquant ne puisse le faire. Un test d'intrusion qui n'a rien trouvé est généralement révélateur de lacunes du testeur d'intrusion, plutôt qu'un reflet positif de la posture de sécurité de l'entité.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.3</b> Un test d'intrusion externe est effectué :</p> <ul style="list-style-type: none"> <li>• Selon la méthodologie définie par l'entité</li> <li>• Au moins une fois tous les 12 mois.</li> <li>• Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application</li> <li>• Par une ressource interne qualifiée ou un tiers externe qualifié</li> <li>• L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.3.a</b> Examiner la périmètre des travaux et les résultats du test d'intrusion externe le plus récent afin de vérifier que les tests d'intrusion sont effectués conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>11.4.3.b</b> Interroger le personnel afin de vérifier que le test d'intrusion externe a été effectué par une ressource interne qualifiée ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les défenses externes du système sont vérifiées par des tests techniques conformément à la méthodologie définie par l'entité aussi souvent que nécessaire afin de faire face aux attaques et menaces nouvelles et évolutives, et de garantir que des modifications importantes n'introduisent pas de vulnérabilités inconnues.</p>	<p><b>Bonne Pratique</b></p> <p>Voici quelques considérations lors du choix d'une ressource qualifiée pour effectuer des tests d'intrusion :</p> <ul style="list-style-type: none"> <li>• Des certifications de tests d'intrusion spécifiques, qui peuvent être une indication du niveau de compétence et de connaissances du testeur.</li> <li>• Une expérience antérieure dans la conduite de tests d'intrusion - par exemple, le nombre d'années d'expérience, ainsi que le type et le périmètre des missions précédentes peuvent aider à confirmer si l'expérience du testeur est adaptée aux besoins de la mission.</li> </ul> <p><b>Informations Complémentaires</b></p> <p>Se référer au document : <i>the Information Supplement: Penetration Testing Guidance</i> sur le site Web du PCI SSC pour obtenir des conseils supplémentaires.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.4</b> Les vulnérabilités exploitables et les faiblesses de sécurité détectées lors des tests d'intrusion sont corrigées comme suit :</p> <ul style="list-style-type: none"> <li>Conformément à l'évaluation par l'entité du risque posé par le problème de sécurité tel que défini dans l'exigence 6.3.1.</li> <li>Les tests d'intrusion sont répétés pour vérifier les corrections.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les vulnérabilités et les faiblesses de sécurité découvertes lors de la vérification des défenses du système sont minimisées.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.4</b> Examiner les résultats des tests d'intrusion afin de vérifier que les vulnérabilités exploitables et les faiblesses de sécurité notées ont été corrigées conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>Les résultats d'un test d'intrusion sont généralement une liste hiérarchisée de vulnérabilités découvertes par l'exercice. Souvent, un testeur a enchaîné un certain nombre de vulnérabilités pour compromettre un composant système. La correction des vulnérabilités découvertes par un test d'intrusion réduit considérablement la probabilité que les mêmes vulnérabilités soient exploitées par un attaquant malveillant.</p> <p>L'utilisation du processus d'évaluation des risques de vulnérabilité de l'entité (voir l'exigence 6.3.1) garantit que les vulnérabilités qui présentent le risque le plus élevé pour l'entité seront corrigées plus rapidement.</p> <p><b>Bonne Pratique</b></p> <p>Dans le cadre de l'évaluation des risques par l'entité, les entités doivent examiner la probabilité d'exploiter la vulnérabilité et s'il existe d'autres mesures de sécurité dans l'environnement pour réduire le risque.</p> <p>Toute faiblesse indiquant que les exigences du standard PCI DSS ne sont pas respectées doit être corrigée.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.5</b> Si la segmentation est utilisée pour isoler le CDE des autres réseaux, des tests d'intrusion sont effectués sur les mesures de sécurité de segmentation comme suit :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les 12 mois et après toute modification des mesures ou méthodes de segmentation</li> <li>• Couvrir toutes les mesures ou méthodes de segmentation utilisée.</li> <li>• Conformément à la méthodologie des tests d'intrusion définie par l'entité.</li> <li>• Confirmer que les mesures ou méthodes de segmentation sont opérationnels et efficaces, et isolent le CDE de tous les systèmes hors du périmètre.</li> <li>• Confirmer l'efficacité de toute utilisation de l'isolement pour séparer les systèmes avec des niveaux de sécurité différents (voir l'exigence 2.2.3).</li> <li>• Effectués par une ressource interne qualifiée ou un tiers externe qualifié</li> <li>• L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Si la segmentation est utilisée, elle est vérifiée périodiquement par des tests techniques pour qu'elle demeure continuellement efficace, y compris après toute modification, afin d'isoler le CDE de tous les systèmes hors du périmètre.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.5.a</b> Examiner les mesures de sécurité de segmentation et examiner la méthodologie de test d'intrusion afin de vérifier que les procédures de test d'intrusion sont définies pour tester toutes les méthodes de segmentation conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>11.4.5.b</b> Examiner les résultats du test d'intrusion le plus récent afin de vérifier que le test d'intrusion couvre et traite tous les éléments spécifiés dans cette exigence.</p> <p><b>11.4.5.c</b> Interroger le personnel afin de vérifier que le test a été effectué par une ressource interne qualifiée ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</p>
	<p><b>Objectif</b></p> <p>Lorsqu'une entité utilise des mesures de segmentation pour isoler le CDE des réseaux internes hors de la zone de confiance, la sécurité du CDE dépend du fonctionnement de cette segmentation. De nombreuses attaques ont vu l'attaquant se déplacer latéralement de ce qu'une entité considérait comme un réseau isolé vers le CDE. L'utilisation d'outils et de techniques de test d'intrusion pour valider qu'un réseau hors de la zone de confiance est bien isolé du CDE peut alerter l'entité d'une défaillance ou d'une mauvaise configuration des mesures de segmentation, ce qui peut ensuite être rectifié.</p> <p><b>Bonne Pratique</b></p> <p>Des techniques telles que la découverte d'hôtes et l'analyse des ports peuvent être utilisées afin de vérifier que les segments hors de périmètre n'ont pas accès au CDE.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.6 Exigences supplémentaires pour les prestataires de services uniquement :</b> Si la segmentation est utilisée pour isoler le CDE des autres réseaux, des tests d'intrusion sont effectués sur les mesures de sécurité de segmentation comme suit :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les six mois et après toute modification des mesures de sécurité ou méthodes de segmentation</li> <li>• Couvrir tous les mesures ou méthodes de segmentation utilisée.</li> <li>• Conformément à la méthodologie des tests d'intrusion définie par l'entité.</li> <li>• Confirmer que les mesures ou méthodes de segmentation sont opérationnelles et efficaces, et isolent le CDE de tous les systèmes hors du périmètre.</li> <li>• Confirmer l'efficacité de toute utilisation de l'isolement pour séparer les systèmes avec des niveaux de sécurité différents (voir l'exigence 2.2.3).</li> <li>• Effectués par une ressource interne qualifiée ou un tiers externe qualifié</li> <li>• L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.6.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les résultats du test d'intrusion le plus récent afin de vérifier que l'intrusion couvre et a traité tous les éléments spécifiés dans cette exigence.</p> <p><b>11.4.6.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Interroger le personnel afin de vérifier que le test a été effectué par une ressource interne qualifiée ou un tiers externe qualifié et que l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Si la segmentation est utilisée, elle est vérifiée par des tests techniques pour qu'elle demeure continuellement efficace, y compris après toute modification, afin d'isoler le CDE des systèmes hors du périmètre.</p>	<p><b>Objectif</b> Les prestataires de services ont généralement accès à de plus grands volumes de données de titulaires de carte ou peuvent fournir un point d'entrée qui peut être exploité pour ensuite compromettre plusieurs autres entités. En général, les prestataires de services ont également des réseaux plus grands et plus complexes qui sont sujets à des modifications plus fréquentes. La probabilité d'échec des mesures de sécurité de segmentation dans les réseaux complexes et dynamiques est plus élevée dans les environnements des prestataires de services.</p> <p>La validation plus fréquente des mesures de sécurité de segmentation est susceptible de permettre la découverte de telles défaillances avant qu'elles ne puissent être exploitées par un attaquant tentant de basculer latéralement d'un réseau hors de la zone de confiance hors du périmètre du CDE.</p> <p><b>Bonne Pratique</b> Bien que l'exigence précise que cette validation du périmètre est effectuée au moins tous les six mois et après une modification importante, cet exercice doit être effectué aussi fréquemment que possible afin de s'assurer qu'il reste efficace pour isoler le CDE des autres réseaux.</p>
<p><b>Notes d'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.4.7 Exigence supplémentaire pour les prestataires de services mutualisés uniquement :</b> Les prestataires de services mutualisés assistent leurs clients dans les tests d'intrusion externes conformément aux exigences 11.4.3 et 11.4.4.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les prestataires de services mutualisés répondent aux besoins de leurs clients en matière de tests techniques, soit en fournissant un accès, soit en fournissant la preuve que des tests techniques comparables ont été effectués.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique uniquement lorsque l'entité en cours d'évaluation est un prestataire de services mutualisés.</p> <p>Pour satisfaire à cette exigence, les prestataires de services mutualisés peuvent :</p> <ul style="list-style-type: none"> <li>• Fournir des preuves à ses clients pour montrer que les tests d'intrusion ont été effectués conformément aux exigences 11.4.3 et 11.4.4 sur l'infrastructure souscrite par les clients, ou</li> <li>• Fournir un accès rapide à chacun de ses clients, afin que les clients puissent effectuer leurs propres tests d'intrusion.</li> </ul> <p>Les preuves fournies aux clients peuvent inclure des résultats de tests d'intrusion caviardés, mais doivent inclure des informations suffisantes pour prouver que tous les éléments des exigences 11.4.3 et 11.4.4 ont été satisfaits pour les besoins du consommateur.</p> <p>(suite à la page suivante)</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.4.7 Procédure de test supplémentaire uniquement pour les prestataires de services mutualisés :</b> Examiner les justificatifs pour vérifier que les prestataires de services mutualisés assistent leurs clients dans les tests d'intrusion externes conformément aux exigences 11.4.3 et 11.4.4.</p> <p><b>Objectif</b></p> <p>Les entités doivent effectuer des tests d'intrusion conformément au standard PCI DSS pour simuler le comportement des attaques et découvrir les vulnérabilités de leurs environnements. Dans les environnements partagés et cloud, le prestataire de services mutualisés peut être préoccupé par les activités d'un testeur d'intrusion touchant les systèmes d'autres clients.</p> <p>Ces fournisseurs de services mutualisés ne peuvent pas interdire les tests d'intrusion car cela laisserait les systèmes de leurs clients ouverts à l'exploitation. Par conséquent, les prestataires de services mutualisés doivent prendre en charge les demandes des clients pour effectuer des tests d'intrusion ou pour obtenir les résultats de tests d'intrusion.</p>

Exigences et Procédures de Test	Directives
<p>Reportez-vous également à l'<a href="#">Annexe A1</a> : <i>Exigences supplémentaires du standard PCI DSS pour les prestataires de services mutualisés.</i></p> <p><i>Cette exigence s'applique uniquement lorsque l'entité évaluée est un prestataire de services gérant des environnements hébergés/cloud tiers.</i></p>	

Exigences et Procédures de Test	Directives
<b>11.5 Les intrusions réseau et les modifications imprévues de fichiers sont détectées et traitées.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.5.1</b> Les techniques de détection des intrusions et/ou de prévention des intrusions sont utilisées pour détecter et/ou empêcher les intrusions dans le réseau comme suit :</p> <ul style="list-style-type: none"> <li>• Tout le trafic est surveillé à la périphérie du CDE.</li> <li>• Tout le trafic est surveillé aux points critiques du CDE.</li> <li>• Le personnel est alerté des suspicions de compromissions.</li> <li>• Tous les moteurs de détection et de prévention des intrusions, les lignes de base et les signatures sont tenus à jour.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.5.1.a</b> Examiner les configurations système et les schémas de réseau afin de vérifier que des techniques de détection et/ou de prévention des intrusions sont en place pour surveiller tout le trafic :</p> <ul style="list-style-type: none"> <li>• A la périphérie du CDE.</li> <li>• Aux points critiques du CDE.</li> </ul> <p><b>11.5.1.b</b> Examiner les configurations du système et interroger le personnel responsable afin de vérifier les techniques de détection et/ou de prévention des intrusions alertant le personnel des suspicions de compromissions.</p> <p><b>11.5.1.c</b> Examiner les configurations système et la documentation du fournisseur afin de vérifier que les techniques de détection et/ou de prévention des intrusions sont configurées pour maintenir à jour tous les moteurs, les références et les signatures.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des mécanismes de détection en temps réel du trafic réseau suspect ou anormal pouvant indiquer l'activité d'un acteur menaçant sont mis en œuvre. Les alertes générées par ces mécanismes sont traitées par le personnel ou par des moyens automatisés qui garantissent que les composants système ne peuvent pas être compromis en raison de l'activité détectée.</p>	<p><b>Objectif</b></p> <p>Les techniques de détection et/ou de prévention des intrusions (telles que IDS/IPS) comparent le trafic entrant sur le réseau à des « signatures » et/ou des comportements connus de milliers de types de compromissions (outils de piratage, chevaux de Troie et autres logiciels malveillants), et puis envoient des alertes et/ou arrêtent la tentative lorsqu'elle se produit. Sans une approche proactive pour détecter les activités non autorisées, les attaques (ou l'utilisation abusive) des ressources informatiques pourraient passer inaperçues pendant de longues périodes. L'impact d'une intrusion dans le CDE est, à bien des égards, un facteur lié au temps dont dispose un attaquant dans l'environnement avant d'être détecté.</p> <p><b>Bonne Pratique</b></p> <p>Les alertes de sécurité générées par ces techniques doivent être surveillées en permanence, afin que les intrusions tentées ou réelles puissent être bloquées et les dommages potentiels limités.</p> <p><b>Définitions</b></p> <p>Les emplacements critiques peuvent inclure, sans toutefois s'y limiter, les mesures de sécurité de sécurité réseau entre les segments de réseau (par exemple, entre une DMZ et un réseau interne ou entre un réseau dans le périmètre et hors de portée) et des points protégeant les connexions entre un réseau auquel on fait moins confiance et un composant système de confiance.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.5.1.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les techniques de détection et/ou de prévention des intrusions détectent, alertent/préviennent et traitent les canaux secrets de communication des logiciels malveillants.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.5.1.1.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner la documentation et les paramètres de configuration afin de vérifier que les méthodes de détection et d'alerte ou de prévention des canaux de communication malveillants secrets sont en place et fonctionnent comme prévu.</p> <p><b>11.5.1.1.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner le plan de réponse aux incidents de l'entité (Exigence 12.10.1) afin de vérifier qu'il demande et définit une réponse au cas où des canaux de communication secrets de logiciels malveillants seraient détectés.</p> <p><b>11.5.1.1.c Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Interroger le personnel responsable et observer les processus afin de vérifier que le personnel maintient une connaissance des techniques de communication secrètes et de contrôle des programmes malveillants et sait comment réagir lorsque des programmes malveillants sont suspectés.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des mécanismes sont en place pour détecter et alerter ou empêcher les communications secrètes avec les systèmes de commande et de contrôle. Les alertes générées par ces mécanismes sont traitées par le personnel ou par des moyens automatisés qui garantissent que ces communications sont bloquées.</p>	<p><b>Objectif</b> La détection des tentatives de communication secrètes de logiciels malveillants (par exemple, la tunnelisation DNS) peut aider à bloquer la propagation latérale des logiciels malveillants à l'intérieur d'un réseau et l'exfiltration de données. Lorsqu'elles décident de l'emplacement de cette mesure, les entités doivent prendre en compte les emplacements critiques dans le réseau et les itinéraires probables pour les canaux secrets.</p> <p>Lorsqu'un programme malveillant s'implante dans un environnement infecté, il essaie souvent d'établir un canal de communication vers un serveur de commande et de contrôle (C&amp;C). Par le biais du serveur C&amp;C, l'attaquant communique et contrôle les programmes malveillants sur les systèmes compromis afin de fournir des charges utiles ou des instructions malveillantes, ou pour lancer l'exfiltration de données. Dans de nombreux cas, le programme malveillant communiquera avec le serveur C&amp;C de manière indirecte via des botnets, contournant ainsi la surveillance, bloquant les mesures de sécurité et rendant ces méthodes inefficaces pour détecter les canaux secrets.</p> <p><b>Bonne Pratique</b> Les méthodes qui peuvent aider à détecter et à traiter les canaux de communication des programmes malveillants incluent l'analyse des points de terminaison en temps réel, le filtrage du trafic de sortie, une liste blanche, des outils de prévention des pertes de données et des outils de surveillance de la sécurité du réseau tels que IDS/IPS.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p>De plus, les requêtes et réponses DNS sont une source de données clé utilisée par les défenseurs du réseau pour prendre en charge la réponse aux incidents ainsi que la découverte des intrusions. Lorsque ces transactions sont collectées à des fins de traitement et d'analyse, elles peuvent activer un certain nombre de scénarios précieux d'analyse de la sécurité.</p> <p>Il est important que les entreprises maintiennent des connaissances à jour sur les modes de fonctionnement des programmes malveillants, car leur prise en compte peut aider à détecter et à limiter l'impact des logiciels malveillants dans l'environnement.</p>
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.5.2</b> Un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) est déployé de la façon suivante :</p> <ul style="list-style-type: none"> <li>• Pour alerter le personnel de modifications non autorisées (y compris les modifications, les ajouts et les suppressions) de fichiers critiques</li> <li>• Pour effectuer des comparaisons de fichiers critiques au moins une fois par semaine.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.5.2.a</b> Examiner les paramètres système, les fichiers surveillés et les résultats des activités de surveillance afin de vérifier l'utilisation d'un mécanisme de détection des modifications.</p> <p><b>11.5.2.b</b> Examiner les paramètres du mécanisme de détection des modifications afin de vérifier qu'il est configuré conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les fichiers critiques ne peuvent pas être modifiés par du personnel non autorisé sans qu'une alerte ne soit générée.</p>	<p><b>Objectif</b></p> <p>Les modifications apportées aux fichiers critiques du système, fichiers de configuration ou fichiers de contenu peuvent indiquer qu'un attaquant a accédé au système d'une entreprise. De telles modifications peuvent permettre à un attaquant d'effectuer d'autres actions malveillantes, d'accéder aux données des titulaires de cartes et/ou de mener des activités sans détection ni enregistrement.</p> <p>Un mécanisme de détection des modifications détectera et évaluera ces modifications apportées aux fichiers critiques et générera des alertes auxquelles il sera possible de répondre en suivant les processus définis afin que le personnel puisse prendre les mesures appropriées.</p> <p>Si elle n'est pas mise en œuvre de manière correcte, et que les informations de sortie de la solution de détection des modifications ne sont pas surveillées, une personne malveillante pourrait ajouter, supprimer ou modifier le contenu du fichier de configuration, les programmes du système d'exploitation ou les fichiers exécutables de l'application.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Pour la détection des changements, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une compromission ou un risque de compromission du système. Les mécanismes de détection des changements, tels que les outils de surveillance de l'intégrité des fichiers, sont généralement préconfigurés avec des fichiers critiques pour le système d'exploitation associé. D'autres fichiers critiques, tels que ceux des applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).</p>	<p>Les modifications non autorisées, si elles ne sont pas détectées, pourraient rendre les mesures de sécurité de sécurité existants inefficaces et/ou entraîner le vol de données des titulaires de cartes sans impact perceptible sur le traitement normal.</p> <p><b>Bonne Pratique</b></p> <p>Des exemples de types de fichiers qui doivent être surveillés comportent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Des fichiers exécutables système.</li> <li>• Des fichiers exécutables des applications.</li> <li>• Des fichiers de configuration et de paramétrage.</li> <li>• Des journaux d'audit stockés de manière centralisée, historiques ou archivés.</li> <li>• Des dossiers critiques supplémentaires déterminés par entité (par exemple, par le biais d'une évaluation des risques ou d'autres moyens).</li> </ul> <p><b>Exemples</b></p> <p>Des solutions de détection des modifications telles que les outils de surveillance de l'intégrité des fichiers (FIM) vérifient les modifications, les ajouts et les suppressions de fichiers critiques et notifient lorsque de telles modifications sont détectées.</p>

Exigences et Procédures de Test	Directives	
<b>11.6 Les modifications non autorisées sur les pages de paiement sont détectées et traitées.</b>		
<p><b>Exigences de L'approche Définie</b></p> <p><b>11.6.1</b> Un mécanisme de détection des changements et des altérations est déployé de la manière suivante :</p> <ul style="list-style-type: none"> <li>• Alerter le personnel des modifications non autorisées (y compris les indicateurs de compromission, de changements, d'ajouts et de suppressions) de la sécurité impactant les en-têtes HTTP et du contenu des scripts des pages de paiement comme reçus par le navigateur du consommateur.</li> <li>• Le mécanisme est configuré pour évaluer les en-têtes HTTP et les pages de paiement reçus.</li> <li>• Les fonctions des mécanismes sont exécutées comme suit : <ul style="list-style-type: none"> <li>– Au moins une fois toutes les semaines <b>OU</b></li> <li>– Périodiquement, (à la fréquence définie dans l'analyse de risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1).</li> </ul> </li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>11.6.1.a</b> Examiner les paramètres du système, les pages de paiement surveillées et les résultats des activités de surveillance afin de vérifier l'utilisation d'un mécanisme de détection des modifications et des altérations.</p> <p><b>11.6.1.b</b> Examiner les paramètres de configuration afin de vérifier que le mécanisme est configuré conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>11.6.1.c</b> Si les fonctions du mécanisme sont exécutées à une fréquence définie par l'entité, examiner l'analyse de risque ciblée de l'entité pour déterminer la fréquence afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés à l'Exigence 12.3.1.</p> <p><b>11.6.1.d</b> Examiner les paramètres de configuration et interroger le personnel afin de vérifier que les fonctions du mécanisme sont effectuées :</p> <ul style="list-style-type: none"> <li>• Au moins une fois toutes les semaines <b>OU</b></li> <li>• A la fréquence définie dans l'analyse de risques ciblée de l'entité réalisée pour la présente exigence.</li> </ul>	<p><b>Objectif</b></p> <p>De nombreuses pages Web reposent désormais sur l'assemblage d'objets, y compris du contenu actif (principalement JavaScript), à partir de plusieurs emplacements Internet. De plus, le contenu de nombreuses pages Web est défini à l'aide de systèmes de gestion de contenu et de gestion de balises qu'il pourrait être impossible de surveiller à l'aide des mécanismes classiques toute détection de modifications.</p> <p>Par conséquent, le seul endroit pour détecter les modifications ou les indicateurs d'activité malveillante est dans le navigateur du consommateur lors de la construction de la page et de l'interprétation de tous les scripts JavaScript.</p> <p>En comparant la version actuelle de l'en-tête HTTP et le contenu actif des pages de paiement telles que reçues par le navigateur du consommateur avec des versions antérieures ou connues, il est possible de détecter des modifications non autorisées pouvant indiquer une attaque par écrémage, ou une tentative de désactiver un contrôle conçu pour protéger contre ou détecter les attaques d'écrémage.</p> <p>Aussi, en recherchant des indicateurs connus de compromission et des éléments de script ou un comportement typique des écumeurs, des alertes suspectes peuvent être déclenchées.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le code ou les techniques d'écrémage du commerce électronique ne peuvent pas être ajoutés aux pages de paiement telles qu'elles sont reçues par le navigateur du consommateur sans qu'une alerte ne soit générée en temps opportun. Les mesures contre l'écrémage ne peuvent pas être supprimées des pages de paiement sans qu'une alerte rapide ne soit générée.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique également aux entités disposant d'une ou plusieurs pages Web qui incluent la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un ou plusieurs cadres en ligne ou iframes.).</p> <p>Cette exigence ne s'applique pas à une entité pour les scripts dans la page/formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, une ou plusieurs iframes), lorsque l'entité inclut la page/formulaire de paiement d'un TPSP/processeur de paiement sur sa page Web.</p> <p>Il incombe au TPSP/processeur de paiement de gérer les scripts dans la page/le formulaire de paiement intégré du TPSP/processeur de paiement conformément à cette exigence.</p> <p>L'intention de cette exigence n'est pas qu'une entité soit obligée d'installer un logiciel dans les systèmes ou les navigateurs de ses consommateurs, mais plutôt qu'elle utilise des techniques telles que celles décrites dans les exemples ci-dessus afin d'empêcher et de détecter des activités de script imprévues.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Bonne Pratique</b></p> <p>Lorsqu'une entité inclut la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement sur sa page Web, l'entité doit s'attendre à ce que le TPSP/processeur de paiement fournisse la preuve que le TPSP/processeur de paiement satisfait à cette exigence, conformément à l'évaluation PCI DSS du TPSP/processeur de paiement et à l'exigence 12.9.</p> <p><b>Exemples</b></p> <p>Les mécanismes qui détectent et signalent les modifications apportées aux en-têtes et au contenu de la page de paiement pourraient comporter, sans toutefois s'y limiter une combinaison des techniques suivantes :</p> <ul style="list-style-type: none"> <li>• Les violations de la politique de sécurité du contenu (CSP) peuvent être signalées à l'entité par le biais des directives CSP <i>report-to</i> ou <i>report-uri</i>.</li> <li>• Les modifications apportées au CSP lui-même peuvent indiquer une tentative d'altération.</li> <li>• La surveillance externe par des systèmes qui demandent et analysent les pages Web reçues (également appelée surveillance synthétique des utilisateurs) peut détecter les modifications apportées au script JavaScript dans les pages de paiement et alerter le personnel.</li> <li>• L'intégration d'un script de détection d'altération inviolable dans la page de paiement peut alerter et bloquer lorsqu'un comportement de script malveillant est détecté.</li> <li>• Les serveurs proxy inverse et les réseaux de diffusion de contenu peuvent détecter les changements dans les scripts et alerter le personnel.</li> </ul> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
	<p>La liste de mécanismes ci-dessus n'est pas exhaustive et l'utilisation d'un mécanisme donné ne constitue pas nécessairement un mécanisme complet de détection et de signalement. Ces mécanismes sont souvent des abonnements ou basés sur le cloud, mais peuvent également être basés sur des solutions personnalisées et sur mesure.</p>

## Maintenir une Politique de Sécurité de L'information

### ***Exigence 12 : Appuyer la Sécurité de l'Information sur des Politiques et des Programmes Organisationnels***

#### Sections

- 12.1** Une politique complète de sécurité de l'information qui régit et fournit une orientation pour la protection des actifs informationnels de l'entité est connue et à jour.
- 12.2** Des politiques d'utilisation acceptable des technologies de l'utilisateur final sont définies et mises en œuvre.
- 12.3** Les risques pour l'environnement des données des titulaires de cartes sont formellement identifiés, évalués et gérés.
- 12.4** La conformité au standard PCI DSS est gérée.
- 12.5** Le périmètre où s'applique PCI DSS est documenté et validé.
- 12.6** La sensibilisation à la sécurité est une activité continue.
- 12.7** La vérification des antécédents du personnel est effectuée afin de réduire les risques d'attaques internes.
- 12.8** Le risque pour les actifs de données associés aux relations avec les prestataires de services tiers (TPSP) est géré.
- 12.9** Les prestataires de services tiers (TPSP) prennent en charge la conformité du standard PCI DSS de leurs clients.
- 12.10** Les incidents de sécurité soupçonnés et confirmés pouvant avoir un impact sur le CDE sont traités immédiatement.

#### Aperçu

La politique globale de sécurité de l'information de l'entreprise donne le ton à l'ensemble de l'entité et informe le personnel de ce que l'entreprise attend d'eux. Tout le personnel doit être conscient de la sensibilité des données des titulaires de cartes et de leurs responsabilités en matière de leur protection.

Pour ce qui concerne l'exigence 12, le « personnel » fait référence aux employés à temps plein et à temps partiel, aux employés temporaires, aux sous-traitants et aux consultants ayant des responsabilités en matière de sécurité pour la protection des données de carte ou pouvant avoir un impact sur la sécurité des données des titulaires de compte et/ou des données d'authentification sensibles.

Se référer à [l'Annexe G](#) pour les définitions des termes du standard PCI DSS.

Exigences et Procédures de Test	Directives
<b>12.1 Une politique complète de sécurité de l'information qui régit et fournit une orientation pour la protection des actifs informationnels de l'entité est connue et à jour.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.1.1</b> Une politique globale de sécurité de l'information est :</p> <ul style="list-style-type: none"> <li>• Établie.</li> <li>• Publiée.</li> <li>• Maintenue.</li> <li>• Diffusée à tout le personnel concerné, ainsi qu'aux fournisseurs et partenaires commerciaux concernés.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.1.1</b> Examiner la politique de sécurité de l'information et interroger le personnel afin de vérifier que la politique globale de sécurité de l'information est gérée conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les objectifs stratégiques et les principes de la sécurité de l'information sont définis, adoptés et connus de l'ensemble du personnel.</p>	<b>Objectif</b> <p>La politique globale de sécurité de l'information d'une entreprise est liée à et régit toutes les autres politiques et procédures qui définissent la protection des données des titulaires de cartes.</p> <p>La politique de sécurité de l'information communique l'intention et les objectifs de la direction concernant la protection de ses actifs les plus précieux, y compris les données des titulaires de cartes.</p> <p>Sans politique de sécurité de l'information, des personnes prendront leurs propres décisions sur les mesures de sécurité requis au sein de l'entreprise, ce qui pourrait empêcher l'organisation de respecter ses obligations légales, réglementaires et contractuelles, ni de pouvoir protéger adéquatement ses actifs de manière cohérente.</p> <p>Pour garantir la mise en œuvre de la politique, il est important que tout le personnel concerné au sein de l'entreprise, ainsi que les tiers, les fournisseurs et les partenaires commerciaux concernés soient conscients de la politique de sécurité de l'information de l'entreprise et de leurs responsabilités en matière de protection des actifs de données.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p><b>Bonne Pratique</b></p> <p>La politique de sécurité de l'entreprise identifie l'objectif, le périmètre, la responsabilité et les informations qui définissent clairement la position de l'entreprise concernant la sécurité d de l'information.</p> <p>La politique globale de sécurité des informations diffère des politiques de sécurité individuelles qui traitent de technologies spécifiques ou de disciplines de sécurité. Cette politique énonce les directives pour l'ensemble de l'entreprise tandis que les politiques de sécurité individuelles s'alignent sur et soutiennent la politique de sécurité globale et communiquent des objectifs spécifiques pour les disciplines liées aux technologies ou à la sécurité.</p> <p>Il est important que tout le personnel concerné au sein de l'entreprise, ainsi que les tiers, les fournisseurs et les partenaires commerciaux concernés soient conscients de la politique de sécurité des informations de l'entreprise et de leurs responsabilités en matière de protection des fonds documentaires.</p> <p><b>Définitions</b></p> <p>Le terme « pertinent » dans cette exigence signifie que la politique de sécurité de l'information est diffusée à ceux qui ont des rôles applicables à certains ou à tous les sujets de la politique, soit au sein de l'entreprise, soit en raison de services/fonctions exécutés par un fournisseur ou un tiers.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.1.2</b> La politique de sécurité de l'information est :</p> <ul style="list-style-type: none"> <li>• Examinée au moins une fois tous les 12 mois.</li> <li>• Mise à jour, si besoin, pour refléter les modifications apportées aux objectifs professionnels ou les risques pour l'environnement.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.1.2</b> Examiner la politique de sécurité de l'information et interroger le personnel responsable afin de vérifier que la politique est gérée conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>La politique de sécurité de l'information continue de refléter les objectifs et les principes stratégiques de l'entreprise.</p>	<b>Objectif</b> Les menaces de sécurité et les méthodes de protection associées évoluent rapidement. Sans mettre à jour la politique de sécurité de l'information afin de refléter les changements pertinents, de nouvelles mesures de défense contre ces menaces pourraient ne pas être prises en compte.
<b>Exigences de L'approche Définie</b> <p><b>12.1.3</b> La politique de sécurité définit clairement les rôles et les responsabilités en matière de sécurité de l'information pour tout le personnel, et tout le personnel est conscient et reconnaît ses responsabilités en matière de sécurité de l'information.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.1.3.a</b> Examiner la politique de sécurité de l'information afin de vérifier qu'elles définissent clairement les rôles et les responsabilités en matière de sécurité des informations pour tout le personnel.</p> <p><b>12.1.3.b</b> Interroger le personnel dans divers rôles afin de vérifier qu'il comprend ses responsabilités en matière de sécurité de l'information.</p> <p><b>12.1.3.c</b> Examiner les preuves documentées afin de vérifier que le personnel reconnaît ses responsabilités en matière de sécurité de l'information.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le personnel comprend son rôle dans la protection des données des titulaires de carte de l'entité.</p>	<b>Objectif</b> Sans rôles et responsabilités de sécurité clairement définis, il pourrait y avoir une mauvaise utilisation des fonds documentaires de l'entreprise ou une interaction incohérente avec le personnel de sécurité de l'information, entraînant une mise en œuvre non sécurisée de technologies ou à l'utilisation de technologies obsolètes ou non sécurisées.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.1.4</b> La responsabilité de la sécurité de l'information est officiellement attribuée à un responsable de la sécurité de l'information ou à un autre membre de la direction compétent en matière de sécurité de l'information.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.1.4</b> Examiner la politique de sécurité de l'information afin de vérifier que la sécurité des informations est officiellement attribuée à un responsable de la sécurité de l'information ou à un autre membre de la direction compétent en matière de sécurité des informations.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un membre désigné de la direction générale est responsable de la sécurité de l'information.</p>	<p><b>Objectif</b> Pour s'assurer qu'une personne ayant suffisamment d'autorité et de responsabilité gère et protège activement le programme de sécurité de l'information de l'entreprise, l'obligation de rendre compte et la responsabilité de la sécurité de l'information doivent être attribuées au niveau exécutif au sein d'une entreprise.</p> <p><b>Bonne Pratique</b> Ces postes de direction exécutive se situent souvent au niveau de direction le plus élevé et font partie du niveau de la direction ou du niveau C, relevant généralement du président-directeur général ou du conseil d'administration. Les connaissances en sécurité de l'information pour ce rôle de direction peuvent être indiquées par une expérience professionnelle, une formation et/ou des certifications professionnelles pertinentes. On s'attend à ce que cette personne puisse fournir une assurance quant à la mise en œuvre d'un programme de sécurité efficace et garantir que les experts techniques appropriés sont employés. Les entités doivent également envisager des plans de transition et/ou de succession pour ce personnel clé afin d'éviter d'éventuelles lacunes dans les activités de sécurité critiques.</p>

Exigences et Procédures de Test	Directives
<b>12.2 Des politiques d'utilisation acceptable des technologies de l'utilisateur final sont définies et mises en œuvre.</b>	
<b>Exigences de L'approche Définie</b>	<b>Procédures de Test de L'approche Définie</b>
<p><b>12.2.1</b> Des politiques d'utilisation acceptable pour les technologies d'utilisateur final sont documentées et mises en œuvre, notamment :</p> <ul style="list-style-type: none"> <li>• Une approbation expresse par les parties autorisées.</li> <li>• Des utilisations acceptables de la technologie.</li> <li>• Une liste de produits approuvés par l'entreprise pour une utilisation par les employés, y compris le matériel et les logiciels.</li> </ul>	<p><b>12.2.1</b> Examiner les politiques d'utilisation acceptable des technologies de l'utilisateur final et interroger le personnel responsable afin de vérifier que les processus sont documentés et mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>L'utilisation des technologies de l'utilisateur final est définie et gérée afin de garantir une utilisation autorisée.</p>	<p><b>Objectif</b></p> <p>Les technologies de l'utilisateur final représentent un investissement important et peuvent présenter un risque important pour une entreprise si elles ne sont pas gérées correctement. Les politiques d'utilisation acceptable décrivent le comportement attendu du personnel lors de l'utilisation des technologies de l'information de l'entreprise et reflètent le niveau de tolérance au risque de l'entreprise</p> <p>Ces politiques informent le personnel sur ce qu'il peut et ne peut pas faire avec l'équipement de l'entreprise, et indiquent le personnel sur les utilisations correctes et incorrectes des ressources Internet et de messagerie de l'entreprise. De telles politiques peuvent juridiquement protéger une entreprise et lui permettre d'agir lorsque les politiques sont violées.</p>
<b>Notes D'applicabilité</b> <p>Des exemples de technologies d'utilisateur final pour lesquelles des politiques d'utilisation acceptables sont prévues incluent, sans toutefois s'y limiter, les technologies d'accès à distance et sans fil, les ordinateurs portables, les tablettes, les téléphones portables et les supports électroniques amovibles, l'utilisation de la messagerie électronique et l'utilisation d'Internet.</p>	<p><b>Bonne Pratique</b></p> <p>Il est important que les politiques d'utilisation soient appuyées par des mesures de sécurité techniques afin de gérer l'application des politiques.</p> <p>Structurer les politiques comme de simples exigences « faire » et « ne pas faire » liées à un objectif peut aider à lever l'ambiguité et fournir au personnel le contexte de l'exigence.</p>

Exigences et Procédures de Test	Directives
<b>12.3 Les risques pour l'environnement des données des titulaires de cartes sont formellement identifiés, évalués et gérés.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.3.1</b> Pour chaque exigence du standard PCI DSS qui spécifie l'accomplissement d'une analyse de risque ciblée, l'analyse est documentée et comprend :</p> <ul style="list-style-type: none"> <li>• L'identification des actifs à protéger.</li> <li>• L'identification de la ou des menaces contre lesquelles l'exigence protège.</li> <li>• L'identification des facteurs qui contribuent à la probabilité et/ou à l'impact d'une menace.</li> <li>• L'analyse résultante qui détermine et inclut la justification de la manière dont la fréquence et les processus définis par l'entité pour satisfaire à l'exigence minimisent la probabilité et/ou l'impact de la menace qui se matérialise.</li> <li>• L'examen de chaque analyse de risque ciblée au moins une fois tous les 12 mois afin de déterminer si les résultats sont toujours valides ou si une analyse de risque mise à jour est nécessaire.</li> <li>• La réalisation d'analyses de risques mises à jour au besoin, tel que déterminé par l'examen annuel.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.3.1</b> Examiner les politiques et procédures documentées afin de vérifier qu'un processus est défini pour effectuer des analyses de risques ciblées pour chaque exigence du standard PCI DSS qui indique l'accomplissement d'une analyses de risques ciblée et que le processus comporte tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Des connaissances et une évaluation à jour des risques pour le CDE sont maintenues.</p> <p>(suite à la page suivante)</p>	<b>Objectif</b> <p>Certaines exigences du standard PCI DSS permettent à une entité de définir la fréquence à laquelle une activité est effectuée en fonction du risque pour l'environnement de l'entité. La réalisation de cette analyse de risques selon une méthodologie garantit la validité et la conformité avec les politiques et les procédures.</p> <p>Cette analyse de risques ciblée (par opposition à une évaluation classique des risques à l'échelle de l'entreprise) est axée sur les exigences du standard PCI DSS qui permettent à une entité une flexibilité quant à la fréquence à laquelle une entité exécute un contrôle donné. Pour cette analyse de risques, l'entité évalue soigneusement chaque exigence du standard PCI DSS qui offre cette flexibilité et détermine la fréquence qui favorise une sécurité adéquate pour l'entité, ainsi que le niveau de risque que l'entité est prête à accepter.</p> <p>L'analyse de risques identifie les actifs spécifiques, tels que les composants système et les données (par exemple, les fichiers journaux ou les informations d'identification) que l'exigence est destinée à protéger, ainsi que la ou les menaces ou les résultats que l'exigence protège les actifs de—par exemple, un programme malveillant, un intrus non détecté ou une mauvaise utilisation des informations d'identification. Des exemples de facteurs qui pourraient contribuer à la probabilité ou à l'impact comportent ceux qui pourraient augmenter la vulnérabilité d'un actif à une menace ; par exemple, l'exposition à des réseaux hors zone de confiance, la complexité de l'environnement ou le roulement élevé du personnel, ainsi que la criticité des composants système, ou le volume et la sensibilité des données protégées.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p>L'examen des résultats de ces analyses de risques ciblées au moins une fois tous les 12 mois et en cas de changements qui pourraient avoir un impact sur le risque pour l'environnement, permet à l'entreprise de s'assurer que les résultats de l'analyse de risques restent à jour avec les changements organisationnels et l'évolution des menaces, des tendances et des technologies, et que les fréquences choisies répondent toujours adéquatement au risque de l'entité.</p> <p><b>Bonne Pratique</b></p> <p>Une évaluation des risques à l'échelle de l'entreprise, qui est une activité ponctuelle qui permet aux entités d'identifier les menaces et les vulnérabilités associées, est recommandée, mais n'est pas obligatoire, afin que les entités déterminent et comprennent les menaces plus larges et émergentes susceptibles d'avoir une incidence négative sur la sécurité de leur entreprise. Cette évaluation des risques à l'échelle de l'entreprise pourrait être établie dans le cadre d'un programme global de gestion des risques, utilisé comme contribution à l'examen annuel de la politique globale de sécurité de l'information d'une entreprise (voir l'exigence 12.1.1).</p> <p>Des exemples de méthodologies d'évaluation des risques pour les évaluations des risques à l'échelle de l'entreprise comportent, sans toutefois s'y limiter, les standards ISO 27005 et NIST SP 800-30.</p> <p><b>Informations Complémentaires</b></p> <p>Reportez-vous aux documents suivants sur le site Web PCI SSC</p> <ul style="list-style-type: none"> <li>• <i>Supplément d'information : Orientation TRA</i></li> <li>• <i>Exemple de modèle : TRA pour fréquence d'activité.</i></li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.3.2</b> Une analyse de risque ciblée est effectuée pour chaque exigence du standard PCI DSS que l'entité satisfait à l'approche personnalisée, pour inclure :</p> <ul style="list-style-type: none"> <li>• Une preuve documentée détaillant chaque élément spécifié à l'annexe D : Une approche personnalisée (incluant, au minimum, une matrice de mesures de sécurité et une analyse de risques).</li> <li>• Une approbation des preuves documentées par la haute direction.</li> <li>• Une réalisation de l'analyse de risque ciblée au moins une fois tous les 12 mois.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.3.2</b> Examiner l'analyse ciblée de risques documentée pour chaque exigence du standard PCI DSS que l'entité satisfait à l'approche personnalisée afin de vérifier que la documentation pour chaque exigence existe et est conforme à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence fait partie de l'approche personnalisée et doit être observée pour les entités qui utilisent l'approche personnalisée.</p>	<p><b>Objectif</b> Une analyse de risques basée sur une méthodologie reproductible et robuste permet à une entité d'atteindre l'objectif de l'approche personnalisée.</p> <p><b>Définitions</b> L'approche personnalisée pour satisfaire à une exigence du standard PCI DSS permet aux entités de définir les mesures de sécurité utilisée pour répondre à l'objectif d'approche personnalisée d'une exigence donnée d'une manière qui ne suit pas strictement l'exigence définie. Ces mesures de sécurité devraient au moins atteindre ou dépasser la sécurité fournie par l'exigence définie et nécessiterait une documentation complète de la part de l'entité utilisant l'approche personnalisée.</p> <p><b>Informations Complémentaires</b> Voir <a href="#">l'Annexe D : Approche personnalisée</a> afin d'obtenir des instructions sur la façon de documenter les justificatifs nécessaires pour l'approche personnalisée.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence s'applique uniquement aux entités utilisant une approche personnalisée.</p>	<p>Voir PCI DSS v4.x : Exemples de modèles pour prendre en charge une approche personnalisée pour obtenir des modèles que les entités peuvent utiliser afin de documenter leurs mesures de sécurité personnalisée. Notez que bien que l'utilisation des modèles soit facultative, les informations spécifiées dans chaque modèle doivent être documentées et fournies à l'auditeur de chaque entité.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.3.3</b> Les suites de chiffrement cryptographiques et les protocoles utilisés sont documentés et examinés au moins une fois tous les 12 mois, y compris au moins les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Un inventaire tenu à jour de toutes les suites et protocoles de chiffrement cryptographiques utilisés, y compris le but et le lieu d'utilisation.</li> <li>• Une surveillance active des tendances de l'industrie concernant la viabilité continue de toutes les suites et protocoles de chiffrement cryptographiques utilisés.</li> <li>• Une documentation d'un plan pour répondre aux changements anticipés des vulnérabilités cryptographiques.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.3.3</b> Examiner la documentation relative aux suites et protocoles cryptographiques utilisés et interroger le personnel afin de vérifier que la documentation et l'examen sont conformes à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'entité est en mesure de réagir rapidement à toute vulnérabilité dans les protocoles ou algorithmes cryptographiques, lorsque ces vulnérabilités affectent la protection des données des titulaires de cartes.</p>	<p><b>Objectif</b> Les protocoles et les niveaux de chiffrement peuvent changer rapidement ou être dépréciés en raison de l'identification de vulnérabilités ou de défauts de conception. Pour répondre aux besoins actuels et futurs des exigences en termes de sécurité des données, les entités doivent savoir où la cryptographie est utilisée et comprendre comment elles pourraient réagir rapidement aux changements affectant la robustesse de leurs mises en œuvre cryptographiques.</p> <p><b>Bonne Pratique</b> L'agilité cryptographique est essentielle pour garantir qu'une alternative à la méthode de chiffrement d'origine ou à la primitive cryptographique est disponible, avec des plans pour passer à l'alternative sans modification importante de l'infrastructure du système. Par exemple, si l'entité sait quand les protocoles ou les algorithmes seront dépréciés par les organismes de normalisation, les plans proactifs aideront l'entité dans la mise à niveau avant que la dépréciation n'ait un impact sur ses opérations.</p> <p><b>Définitions</b> « L'agilité cryptographique » fait référence à la capacité de surveiller et de gérer le chiffrement et les technologies de vérification associées déployées dans une entreprise.</p> <p><b>Informations Complémentaires</b> Se referrer au <i>NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths</i>.</p>
<p><b>Notes D'applicabilité</b></p> <p>L'exigence s'applique à toutes les suites et protocoles cryptographiques utilisés pour répondre aux exigences du standard PCI DSS, y compris, sans toutefois s'y limiter, ceux utilisés pour rendre les PAN illisibles lors du stockage et de la transmission, pour protéger les mots de passe et dans le cadre de l'authentification de l'accès.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.3.4</b> Les technologies matérielles et logicielles utilisées sont examinées au moins une fois tous les 12 mois, en incluant au moins les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Une analyse démontrant que les technologies continuent de recevoir rapidement des correctifs de sécurité des fournisseurs.</li> <li>• Une analyse démontrant que les technologies continuent de prendre en charge (et n'empêchent pas) la conformité au standard PCI DSS de l'entité.</li> <li>• Une documentation de toute annonce ou tendance de l'industrie liée à une technologie ; par exemple, lorsqu'un fournisseur annonce des plans de « fin de vie » pour une technologie.</li> <li>• La documentation d'un plan, approuvé par la haute direction, pour traiter les technologies obsolètes, y compris celles pour lesquelles les fournisseurs ont annoncé des plans de « fin de vie ».</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.3.4</b> Examiner la documentation pour l'examen des technologies matérielles et logicielles utilisées et interroger le personnel afin de vérifier que l'examen est conforme à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les technologies matérielles et logicielles de l'entité sont à jour et prises en charge par le vendeur. Les plans de suppression ou de remplacement de tous les composants système non pris en charge sont examinés périodiquement.</p>	<p><b>Objectif</b> Les technologies matérielles et logicielles évoluent constamment, et les entreprises doivent être conscientes des changements apportés aux technologies qu'elles utilisent, ainsi que de l'évolution des menaces pesant sur ces technologies afin de s'assurer qu'elles peuvent se préparer et gérer les vulnérabilités du matériel et des logiciels qui ne seront pas corrigé par le fournisseur ou le développeur.</p> <p><b>Bonne Pratique</b> Les entreprises doivent examiner les versions des firmwares afin de s'assurer qu'elles restent à jour et supportées par les fournisseurs. Les entreprises doivent également être conscientes des modifications apportées par les fournisseurs de technologies à leurs produits ou processus pour comprendre la manière dont ces modifications peuvent avoir un impact sur l'utilisation de la technologie par l'entreprise. Des revues régulières des technologies qui ont un impact ou une influence sur les mesures de sécurité du standard PCI DSS peuvent aider à l'achat, à l'utilisation et aux stratégies de déploiement, et garantir que les mesures de sécurité qui reposent sur ces technologies restent efficaces. Ces revues comportent, sans toutefois s'y limiter, l'examen des technologies qui ne sont plus prises en charge par le fournisseur et/ou qui ne répondent plus aux besoins de sécurité de l'entreprise.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>12.4 La conformité au standard PCI DSS est gérée.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.4.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> La responsabilité est établie par la direction générale pour la protection des données des titulaires de cartes et un programme de conformité PCI DSS incluant :</p> <ul style="list-style-type: none"> <li>Responsabilité globale pour le maintien de la conformité PCI DSS.</li> <li>Définition d'une charte pour un programme de conformité PCI DSS et sa communication à la direction générale.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.4.1 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner la documentation afin de vérifier que la haute direction a établi la responsabilité de la protection des données des titulaires de cartes et un programme de conformité PCI DSS conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les cadres sont responsables et comptables de la sécurité des données des titulaires de cartes.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>La direction générale peut inclure des postes au niveau exécutif, comité de direction ou équivalent. Les titres spécifiques dépendront de la structure organisationnelle.</p> <p>La responsabilité du programme de conformité PCI DSS peut être attribuée à des rôles individuels et/ou à des départements au sein de l'entreprise.</p>	<b>Objectif</b> L'attribution par la direction générale des responsabilités de conformité PCI DSS garantit une visibilité au niveau de la direction sur le programme de conformité PCI DSS, et permet de poser les questions appropriées pour déterminer l'efficacité du programme et influer sur les priorités stratégiques.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.4.2 Exigences supplémentaires pour les prestataires de services uniquement :</b> Des revues sont effectuées au moins une fois tous les trois mois, par du personnel autre que ceux responsables de l'exécution de la tâche donnée afin de confirmer que le personnel exécute ses tâches, conformément à toutes les politiques de sécurité et à toutes les procédures opérationnelles, y compris, sans toutefois s'y limiter, les tâches suivantes :</p> <ul style="list-style-type: none"> <li>• Examens quotidiens des journaux.</li> <li>• Examens des configurations pour les mesures de sécurité réseau.</li> <li>• Application des standards de configuration aux nouveaux systèmes.</li> <li>• Réponse aux alertes de sécurité.</li> <li>• Processus de gestion des changements.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.4.2.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les politiques et procédures afin de vérifier que des processus sont définis pour effectuer des revues pour confirmer que le personnel effectue ses tâches conformément à toutes les politiques de sécurité et à toutes les procédures opérationnelles, y compris, sans toutefois s'y limiter, les tâches spécifiées dans cette exigence.</p> <p><b>12.4.2.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Interroger le personnel responsable et consulter les enregistrements des revues afin de vérifier que les revues sont effectuées :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les trois mois.</li> <li>• Par du personnel autre que ceux chargés de l'exécution de la tâche donnée.</li> </ul>
<b>Objectif de L'approche Personnalisée</b> <p>L'efficacité opérationnelle des mesures de sécurité critiques du standard PCI DSS est vérifiée périodiquement par une inspection manuelle des enregistrements.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	
	<b>Objectif</b> <p>Une confirmation régulière que les politiques et procédures de sécurité sont suivies donne l'assurance que les mesures de sécurité attendue sont actives et fonctionnent comme prévu. Cette exigence est distincte des autres exigences qui spécifient une tâche à effectuer. L'objectif de ces revues n'est pas d'effectuer à nouveau d'autres exigences PCI DSS, mais de confirmer que les activités de sécurité sont effectuées de manière continue.</p> <p><b>Bonne Pratique</b></p> <p>Ces revues peuvent également être utilisées afin de vérifier que les preuves appropriées sont conservées (par exemple, journaux d'audit, rapports d'analyse de vulnérabilités, examens des ensembles de règles de contrôle de sécurité réseau) pour aider l'entité à préparer sa prochaine évaluation de la conformité au standard PCI DSS.</p> <p><b>Exemples</b></p> <p>Prenant l'exigence 1.2.7 comme exemple, on répond à l'exigence 12.4.2 en confirmant, au moins une fois tous les trois mois, que les revues des configurations des mesures de sécurité de sécurité réseau ont eu lieu à la fréquence requise. D'autre part, l'exigence 1.2.7 est satisfaite en examinant ces configurations comme spécifié dans l'exigence.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b>	<b>Procédures de Test de L'approche Définie</b>
<p><b>12.4.2.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les revues effectuées conformément à l'exigence 12.4.2 sont documentées pour inclure :</p> <ul style="list-style-type: none"> <li>• Les résultats des revues.</li> <li>• La documentation des mesures correctives prises pour toutes les tâches qui se sont avérées non exécutées à l'exigence 12.4.2.</li> <li>• Revue et approbation des résultats par le personnel affecté à la responsabilité du programme de conformité PCI DSS.</li> </ul>	<p><b>12.4.2.1 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner la documentation des revues effectuées conformément à l'exigence 12.4.2 du standard PCI DSS afin de vérifier que la documentation comprend tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les conclusions des revues de l'efficacité opérationnelle sont évaluées par la direction ; des mesures correctives appropriées sont mises en œuvre.</p>	<b>Objectif</b> <p>Le but de ces vérifications indépendantes est de confirmer que les activités de sécurité sont exécutées de façon continue. Ces revues peuvent également être utilisées afin de vérifier que les preuves appropriées sont conservées (par exemple, journaux d'audit, rapports d'analyse de vulnérabilités, examens des ensembles de règles de contrôle de sécurité réseau) pour aider l'entité à préparer sa prochaine évaluation de la conformité au standard PCI DSS.</p>
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	

Exigences et Procédures de Test	Directives
<b>12.5 La périphérie du standard PCI DSS est documentée et validée.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.5.1</b> Un inventaire des composants système qui sont dans le périphérie PCI DSS, incluant une description de la fonction ou de l'utilisation, est maintenu et tenu à jour.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.5.1.a</b> Examiner l'inventaire afin de vérifier qu'il comprend tous les composants système concernés et une description de la fonction ou de l'utilisation de chacun.</p> <p><b>12.5.1.b</b> Interroger le personnel afin de vérifier que l'inventaire est tenu à jour.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Tous les composants systèmes concernés par le standard PCI DSS sont identifiés et connus.</p>	<b>Objectif</b> Le maintien d'une liste à jour de tous les composants système permettra à une entreprise de définir le périphérie de son environnement et de mettre en œuvre les exigences du standard PCI DSS avec précision et efficacité. Sans inventaire, certains composants système pourraient être négligés et exclus par mégarde des standards de configuration de l'entreprise. <b>Bonne Pratique</b> Si une entité maintient un inventaire de tous les actifs, les composants systèmes dans le périphérie PCI DSS doivent être clairement identifiables parmi les autres actifs. Les inventaires doivent inclure des conteneurs ou des images pouvant être instanciées. L'affectation d'un propriétaire à l'inventaire permet de s'assurer que l'inventaire reste à jour. <b>Exemples</b> Les méthodes pour maintenir un inventaire comprennent une base de données, une série de fichiers ou un outil de gestion d'inventaire.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.5.2</b> Le périmètre soumis au standard PCI DSS est documenté et confirmé par l'entité au moins une fois tous les 12 mois et en cas de modification importante de l'environnement dans le périmètre. Au minimum, la validation du périmètre comprend :</p> <ul style="list-style-type: none"> <li>• L'identification tous les flux de données pour les différentes étapes de paiement (par exemple, l'autorisation, la capture des règlements, les rétro facturations et les remboursements) et les canaux d'acceptation (par exemple, la carte présente, la carte non présente et le commerce électronique).</li> <li>• La mise à jour tous les diagrammes de flux de données conformément à l'exigence 1.2.4.</li> <li>• L'identification de tous les emplacements où les données de carte sont stockées, traitées et transmises, y compris, sans toutefois s'y limiter : 1) tous les emplacements en dehors du CDE actuellement défini, 2) les applications qui traitent les CHD, 3) les transmissions entre les systèmes et les réseaux, et 4) les sauvegardes de fichiers.</li> <li>• L'identification de tous les composants système dans le CDE, connectés au CDE, ou qui pourraient avoir une incidence sur la sécurité du CDE.</li> <li>• L'identification de tous les mesures de segmentation utilisée et le ou les environnements à partir desquels le CDE est segmenté, y compris la justification des environnements hors de portée.</li> <li>• L'identification de toutes les connexions d'entités tierces ayant accès au CDE.</li> <li>• La confirmation que tous les flux de données identifiés, les données de carte, les composants système, les mesures de segmentation et les connexions de tiers ayant accès au CDE sont inclus dans le périmètre.</li> </ul> <p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.5.2.a</b> Examiner les résultats documentés des revues du périmètre et interroger le personnel afin de vérifier que les revues sont effectuées :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les 12 mois.</li> <li>• Après des modifications importantes de l'environnement dans le périmètre.</li> </ul> <p><b>12.5.2.b</b> Examiner les résultats documentés des examens de la périphérie effectués par l'entité afin de vérifier que l'activité de confirmation du périmètre du standard PCI DSS comporte tous les éléments spécifiés dans cette exigence.</p>	<p><b>Objectif</b></p> <p>La validation fréquente du périmètre PCI DSS permet de garantir que le périmètre PCI DSS reste à jour et aligné sur les objectifs métiers changeants, et donc que les mesures de sécurité de sécurité protègent tous les composants systèmes appropriés.</p> <p><b>Bonne Pratique</b></p> <p>Une délimitation précise implique une évaluation critique du CDE et de tous les composants du système connecté afin de déterminer la couverture nécessaire pour les exigences du standard PCI DSS. Les activités de délimitation, y compris une analyse minutieuse et une surveillance continue, aident à garantir que les systèmes concernés sont correctement sécurisés. Lors de la documentation des emplacements des données de carte, l'entité peut envisager de créer un tableau ou une feuille de calcul contenant les informations suivantes :</p> <ul style="list-style-type: none"> <li>• Les magasins de données (bases de données, fichiers, cloud, etc.), en incluant la finalité du stockage des données et leur durée de rétention,</li> <li>• Quels éléments des CHD sont stockés (PAN, date d'expiration, nom du titulaire de la carte et/ou tout élément des données d'authentification sensibles avant la fin de l'autorisation),</li> <li>• Comment les données sont sécurisées (type de chiffrement et force, algorithme de hachage et force, troncature, tokenisation),</li> <li>• Comment l'accès aux magasins de données est enregistré, y compris une description du ou des mécanismes de journalisation utilisés (solution d'entreprise, niveau de l'application, niveau de système d'exploitation, etc.).</li> </ul> <p><i>(suite à la page suivante)</i></p>

Exigences et Procédures de Test	Directives
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le périmètre de validation au standard PCI DSS est vérifié périodiquement et, après des modifications importantes, par une analyse complète et des mesures techniques appropriées.</p>	<p>En plus des systèmes et réseaux internes, toutes les connexions d'entités tierces ; par exemple, des partenaires commerciaux, des entités fournissant des services d'assistance à distance et d'autres prestataires de services, doivent être identifiées pour déterminer leur inclusion dans le périmètre PCI DSS. Une fois que les connexions concernées ont été identifiées, les mesures de sécurité applicables du standard PCI DSS peuvent être mis en œuvre afin de réduire le risque qu'une connexion tierce soit utilisée pour compromettre le CDE d'une entité.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette confirmation annuelle du périmètre PCI DSS est une activité qui doit être effectuée par l'entité évaluée, et n'est pas la même que, ni se substitue à la confirmation du périmètre effectuée par l'auditeur de l'entité lors de l'évaluation annuelle.</p>	<p>Un outil ou une méthodologie de découverte de données peuvent être utilisés pour faciliter l'identification de toutes les sources et emplacements des PAN, et pour rechercher des PAN qui résident sur des systèmes et des réseaux en dehors du CDE actuellement défini ou dans des endroits inattendus au sein du CDE : par exemple, dans un journal d'erreurs ou un fichier de vidage de la mémoire. Cette approche peut aider à garantir que des emplacements de PAN précédemment inconnus sont détectés et que le PAN est soit éliminé, soit correctement sécurisé.</p> <p><b>Informations Complémentaires</b></p> <p>Pour plus d'informations, se référer au document : <i>Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation</i>.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.5.2.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Le périmètre PCI DSS est documenté et confirmé par l'entité au moins une fois tous les 6 mois et en cas de modification importante de l'environnement dans le périmètre. Au minimum, la validation du périmètre comprend tous les éléments spécifiés dans l'exigence 12.5.2.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.5.2.1.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les résultats documentés des revues du périmètre et interroger le personnel afin de vérifier que des examens selon l'exigence 12.5.2 sont effectués :</p> <ul style="list-style-type: none"> <li>• Au moins une fois tous les six mois, et</li> <li>• Après des modifications importantes</li> </ul>
<b>Objectif de L'approche Personnalisée</b> <p>L'exactitude du périmètre PCI DSS est vérifiée en permanence par une analyse complète et des mesures techniques appropriées.</p>	<p><b>12.5.2.1.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les résultats documentés des revues du périmètre afin de vérifier que la validation du périmètre comporte tous les éléments spécifiés dans l'exigence 12.5.2.</p>
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> <p>Les prestataires de services ont généralement accès à de plus grands volumes de données de titulaires de carte que les commerçants ou peuvent fournir un point d'entrée qui peut être exploité pour ensuite compromettre plusieurs autres entités. En général, les prestataires de services ont également des réseaux plus grands et plus complexes qui sont sujets à des modifications plus fréquentes. La probabilité de modifications de la périmètre ignorées dans les réseaux complexes et dynamiques est plus élevée dans les environnements des prestataires de services.</p> <p>La validation plus fréquente du périmètre PCI DSS est susceptible de découvrir ces modifications négligées avant qu'elles ne puissent être exploitées par un attaquant.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.5.3 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les modifications importantes apportées à la structure de l'entreprise entraînent un examen documenté (interne) de l'impact sur le périmètre PCI DSS et l'applicabilité des mesures de sécurité, les résultats étant communiqués à la direction générale.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.5.3.a Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis de sorte qu'une modification importante de la structure de l'entreprise entraîne un examen documenté de l'impact sur le périmètre PCI DSS et l'applicabilité des mesures de sécurité.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le périmètre PCI DSS est confirmé après une modification organisationnelle importante.</p>	<p><b>12.5.3.b Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner la documentation (par exemple, les procès-verbaux des réunions) et interroger le personnel responsable afin de vérifier que les modifications importantes apportées à la structure de l'entreprise ont donné lieu à des examens documentés comprenant tous les éléments spécifiés dans cette exigence, les résultats étant communiqués à la direction générale.</p>
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Objectif</b> La structure et la gestion d'une entreprise définissent les exigences et le protocole pour des opérations efficaces et sécurisées. Les modifications apportées à cette structure pourraient avoir des effets négatifs sur les mesures de sécurité et les cadres existants en réaffectant ou en supprimant des ressources qui prenaient autrefois en charge les mesures de sécurité liée au standard PCI DSS, ou en héritant de nouvelles responsabilités pour lesquelles des mesures de sécurité n'ont peut-être pas encore été établies. Par conséquent, il est important de revoir le périmètre et les mesures de sécurité en place pour PCI DSS lorsque des modifications sont apportées à la structure et à la gestion d'une entreprise afin de s'assurer que les mesures sont en place et actives. <b>Exemples</b> Les modifications apportées à la structure de l'entreprise comprennent, sans toutefois s'y limiter, les fusions ou acquisitions d'entreprises et les modifications ou réaffectations importantes du personnel responsable des mesures de sécurité de sécurité.

Exigences et Procédures de Test	Directives
<b>12.6 La sensibilisation à la sécurité est une activité continue.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.6.1</b> Un programme formel de sensibilisation à la sécurité est mis en œuvre pour informer tout le personnel de la politique et des procédures de sécurité des informations de l'entité, ainsi que de son rôle dans la protection des données des titulaires de cartes.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.6.1</b> Examiner le programme de sensibilisation à la sécurité afin de vérifier qu'il sensibilise tout le personnel à la politique et aux procédures de sécurité des informations de l'entité, ainsi qu'au rôle du personnel dans la protection des données des porteurs de cartes.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le personnel est informé le paysage des menaces, sa responsabilité dans le fonctionnement des mesures de sécurité pertinentes et est en mesure d'accéder à une assistance et à des conseils en cas de besoin.</p>	<b>Objectif</b> <p>Si le personnel n'est pas informé des politiques et procédures de sécurité des informations de son entreprise et de ses propres responsabilités en matière de sécurité, les mesures de sécurité et les procédures qui ont été mises en œuvre peuvent devenir inefficaces en raison d'erreurs involontaires ou d'actions intentionnelles.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.6.2</b> Le programme de sensibilisation à la sécurité est :</p> <ul style="list-style-type: none"> <li>• Revu au moins une fois tous les 12 mois.</li> <li>• Mis à jour si nécessaire pour prendre en compte toute nouvelle menace et vulnérabilité susceptible d'avoir une incidence sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles de l'entité, ou les informations fournies au personnel concernant son rôle dans la protection des données des porteurs de cartes.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.6.2</b> Examiner le contenu du programme de sensibilisation à la sécurité, les preuves des revues et interroger le personnel afin de vérifier que le programme de sensibilisation à la sécurité est conforme à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le contenu du support de sensibilisation à la sécurité est révisé et mis à jour périodiquement.</p>	<p><b>Objectif</b></p> <p>L'environnement des menaces et les défenses d'une entité ne sont pas statiques. A ce titre, les supports du programme de sensibilisation à la sécurité doivent être mis à jour aussi souvent que nécessaire afin de garantir que la formation reçue par le personnel est à jour et représente l'environnement actuel des menaces.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.6.3</b> Le personnel reçoit une formation de sensibilisation à la sécurité comme suit :</p> <ul style="list-style-type: none"> <li>• À l'embauche et au moins une fois tous les 12 mois.</li> <li>• Plusieurs méthodes de communication sont utilisées.</li> <li>• Le personnel confirme au moins une fois tous les 12 mois avoir lu et compris la politique et les procédures de sécurité des informations.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.6.3.a</b> Examiner les éléments du programme de sensibilisation à la sécurité afin de vérifier que le personnel suit une formation de sensibilisation à la sécurité lors de son embauche et au moins une fois tous les 12 mois.</p> <p><b>12.6.3.b</b> Examiner les supports du programme de sensibilisation à la sécurité afin de vérifier que le programme comprend plusieurs méthodes de communication de la sensibilisation et de la formation du personnel.</p> <p><b>12.6.3.c</b> Interroger le personnel afin de vérifier qu'il a suivi une formation de sensibilisation et qu'il est conscient de son rôle dans la protection des données des titulaires de cartes.</p> <p><b>12.6.3.d</b> Examiner les documents du programme de sensibilisation à la sécurité et les confirmations du personnel afin de vérifier que le personnel confirme au moins une fois tous les 12 mois avoir lu et compris la politique et les procédures de sécurité des informations.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Le personnel demeure informé du paysage des menaces, de sa responsabilité dans le fonctionnement des mesures de sécurité pertinentes et est en mesure d'accéder à une assistance et à des conseils en cas de besoin.</p>	<p><b>Objectif</b> La formation du personnel assure que celui-ci reçoit les informations sur l'importance de la sécurité des informations et qu'il comprend son rôle dans la protection de l'entreprise.</p> <p><b>Bonne Pratique</b> Les entités peuvent intégrer la formation des nouveaux employés dans le cadre du processus d'intégration des ressources humaines. La formation doit décrire les « faire » et les « ne pas faire » liés à la sécurité. Une formation de recyclage périodique renforce les processus et procédures de sécurité clés qui pourraient être oubliés ou contournés.</p> <p>Les entités doivent envisager d'exiger une formation de sensibilisation à la sécurité chaque fois que du personnel est transféré dans des rôles où ils peuvent avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles à partir de rôles alors qu'ils n'avaient pas cet impact.</p> <p>Les méthodes et le contenu de la formation peuvent varier en fonction des rôles des membres du personnel.</p> <p><b>Exemples</b> Les différentes méthodes qui peuvent être utilisées pour fournir une sensibilisation et une éducation à la sécurité comprennent des affiches, des lettres, une formation sur le Web, une formation en présentiel, des réunions d'équipe et des incitations.</p> <p>Les confirmations du personnel peuvent être consignées par écrit ou par voie électronique.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.6.3.1</b> La formation de sensibilisation à la sécurité comprend la sensibilisation aux menaces et aux vulnérabilités qui pourraient avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• L'hameçonnage et attaques associées.</li> <li>• L'ingénierie sociale.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Le personnel est conscient de ses propres vulnérabilités humaines et la façon dont les acteurs de la menace tenteront d'exploiter de telles vulnérabilités. Le personnel peut accéder à une assistance et à des conseils en cas de besoin.</p> <p><b>Notes D'applicabilité</b></p> <p>Voir l'exigence 5.4.1 pour des conseils sur la différence entre les mesures de sécurité techniques et automatisés pour détecter et protéger les utilisateurs contre les attaques d'hameçonnage, et cette exigence pour fournir aux utilisateurs une formation de sensibilisation à la sécurité sur l'hameçonnage et l'ingénierie sociale. Ce sont deux exigences séparées et distinctes, et l'une n'est pas satisfaite par la mise en œuvre des mesures de sécurité requis par l'autre.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.6.3.1</b> Examiner le contenu de la formation de sensibilisation à la sécurité afin de vérifier qu'il inclut tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>Éduquer le personnel sur la façon de détecter, de réagir et de signaler les attaques potentielles d'hameçonnage et les attaques connexes, ainsi que les tentatives d'ingénierie sociale est essentiel pour minimiser la probabilité d'une attaque réussie.</p> <p><b>Bonne Pratique</b></p> <p>Un programme efficace de sensibilisation à la sécurité doit inclure des exemples de courriels d'hameçonnage et des tests périodiques afin de déterminer une grande prévalence de personnel signalant de telles attaques. Le support de formation qu'une entité peut envisager pour ce sujet comprend :</p> <ul style="list-style-type: none"> <li>• Comment identifier les attaques d'hameçonnage et autres attaques d'ingénierie sociale.</li> <li>• Comment réagir en cas de soupçon d'hameçonnage et d'ingénierie sociale.</li> <li>• Où et comment signaler une activité suspectée d'hameçonnage et d'ingénierie sociale.</li> </ul> <p>L'accent mis sur le signalement permet à l'entreprise de récompenser les comportements positifs, d'optimiser les défenses techniques (voir l'exigence 5.4.1) et de prendre des mesures immédiates pour supprimer les courriels d'hameçonnage similaires qui ont échappé aux défenses techniques des boîtes de réception des destinataires.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.6.3.2</b> La formation de sensibilisation à la sécurité comporte la sensibilisation à l'utilisation acceptable des technologies de l'utilisateur final conformément à l'exigence 12.2.1.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.6.3.2</b> Examiner le contenu de la formation de sensibilisation à la sécurité afin de vérifier qu'il comprend une sensibilisation à l'utilisation acceptable des technologies de l'utilisateur final conformément à l'exigence 12.2.1.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le personnel au courant de sa responsabilité en matière de sécurité et d'utilisation des technologies de l'utilisateur final et est en mesure d'accéder à de l'aide et à des conseils en cas de besoin.</p>	<b>Objectif</b> En incluant les points clés de la politique d'utilisation acceptable dans la formation régulière et le contexte associé, le personnel comprendra ses responsabilités et leur incidence sur la sécurité des systèmes d'une entreprise.
<b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<b>12.7 Le personnel est contrôlé afin de réduire les risques d'attaques internes.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.7.1</b> Le candidat à l'embauche qui aura accès au CDE fait l'objet d'une vérification des antécédents, dans les limites des lois locales, avant l'embauche afin de minimiser le risque d'attaques provenant de sources internes.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.7.1</b> Interroger la direction responsable du service des ressources humaines afin de vérifier que la sélection est effectuée, dans les limites des lois locales, avant d'embaucher du personnel potentiel qui aura accès au CDE.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le risque lié à l'accès des nouveaux membres du personnel au CDE est compris et maîtrisé.</p>	
<b>Notes D'applicabilité</b> <p>Pour le personnel potentiel à embaucher pour des postes tels que les caissiers de magasin, qui n'ont accès qu'à un seul numéro de carte à la fois lors de la facilitation d'une transaction, cette exigence n'est qu'une recommandation.</p>	<b>Objectif</b> <p>Une sélection approfondie avant l'embauche de personnel potentiel qui devrait avoir accès au CDE fournit aux entités les informations nécessaires pour prendre des décisions éclairées en matière de risque concernant le personnel qu'elles embauchent et qui aura accès au CDE.</p> <p>Parmi les autres avantages de la sélection du personnel potentiel, citons la garantie de la sécurité sur le lieu de travail et la confirmation des informations fournies par les employés potentiels sur leur CV.</p> <b>Bonne Pratique</b> <p>Les entités doivent envisager d'effectuer une vérification du personnel existant chaque fois qu'il est transféré dans des rôles où il a accès au CDE à partir de rôles où il n'avait pas cet accès.</p> <p>Pour être efficace, le niveau de sélection doit être adapté au poste. Par exemple, les postes nécessitant une plus grande responsabilité ou qui ont un accès administratif aux données ou systèmes critiques peuvent justifier une vérification plus détaillée ou plus fréquente que les postes avec moins de responsabilité et d'accès.</p> <b>Exemples</b> <p>Les options de vérification peuvent inclure, selon la région de l'entité, les antécédents professionnels, l'examen des informations publiques ou les ressources de médias sociaux, le casier judiciaire, les antécédents de crédit et la vérification des références.</p>

Exigences et Procédures de Test	Directives
<b>12.8 Le risque pour les fonds documentaires associés aux relations avec les prestataires de services tiers (TPSP) est géré.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.8.1</b> Une liste de tous les prestataires de services tiers (TPSP) avec lesquels les données de carte sont partagées ou qui pourraient affecter la sécurité des données de carte, comprenant une description pour chacun des services fournis est maintenue.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.8.1.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour maintenir une liste des TPSP, avec une description pour chacun des services fournis, pour tous les TPSP avec lesquels les données de carte sont partagées ou qui pourraient affecter la sécurité des données de carte.</p> <p><b>12.8.1.b</b> Examiner la documentation afin de vérifier qu'une liste de tous les TPSP est maintenue et qu'elle comprend une description des services fournis.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Des enregistrements sur les TPSP et les services fournis sont maintenus.</p>	
<b>Notes D'applicabilité</b> <p>L'utilisation d'un TPSP conforme au standard PCI DSS ne rend pas une entité conforme au standard PCI DSS, ni ne supprime la responsabilité de l'entité quant à sa propre conformité au standard PCI DSS.</p>	<b>Objectif</b> La tenue à jour d'une liste de tous les TPSP identifie où le risque potentiel s'étend à l'extérieur de l'entreprise et définit la surface d'attaque étendue de l'entreprise. <b>Exemples</b> Les différents types de TPSP comprennent ceux qui : <ul style="list-style-type: none"> <li>Stockent, traitent ou transmettent les données de carte au nom de l'entité (telles que les passerelles de paiement, les processeurs de paiement, les prestataires de services de paiement (PSP) et les fournisseurs de stockage hors site).</li> <li>Gèrent les composants système inclus dans l'évaluation de la conformité au standard PCI DSS de l'entité (tels que les fournisseurs de services liés aux mesures de la sécurité réseau, les services anti-programmes malveillants et la gestion des incidents et des événements de sécurité (SIEM) ; les centres de contact et d'appel ; les sociétés d'hébergement Web ; et les fournisseurs de services cloud IaaS, PaaS, SaaS et FaaS).</li> <li>Pourraient avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles de l'entité (comme les prestataires fournissant une assistance via un accès à distance et les développeurs de logiciels faits sur mesure).</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.8.2</b> Les accords écrits avec les TPSP sont maintenus comme suit :</p> <ul style="list-style-type: none"> <li>Des accords écrits sont maintenus avec tous les TPSP avec lesquels les données de carte sont partagées ou qui pourraient avoir une incidence sur la sécurité du CDE.</li> <li>Les accords écrits comprennent des reconnaissances des TPSP que les TPSP sont responsables de la sécurité des données de carte que les TPSP possèdent ou autrement stockent, traitent ou transmettent au nom de l'entité, ou dans la mesure où les TPSP pourraient avoir un impact sur la sécurité des données des titulaires de carte et/ou des données d'authentification sensibles de l'entité.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.8.2.a</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour maintenir des accords écrits avec tous les TPSP conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>12.8.2.b</b> Examiner les accords écrits avec les TPSP afin de vérifier qu'ils sont maintenus conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des enregistrements sont conservés de la reconnaissance par chaque TPSP de sa responsabilité de protéger les données de carte.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>La confirmation écrite d'un TPSP démontre son engagement à maintenir une sécurité adéquate des données de carte qu'il obtient de ses clients et que le TPSP est pleinement conscient des actifs qui pourraient être affectés lors de la prestation du service du TPSP. La mesure dans laquelle un TPSP spécifique est responsable de la sécurité des données de carte dépendra du service fourni et des responsabilités convenues entre le prestataire et l'entité évaluée (le consommateur).</p> <p>Conjointement avec l'exigence 12.9.1, cette exigence vise à promouvoir un niveau cohérent de compréhension entre les parties concernant leurs responsabilités liées au standard PCI DSS qui s'appliquent à eux. Par exemple, l'accord peut inclure les exigences applicables du standard PCI DSS à maintenir dans le cadre du service fourni.</p> <p><b>Bonne Pratique</b></p> <p>L'entité peut également envisager d'inclure dans son accord écrit avec un TPSP que le TPSP soutiendra la demande d'informations de l'entité conformément à l'exigence 12.9.2. Les entités devront également comprendre si des TPSP ont des relations « imbriquées » avec d'autres TPSP, ce qui signifie que le TPSP principal passe des contrats avec un ou plusieurs autres TPSP dans le but de fournir un service.</p> <p>Il est important de comprendre si le TPSP principal s'appuie sur le ou les TPSP secondaires pour assurer la conformité globale d'un service, et les types d'accords écrits que le TPSP principal a mis en place avec les TPSP secondaires. Les entités peuvent envisager d'inclure dans leur accord écrit la couverture de tout TPSP « imbriqué » qu'un TPSP principal peut utiliser.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>La formulation exacte d'un accord dépendra des détails du service fourni et des responsabilités attribuées à chaque partie. L'accord n'a pas à inclure la formulation exacte fournie dans cette exigence.</p> <p>La reconnaissance écrite du TPSP est une confirmation qui déclare que le TPSP est responsable de la sécurité des données de carte qu'il peut stocker, traiter ou transmettre au nom du client ou dans la mesure où le TPSP peut avoir un impact sur la sécurité des données du titulaire de carte d'un client et/ ou des données d'authentification sensibles.</p> <p>La preuve qu'un TPSP respecte les exigences du standard PCI DSS n'est pas la même chose qu'une reconnaissance écrite spécifiée dans cette exigence. Par exemple, une attestation de conformité PCI DSS (AOC), une déclaration sur le site Web d'une entreprise, une déclaration de politique, une matrice de responsabilité ou toute autre preuve non incluse dans un accord écrit ne constitue pas une reconnaissance écrite.</p>	<p><b>Informations Complémentaires</b></p> <p>Se référer au document : « <i>Information Supplement: Third-Party Security Assurance</i> for further guidance. »</p>

Exigences et Procédures de Test	Directives
<b>Exigences de l'approche définie</b> <p><b>12.8.3</b> Un processus établi est mis en œuvre pour engager les TPSP, y compris des mesures de sécurité préalables appropriés avant l'engagement.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.8.3.a</b> Examiner les politiques et procédures afin de vérifier que les processus sont définis pour engager les TPSP, y compris des mesures de sécurité préalables appropriés avant l'engagement.</p> <p><b>12.8.3.b</b> Examiner les preuves et interroger le personnel responsable afin de vérifier que le processus d'engagement des TPSP comporte des mesures de sécurité préalables appropriés avant l'engagement.</p>
<b>Objectif de L'approche Personnalisée</b> <p>La capacité, l'intention et les ressources d'un TPSP potentiel pour protéger adéquatement les données de carte sont évaluées avant que le TPSP ne soit engagé.</p>	<b>Objectif</b> Un processus approfondi d'engagement des TPSP, comprenant les détails de la sélection et de la vérification avant l'engagement, permet de garantir qu'un TPSP est soigneusement vérifié en interne par une entité avant d'établir une relation formelle et que le risque pour les données des porteurs de cartes associé à l'engagement du TPSP est compris. <b>Bonne Pratique</b> Les processus et les objectifs spécifiques des mesures de sécurité préalables varieront pour chaque entreprise. Les éléments à prendre en compte comportent les pratiques de signalement du prestataire, les procédures de notification de violation et de réponse aux incidents, les détails de la manière dont les responsabilités liées au standard PCI DSS sont attribuées entre chaque partie prenante, la manière dont le TPSP valide sa conformité au standard PCI DSS et les preuves qu'il fournit.

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.8.4</b> Un programme est mis en œuvre pour surveiller l'état de conformité au standard PCI DSS des TPSP au moins une fois tous les 12 mois.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.8.4.a</b> Examiner les politiques et procédures afin de vérifier que les processus sont définis pour surveiller l'état de conformité au standard PCI DSS des TPSP au moins une fois tous les 12 mois.</p> <p><b>12.8.4.b</b> Examiner la documentation et interroger le personnel responsable afin de vérifier que l'état de conformité au standard PCI DSS de chaque TPSP est contrôlé au moins une fois tous les 12 mois.</p>
<b>Objectif de L'approche Personnalisée</b> <p>L'état de conformité au standard PCI DSS des TPSP est vérifié périodiquement.</p>	<b>Objectif</b> Connaître l'état de conformité au standard PCI DSS de tous les TPSP engagés fournit l'assurance et la conscience quant à savoir s'ils se conforment aux exigences applicables aux services qu'ils offrent à l'entreprise. <b>Bonne Pratique</b> Si le TPSP offre une variété de services, l'état de conformité que l'entité surveille doit être spécifique aux services fournis à l'entité et aux services couverts par l'évaluation du standard PCI DSS de l'entité. Si un TPSP détient une attestation de conformité au standard PCI DSS (AOC), on s'attend à ce que le TPSP la fournit aux clients sur demande pour démontrer leur statut de conformité au standard PCI DSS.
<b>Notes D'applicabilité</b> <p>Lorsqu'une entité passe un accord avec un TPSP pour satisfaire aux exigences du standard PCI DSS au nom de l'entité (par exemple, via un service de pare-feu), l'entité doit travailler avec le TPSP pour s'assurer que les exigences applicables du standard PCI DSS sont satisfaites. Si le TPSP ne satisfait pas aux exigences applicables du standard PCI DSS, ces exigences ne sont pas non plus « en place » chez l'entité.</p>	<b>Informations Complémentaires</b> Pour plus d'informations sur les prestataires de services tiers, consulter : <ul style="list-style-type: none"> <li>• La section du standard PCI DSS : <i>Use of Third-Party Service Providers</i>.</li> <li>• <i>Information Supplement: Third-Party Security Assurance</i>.</li> </ul>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.8.5</b> Des informations sont conservées sur les exigences du standard PCI DSS qui sont gérées par chaque TPSP, celles qui sont gérées par l'entité et celles qui sont partagées entre le TPSP et l'entité.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.8.5.a</b> Examiner les politiques et procédures afin de vérifier que les processus sont définis pour conserver des informations sur les exigences du standard PCI DSS qui sont gérées par chaque TPSP, celles qui sont gérées par l'entité et celles qui sont partagées entre le TPSP et l'entité.</p> <p><b>12.8.5.b</b> Examiner la documentation et interroger le personnel afin de vérifier que l'entité conserve des informations sur les exigences du standard PCI DSS qui sont gérées par chaque TPSP, celles qui sont gérées par l'entité et celles qui sont partagées entre les deux entités.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Des enregistrements détaillant les exigences du standard PCI DSS et les composants systèmes associés dont chaque TPSP est seul ou conjointement responsable sont conservés et révisés périodiquement.</p>	<p><b>Objectif</b> Il est important que l'entité comprenne les exigences et sous-exigences du standard PCI DSS que ses TPSP ont accepté de respecter, les exigences qui sont partagées entre le TPSP et l'entité, et pour celles qui sont partagées, des détails sur la façon dont les exigences sont partagées et l'entité qui est responsable de satisfaire à chaque sous-exigence. Sans cette compréhension commune, il est inévitable que l'entité et le TPSP supposent qu'une sous-exigence donnée du standard PCI DSS relève de la responsabilité de l'autre partie, et par conséquent, cette sous-exigence peut ne pas être traitée du tout. Les informations spécifiques qu'une entité conserve dépendent de l'accord particulier passé avec ses prestataires, du type de service, etc. Les TPSP peuvent définir leurs responsabilités du standard PCI DSS comme étant les mêmes pour tous leurs clients ; sinon, cette responsabilité doit être convenue à la fois par l'entité et le TPSP.</p> <p><b>Bonne Pratique</b> Les entités peuvent documenter ces responsabilités via une matrice qui identifie toutes les exigences applicables du standard PCI DSS et indique pour chaque exigence si l'entité ou le TPSP est responsable du respect de cette exigence ou s'il s'agit d'une responsabilité partagée. Ce type de document est souvent appelé <i>matrice de responsabilité</i>. (suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Il est également important que les entités comprennent si des TPSP ont des relations « imbriquées » avec d'autres TPSP, ce qui signifie que le TPSP principal passe des contrats avec un ou plusieurs autres TPSP aux fins de fournir un service. Il est important de comprendre si le TPSP principal s'appuie sur le ou les TPSP secondaires pour assurer la conformité globale d'un service, et comment le TPSP principal surveille les performances du service et l'état de conformité du standard PCI DSS du ou des TPSP secondaires. À noter qu'il est de la responsabilité du TPSP principal de gérer et de surveiller tout TPSP secondaire.</p> <p><b>Informations Complémentaires</b></p> <p>Se référer au document <i>Information Supplement: Third-Party Security Assurance</i> pour un exemple de modèle de matrice de responsabilité.</p>

Exigences et Procédures de Test	Directives
<b>12.9 Les prestataires de services tiers (TPSP) prennent en charge la conformité du standard PCI DSS de leurs clients.</b>	
<b>Exigences de L'approche Définie</b> <p><b>12.9.1 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les TPSP fournissent aux clients un accord écrit qui comporte la reconnaissance que les TPSP sont responsables de la sécurité des données de carte que le TPSP possède ou autrement stocke, traite ou transmet au nom du consommateur, ou dans la mesure où les TPSP pourraient avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles du consommateur.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.9.1 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les politiques, les procédures et les modèles du TPSP utilisés pour les accords écrits afin de vérifier que les processus sont définis pour que le TPSP fournit des confirmations écrites aux clients conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les TPSP reconnaissent officiellement leurs responsabilités en matière de sécurité envers leurs clients.</p>	<b>Objectif</b> <p>Conjointement avec l'exigence 12.8.2, cette exigence vise à promouvoir un niveau constant de compréhension entre les TPSP et leurs clients concernant leurs responsabilités applicables du standard PCI DSS. La reconnaissance de la part des TPSP témoigne de leur engagement à maintenir une sécurité adéquate des données de carte qu'ils obtiennent de leurs clients.</p> <p>Les politiques et procédures internes du TPSP liées à leur processus d'engagement client et tous les modèles utilisés pour les accords écrits doivent inclure la fourniture à ses clients d'un accusé de réception PCI DSS applicable.</p> <p>La méthode par laquelle le TPSP fournit une confirmation écrite doit être convenue entre le prestataire et ses clients.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>La formulation exacte d'un accord dépendra des détails du service fourni et des responsabilités attribuées à chaque partie. L'accord n'a pas à inclure la formulation exacte fournie dans cette exigence.</p> <p>La reconnaissance écrite du TPPS est une confirmation qui déclare que le TPPS est responsable de la sécurité des données de compte qu'il peut stocker, traiter ou transmettre au nom du client ou dans la mesure où le TPPS peut avoir un impact sur la sécurité des données du titulaire de carte d'un client et/ou des données d'authentification sensibles.</p> <p>La preuve qu'un TPPS répond aux exigences du standard PCI DSS n'est pas la même chose qu'un accord écrit spécifié dans cette exigence. Par exemple, une attestation de conformité PCI DSS (AOC), une déclaration sur le site Web d'une entreprise, une déclaration de politique, une matrice de responsabilité ou toute autre preuve non incluse dans un accord écrit ne constitue pas une reconnaissance écrite.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.9.2 Exigences supplémentaires pour les prestataires de services uniquement :</b> Les TPSP prennent en charge les demandes d'informations de leurs clients pour répondre aux exigences 12.8.4 et 12.8.5 en fournissant, à la demande du consommateur, ce qui suit :</p> <ul style="list-style-type: none"> <li>Des informations sur l'état de conformité au standard PCI DSS (exigence 12.8.4).</li> <li>Des informations sur les exigences du standard PCI DSS qui relèvent de la responsabilité du TPSP et celles qui relèvent de la responsabilité du consommateur, y compris toute responsabilité partagée (exigence 12.8.5), pour tout service fourni par le TPSP qui répond à une ou plusieurs exigences PCI DSS au nom des clients ou qui peut avoir un impact sur la sécurité des données de titulaire de carte des clients et/ou des données d'authentification sensibles.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les TPSP fournissent les informations nécessaires pour soutenir les efforts de conformité au standard PCI DSS de leurs clients.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.9.2 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les politiques et les procédures afin de vérifier que les processus sont définis pour les TPSP pour prendre en charge la demande d'informations des clients pour répondre aux exigences 12.8.4 et 12.8.5 conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>Si un TPSP ne fournit pas les informations nécessaires pour permettre à ses clients de répondre à leurs exigences de sécurité et de conformité, les clients ne seront pas en mesure de protéger les données des titulaires de cartes ni de respecter leurs propres obligations contractuelles.</p> <p><b>Bonne Pratique</b></p> <p>Si un TPSP détient une attestation de conformité au standard PCI DSS (AOC), on s'attend à ce que le TPSP la fournis aux clients sur demande pour démontrer leur statut de conformité au standard PCI DSS.</p> <p>Si le TPSP n'a pas subi d'évaluation du standard PCI DSS, il peut être en mesure de fournir d'autres preuves suffisantes pour démontrer qu'il a satisfait aux exigences applicables sans subir de validation formelle de conformité. Par exemple, le TPSP peut fournir des preuves spécifiques à l'auditeur de l'entité afin qu'il puisse confirmer que les exigences applicables sont satisfaites. Alternativement, le TPSP peut choisir de subir plusieurs évaluations à la demande par chacun des auditeurs de ses clients, chaque évaluation visant à confirmer que les exigences applicables sont satisfaites.</p> <p>Les TPSP sont tenus de fournir des preuves suffisantes à leurs clients afin de vérifier que le périmètre de l'évaluation PCI DSS du TPSP a couvert les services applicables au consommateur, et que les exigences PCI DSS pertinentes ont été examinées et qu'il a été déterminé qu'elles sont en place.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p>Les TPSP peuvent définir leurs responsabilités liées au standard PCI DSS comme étant les mêmes pour tous leurs clients ; sinon, cette responsabilité doit être convenue entre le consommateur et le TPSP. Il est important que le consommateur comprenne les exigences et sous-exigences du standard PCI DSS que ses TPSP ont accepté de respecter, les exigences qui sont partagées entre le TPSP et le consommateur, et pour celles qui sont partagées, des détails sur la façon dont les exigences sont partagées et l'entité qui est responsable de satisfaire à chaque sous-exigence. Un exemple de la manière de documenter ces responsabilités via une matrice qui identifie toutes les exigences applicables du standard PCI DSS et indique si le consommateur ou le TPSP est responsable du respect de cette exigence ou s'il s'agit d'une responsabilité partagée.</p> <p><b>Informations Complémentaires</b></p> <p>Pour plus d'informations, se référer à :</p> <ul style="list-style-type: none"> <li>• La section du standard PCI DSS : Utilisation de prestataires de services tiers.</li> <li>• <i>Information Supplement: Third-Party Security Assurance</i> (comprend un modèle de matrice de responsabilité)</li> </ul>

Exigences et Procédures de Test	Directives
<b>12.10 Les incidents de sécurité soupçonnés et confirmés qui pourraient avoir un impact sur le CDE sont traités immédiatement.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.10.1</b> Un plan de réponse aux incidents existe et est prêt à être activé en cas d'incident de sécurité soupçonné ou avéré. Le plan comprend, mais n'est pas limité à :</p> <ul style="list-style-type: none"> <li>• Les rôles, responsabilités et stratégies de communication et de contact en cas d'incident de sécurité soupçonné ou avéré, y compris la notification des marques de cartes de paiement et des acquéreurs, au minimum.</li> <li>• Les procédures de réponse aux incidents avec des activités de confinement et d'atténuation spécifiques pour différents types d'incidents.</li> <li>• Les procédures de reprise et de continuité de l'activité.</li> <li>• Les processus de sauvegarde des données.</li> <li>• L'analyse des exigences légales en matière de signalement des compromissions.</li> <li>• La couverture et les réponses de tous les composants critiques du système.</li> <li>• La référence ou l'inclusion des procédures de réponse aux incidents des marques de carte paiement.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.1.a</b> Examiner le plan de réponse aux incidents afin de vérifier que le plan existe et comporte au moins les éléments spécifiés dans cette exigence.</p> <p><b>12.10.1.b</b> Interroger le personnel et examiner la documentation des incidents ou alertes précédemment signalés afin de vérifier que le plan et les procédures documentés de réponse aux incidents ont été suivis.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Un plan complet de réponse aux incidents qui répond aux attentes de la marque de carte est maintenu.</p>	<p><b>Objectif</b></p> <p>Sans un plan complet de réponse aux incidents qui est correctement diffusé, lu et compris par les parties responsables, la confusion et l'absence d'une réponse cohérente pourraient créer des temps d'arrêt supplémentaires pour l'entreprise, une exposition inutile aux médias publics, ainsi qu'un risque de perte financière et/ou de réputation et de responsabilités légales.</p> <p><b>Bonne Pratique</b></p> <p>Le plan de réponse aux incidents doit être complet et contenir tous les éléments clés pour les parties prenantes (par exemple, les aspects juridiques, les communications) afin de permettre à l'entité de réagir efficacement en cas de violation susceptible d'affecter les données de carte. Il est important de maintenir le plan à jour avec les coordonnées actuelles de toutes les personnes désignées comme ayant un rôle à jouer dans la réponse aux incidents. D'autres parties concernées par les notifications peuvent inclure les clients, les institutions financières (acquéreurs et émetteurs) et les partenaires commerciaux.</p> <p>Les entités doivent prendre en considération la manière de traiter toutes les compromissions de données au sein du CDE dans leurs plans de réponse aux incidents, y compris les mises en péril des données de carte, des clés de chiffrement sans fil, des clés de chiffrement utilisées pour la transmission et le stockage ou les données de carte ou les données de titulaires de cartes, etc.</p> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<p><b>Exemples</b>            Les exigences légales en matière de signalement des compromissions comportent celles de la plupart des États américains, le règlement général sur la protection des données (RGPD) de l'UE et la loi sur la protection des données personnelles (Singapour).</p> <p><b>Informations Complémentaires</b>            Pour plus d'informations, se référer au document NIST SP 800-61 Rev. 2, <i>Computer Security Incident Handling Guide</i>.</p>
<p><b>Exigences de l'approche définie</b></p> <p><b>12.10.2</b> Au moins une fois tous les 12 mois, le plan de réponse aux incidents de sécurité est :</p> <ul style="list-style-type: none"> <li>• Revu et le contenu est mis à jour si besoin.</li> <li>• Testé, en incluant tous les éléments énumérés à l'exigence 12.10.1.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Le plan de réponse aux incidents est tenu à jour et testé périodiquement.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.2</b> Interroger le personnel et examiner la documentation afin de vérifier qu'au moins une fois tous les 12 mois, le plan de réponse aux incidents de sécurité est :</p> <ul style="list-style-type: none"> <li>• Examiné et mis à jour au besoin.</li> <li>• Testé, en incluant tous les éléments énumérés à l'exigence 12.10.1.</li> </ul> <p><b>Objectif</b>            Des tests appropriés du plan de réponse aux incidents de sécurité peuvent identifier les processus métier défectueux et garantir que les étapes clés ne sont pas ignorées, ce qui pourrait entraîner une exposition accrue lors d'un incident. Des tests périodiques du plan garantissent que les processus restent viables et, de même, garantissent que tout le personnel concerné de l'entreprise connaît le plan.</p> <p><b>Bonne Pratique</b>            Le test du plan de réponse aux incidents peut inclure des incidents simulés et les réponses correspondantes sous forme d'un « exercice sur table », qui comporte la participation du personnel concerné. Une revue de l'incident et de la qualité de la réponse peut fournir aux entités l'assurance que tous les éléments requis sont inclus dans le plan.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.10.3</b> Du personnel spécifique est désigné pour être disponible 24h/24 et 7j/7 pour répondre aux incidents de sécurité soupçonnés ou avérés.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les incidents sont traités immédiatement, comme il se doit.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.3</b> Examiner la documentation et interroger le personnel responsable occupant les rôles désignés afin de vérifier que le personnel spécifique est désigné pour être disponible 24h/24 et 7j/7 pour répondre aux incidents de sécurité.</p> <p><b>Objectif</b> Un incident peut survenir à tout moment. Par conséquent, si une personne formée à la réponse aux incidents et familiarisée avec le plan de l'entité est disponible lorsqu'un incident est détecté, la capacité de l'entité à réagir correctement à l'incident est augmentée.</p> <p><b>Bonne Pratique</b> Souvent, du personnel spécifique est désigné pour faire partie d'une équipe de réponse aux incidents de sécurité, l'équipe ayant la responsabilité globale de répondre aux incidents (peut-être selon un calendrier tournant) et de gérer ces incidents conformément au plan. L'équipe d'intervention en cas d'incident peut être composée de membres principaux qui sont affectés en permanence ou de personnel « à la demande » qui peut être appelé si nécessaire, en fonction de leur expertise et des spécificités de l'incident.</p> <p>Avoir des ressources disponibles pour répondre rapidement aux incidents minimise les perturbations pour l'entreprise.</p> <p>Les exemples de types d'activités auxquelles l'équipe ou les individus doivent répondre comportent toute preuve d'activité non autorisée, la détection de points d'accès sans fil non autorisés, les alertes IDS critiques et les rapports de modifications critiques non autorisées du système ou des fichiers de contenu.</p>

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>12.10.4</b> Le personnel chargé de répondre aux incidents de sécurité soupçonnés et avérés est formé de manière appropriée et périodique sur ses responsabilités en matière de réponse aux incidents.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.10.4</b> Examiner la documentation de formation et interroger le personnel d'intervention en cas d'incident afin de vérifier que le personnel est formé de manière appropriée et périodique sur ses responsabilités en matière d'intervention en cas d'incident.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Le personnel est au courant de son rôle et de ses responsabilités dans la réponse aux incidents, et est en mesure d'accéder à de l'aide et des conseils en cas de besoin.</p>	<b>Objectif</b> Sans une équipe de réponse aux incidents, formée et facilement disponible, des dommages étendus au réseau pourraient se produire, et les données et systèmes critiques pourraient devenir « pollués » par une manipulation inappropriée des systèmes ciblés. Cela peut entraver le succès d'une enquête après incident. <b>Bonne Pratique</b> Il est important que tout le personnel impliqué dans la réponse aux incidents soit formé et connaisse la gestion des preuves pour les investigations technico-légales.
<b>Exigences de L'approche Définie</b> <p><b>12.10.4.1</b> La fréquence des formations périodiques pour le personnel d'intervention en cas d'incident est définie dans l'analyse de risque ciblée de l'entité, qui est effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p> <b>Objectif de L'approche Personnalisée</b> <p>Le personnel d'intervention en cas d'incident est formé à une fréquence adaptée au risque de l'entité.</p> <b>Notes D'applicabilité</b> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<b>Procédures de Test de L'approche Définie</b> <p><b>12.10.4.1.a</b> Examiner l'analyse de risques ciblée de l'entité pour la fréquence de formation du personnel d'intervention en cas d'incident afin de vérifier que l'analyse de risques a été effectuée conformément à tous les éléments spécifiés dans l'exigence 12.3.1.</p> <p><b>12.10.4.1.b</b> Examiner les résultats documentés de la formation périodique du personnel d'intervention en cas d'incident et interroger le personnel afin de vérifier que la formation est effectuée à la fréquence définie dans l'analyse de risques ciblée de l'entité effectuée pour la présente exigence.</p> <b>Objectif</b> L'environnement et le plan de réponse aux incidents de chaque entité sont différents et l'approche dépendra d'un certain nombre de facteurs, notamment la taille et la complexité de l'entité, le degré de modification de l'environnement, la taille de l'équipe de réponse aux incidents et la rotation du personnel. La réalisation d'une analyse de risques permettra à l'entité de déterminer la fréquence optimale de formation du personnel chargé de répondre aux incidents.

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.10.5</b> Le plan de réponse aux incidents de sécurité comprend la surveillance et la réponse aux alertes des systèmes de surveillance de la sécurité, y compris, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Systèmes de détection et de prévention des intrusions.</li> <li>• Mécanismes de sécurité réseau.</li> <li>• Mécanismes de détection des modifications pour les fichiers critiques.</li> <li>• Mécanisme de détection des modifications et des altérations pour les pages de paiement. <i>Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se référer aux Notes D'applicabilité ci-dessous pour plus de détails.</i></li> <li>• Détection des points d'accès sans fil non autorisés.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Les alertes générées par les technologies de surveillance et de détection sont traitées de manière structurée et reproductible.</p> <p><b>Notes D'applicabilité</b></p> <p><i>La point ci-dessus (pour surveiller et répondre aux alertes d'un mécanisme de détection des modifications et des altérations pour les pages de paiement) est une Bonne Pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire dans le cadre de l'exigence 12.10.5 et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.5</b> Examiner la documentation et observer les processus de réponse aux incidents afin de vérifier que la surveillance et la réponse aux alertes des systèmes de surveillance de la sécurité sont couvertes dans le plan de réponse aux incidents de sécurité, y compris, sans toutefois s'y limiter, les systèmes spécifiés dans cette exigence.</p> <p><b>Objectif</b></p> <p>La réponse aux alertes générées par les systèmes de surveillance de la sécurité qui sont explicitement conçus pour se concentrer sur les risques potentiels pour les données est essentielle pour prévenir une violation et, par conséquent, elle doit être incluse dans les processus de réponse aux incidents.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.10.6</b> Le plan de réponse aux incidents de sécurité est modifié et mis à niveau en fonction des leçons apprises et pour intégrer les développements de l'industrie.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.6.a</b> Examiner les politiques et procédures afin de vérifier que les processus sont définis pour modifier et faire évoluer le plan de réponse aux incidents de sécurité en fonction des leçons apprises et pour intégrer les développements de l'industrie.</p> <p><b>12.10.6.b</b> Examiner le plan de réponse aux incidents de sécurité et interroger le personnel responsable afin de vérifier que le plan de réponse aux incidents est modifié et mis à niveau en fonction des leçons apprises et pour intégrer les développements de l'industrie.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>L'efficacité et la précision du plan de réponse aux incidents sont examinées et mises à jour après chaque invocation.</p>	<p><b>Objectif</b> L'intégration des leçons apprises dans le plan de réponse aux incidents après qu'un incident se produise et en phase avec les développements de l'industrie, aide à maintenir le plan à jour et capable de réagir aux menaces émergentes et aux tendances de sécurité.</p> <p><b>Bonne Pratique</b> L'exercice sur les leçons apprises devrait inclure tous les niveaux du personnel. Bien qu'il soit souvent inclus dans le cadre de l'examen de l'ensemble de l'incident, il doit se concentrer sur la manière dont la réponse de l'entité à l'incident pourrait être améliorée.</p> <p>Il est important de ne pas considérer uniquement les éléments de la réponse qui n'ont pas eu les résultats prévus, mais aussi de comprendre ce qui a bien fonctionné et si les leçons tirées de ces éléments qui ont bien fonctionné peuvent être appliquées aux domaines du plan qui n'ont pas fonctionné.</p> <p>Une autre façon d'optimiser le plan de réponse aux incidents d'une entité consiste à comprendre les attaques lancées contre d'autres entreprises et à utiliser ces informations pour affiner les procédures de détection, de confinement, d'atténuation ou de récupération de l'entité.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>12.10.7</b> Des procédures d'intervention en cas d'incident sont en place, à déclencher dès la détection de PAN stockés là où ça n'est pas prévu, et inclue :</p> <ul style="list-style-type: none"> <li>• Déterminer ce qu'il faut faire si les PAN sont découverts en dehors du CDE, y compris leur récupération, sa suppression sécurisée et/ou sa migration vers le CDE actuellement défini, selon le cas.</li> <li>• Identifier si des données d'authentification sensibles sont stockées avec les PAN.</li> <li>• Déterminer d'où proviennent les données de carte et comment elles se sont retrouvées là où elles n'étaient pas prévues.</li> <li>• Corriger les fuites de données ou les lacunes des processus qui ont fait que les données de carte se trouvaient là où elles n'étaient pas prévues.</li> </ul> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Des processus sont en place pour répondre à, analyser et traiter rapidement les situations dans le cas où des PAN en clair sont détectés là où il n'est pas censé être.</p> <p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date, elle sera obligatoire et devra être pleinement prise en compte lors des évaluations PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>12.10.7.a</b> Examiner les procédures de réponse aux incidents documentées afin de vérifier que les procédures de réponse à la détection de PAN stockés partout où ils ne sont pas censés être, sont prêtes à être lancées et comportent tous les éléments spécifiés dans cette exigence.</p> <p><b>12.10.7.b</b> Interroger le personnel et examiner les enregistrements des actions d'intervention afin de vérifier que les procédures d'intervention en cas d'incident sont exécutées lors de la détection de PAN stockés partout où ils ne sont pas censés être.</p> <p><b>Objectif</b> Avoir des procédures documentées de réponse aux incidents qui sont suivies dans le cas où des PAN stockés sont trouvés là où il n'est pas prévu qu'ils se trouvent, aide à identifier les actions correctives nécessaires et à prévenir d'autres fuites à l'avenir.</p> <p><b>Bonne Pratique</b> Si les PAN ont été trouvés en dehors du CDE, une analyse doit être effectuée pour 1) déterminer s'ils ont été enregistrés indépendamment d'autres données ou avec des données d'authentification sensibles, 2) identifier la source des données et 3) identifier les lacunes de contrôle qui ont entraîné que les données soient en dehors du CDE.</p> <p>Les entités doivent déterminer s'il existe des facteurs contributifs, tels que des processus professionnels, le comportement des utilisateurs, des configurations système inappropriées, etc. qui ont entraîné le stockage des PAN dans un emplacement imprévu. Si de tels facteurs contributifs sont présents, ils doivent être traités conformément à cette exigence afin d'éviter qu'ils ne se reproduisent.</p>

## Annexe A Autres Exigences du Standard PCI DSS

Cette annexe contient des exigences supplémentaires du standard PCI DSS pour différents types d'entités. Les sections de cette Annexe comprennent :

- Annexe A1 : Autres exigences du standard PCI DSS pour les prestataires de services mutualisés
- Annexe A2 : Autres exigences du standard PCI DSS pour les entités utilisant SSL et/ou les versions obsolètes du protocole TLS pour les connexions de terminaux POS POI avec carte
- Annexe A3 : Validation complémentaire des entités désignées (DESV)

Des informations d'orientation et d'applicabilité sont fournies dans chaque section.

### Annexe A1 : Autres Exigences du Standard PCI DSS pour les Prestataires de Services Mutualisés

Sections
<b>A1.1</b> Les fournisseurs de services mutualisés protègent et séparent tous les environnements et données des clients.
<b>A1.2</b> Les fournisseurs de services mutualisés facilitent la journalisation et la réponse aux incidents pour tous les clients.

#### Aperçu

Tous les prestataires de services sont responsables du respect des exigences du standard PCI DSS pour leurs propres environnements, telles qu'elles s'appliquent aux services proposés à leurs clients. De plus, les fournisseurs de services mutualisés doivent satisfaire aux exigences de la présente annexe.

Les fournisseurs de services mutualisés sont un type de prestataires de services qui offre divers services partagés aux commerçants et autres prestataires de services, où les clients partagent des ressources système (telles que des serveurs physiques ou virtuels), l'infrastructure, des applications (y compris des logiciels en tant que service (SaaS) et/ou des bases de données. Les services peuvent inclure, sans toutefois s'y limiter, l'hébergement de plusieurs entités sur un seul serveur partagé, la prestation de services de commerce électronique et/ou de "panier d'achat", les services d'hébergement Web, les applications de paiement, diverses applications et services cloud, et services de passerelles et de processeurs offerts dans un environnement partagé.

Les prestataires qui ne fournissent que des services de centre de données partagés (souvent appelés fournisseurs de colocation ou « co-lo »), où l'équipement, l'espace et la bande passante sont disponibles en service mutualisé, ne sont pas considérés comme des prestataires de services mutualisés aux fins de la présente Annexe.

**Remarque :** Bien qu'un prestataire de service mutualisé respecte ces exigences, chaque consommateur du prestataire doit tout de même respecter les exigences de PCI DSS qui sont applicables à son périmètre et suivre le processus adéquat de validation de la conformité. Souvent, il existe des exigences PCI DSS pour lesquelles la responsabilité est partagée entre le prestataire et le consommateur (pour peut-être différents aspects de l'environnement). Les exigences 12.8 et 12.9 définissent les exigences spécifiques aux relations entre tous les prestataires de services tiers (TPSP) et leurs clients, ainsi que les responsabilités des deux. Cela comprend la définition des services spécifiques que le consommateur reçoit, ainsi que les exigences du standard PCI DSS qu'il incombe au consommateur de respecter, celles qui relèvent de la responsabilité du TPSP et les exigences partagées entre le consommateur et le TPSP.

Exigences et Procédures de Test	Directives
<b>A1.1 Les fournisseurs de services mutualisés protègent et séparent tous les environnements et données des clients.</b>	
<b>Exigences de L'approche Définie</b> <p><b>A1.1.1</b> La séparation logique est mise en œuvre comme suit :</p> <ul style="list-style-type: none"> <li>Le prestataire ne peut pas accéder aux environnements de ses clients sans autorisation.</li> <li>Les clients ne peuvent pas accéder à l'environnement du fournisseur sans autorisation.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>A1.1.1</b> Examiner la documentation et les configurations système et réseau et interroger le personnel afin de vérifier que la séparation logique est mise en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Les clients ne peuvent pas accéder à l'environnement du prestataire. Le prestataire ne peut pas accéder aux environnements de ses clients sans autorisation.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence reste une <i>Bonne Pratique</i> jusqu'au 31 mars 2025. Après cette date elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</p>	<b>Objectif</b> Cloisonner l'environnement du prestataire et l'environnement du consommateur afin d'empêcher qu'un acteur malveillant dans l'environnement du prestataire puisse compromettre l'environnement du consommateur, et de même, qu'un acteur malveillant dans l'environnement d'un consommateur puisse compromettre le prestataire et potentiellement d'autres clients du prestataire. Les environnements mutualisés doivent être isolés les uns des autres et de l'infrastructure du fournisseur de sorte qu'ils puissent être des entités gérées séparément sans connectivité entre eux. <b>Bonne Pratique</b> Les prestataires doivent assurer une séparation robuste entre les environnements conçus pour l'accès des clients ; par exemple, les portails de configuration et de facturation, et l'environnement privé du prestataire auquel seul le personnel autorisé du prestataire doit accéder. L'accès des prestataires de services aux environnements des clients est effectué conformément à l'exigence 8.2.3. <b>Informations Complémentaires</b> Se reporter au <i>Complément d'informations : Directives du PCI SSC pour l'informatique en cloud</i> pour plus d'informations sur les environnements cloud.

Exigences et Procédures de Test		Directives
<b>Exigences de L'approche Définie</b>  <b>A1.1.2</b> Des mesures de sécurité sont mises en place de manière à ce que chaque consommateur n'ait l'autorisation d'accéder qu'à ses propres données de porteurs de cartes et au CDE.	<b>Procédures de Test de L'approche Définie</b>  <b>A1.1.2.a</b> Examiner la documentation afin de vérifier que les mesures sont définies de sorte que chaque consommateur n'ait l'autorisation d'accéder qu'à ses propres données de titulaires de cartes et au CDE.  <b>A1.1.2.b</b> Examiner les configurations du système afin de vérifier que les clients disposent de priviléges établis pour accéder uniquement à leurs propres données de carte et leur CDE.	<b>Objectif</b> Il est important qu'un prestataire de services mutualisés définisse des mesures de sécurité afin que chaque consommateur ne puisse accéder qu'à son propre environnement et CDE afin d'éviter l'accès non autorisé d'un environnement consommateur à un autre.  <b>Exemples</b> Dans une infrastructure basée sur le cloud, telle qu'une offre d'infrastructure en tant que service (IaaS), le CDE des clients peut inclure des périphériques réseaux virtuels et des serveurs virtuels qui sont configurés et gérés par les clients, y compris les systèmes d'exploitation, les fichiers, la mémoire, etc.
<b>Objectif de L'approche Personnalisée</b>  Les clients ne peuvent pas accéder aux environnements d'autres clients.		
<b>Exigences de L'approche Définie</b>  <b>A1.1.3</b> Des mesures de sécurité sont mises en place de sorte que chaque consommateur ne puisse accéder qu'aux ressources qui lui sont allouées.	<b>Procédures de Test de L'approche Définie</b>  <b>A1.1.3</b> Examiner les priviléges des clients afin de vérifier que chaque consommateur ne peut accéder qu'aux ressources qui lui sont allouées.	<b>Objectif</b> Pour éviter tout impact involontaire ou intentionnel sur les environnements ou les données de carte d'autres clients, il est important que chaque consommateur puisse accéder uniquement aux ressources qui lui sont allouées.
<b>Objectif de L'approche Personnalisée</b>  Les clients ne peuvent pas impacter les ressources allouées à d'autres clients.		

Exigences et Procédures de Test		Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A1.1.4</b> L'efficacité des mesures de séparation logique utilisées pour séparer les environnements des clients est testée et confirmée au moins une fois tous les six mois via des tests d'intrusion.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>La segmentation des environnements consommateur à partir d'autres environnements est périodiquement validée comme efficace.</p> <p><b>Notes D'applicabilité</b></p> <p>Le test d'une séparation adéquate entre les clients dans un environnement de prestataires de services mutualisés s'ajoute aux tests d'intrusion spécifiés dans l'exigence 11.4.6.</p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A1.1.4</b> Examiner les résultats des tests d'intrusion les plus récents afin de vérifier que les tests ont confirmé l'efficacité des mesures de séparation logique utilisées pour séparer les environnements des clients.</p>	<p><b>Objectif</b> Les prestataires de services mutualisés sont tenus de gérer la segmentation entre leurs clients. Sans l'assurance technique que les mesures de segmentation sont efficaces, il est possible que des modifications apportées à la technologie du prestataire de services créent par inadvertance une vulnérabilité qui pourrait être exploitée par tous les clients du prestataire de services.</p> <p><b>Bonne Pratique</b> L'efficacité des techniques de séparation peut être confirmée en utilisant des environnements temporaires (maquettes) créés par le prestataire de services qui représentent les environnements des clients et en tentant 1) d'accéder à un environnement temporaire à partir d'un autre environnement, et 2) d'accéder à un environnement temporaire à partir d'Internet.</p>

Exigences et Procédures de Test	Directives	
<b>A1.2 Les fournisseurs de services mutualisés facilitent la journalisation et la réponse aux incidents pour tous les clients.</b>		
<b>Exigences de L'approche Définie</b> <p><b>A1.2.1</b> La fonction des journaux d'audit est activée pour l'environnement de chaque consommateur conformément à l'exigence 10 du standard PCI DSS, notamment :</p> <ul style="list-style-type: none"> <li>• Les journaux sont activés pour les applications courantes de tiers.</li> <li>• Les journaux sont actifs par défaut.</li> <li>• Les journaux sont disponibles pour examen uniquement par le consommateur qui en est le propriétaire.</li> <li>• Les emplacements des journaux sont clairement communiqués au consommateur propriétaire.</li> <li>• Les données de journaux et la disponibilité sont conformes à l'exigence 10 du standard PCI DSS.</li> </ul>	<b>Procédures de Test de L'approche Définie</b> <p><b>A1.2.1</b> Examiner la documentation et les paramètres de configuration du système afin de vérifier que le prestataire a activé la fonctionnalité des journaux d'audit pour chaque environnement consommateur conformément à tous les éléments spécifiés dans cette exigence.</p>	
<b>Objectif de L'approche Personnalisée</b> <p>La capacité de journalisation est disponible pour tous les clients sans affecter la confidentialité des autres clients.</p>	<b>Objectif</b> Les informations de journalisation sont utiles pour détecter et diagnostiquer les incidents de sécurité et sont inestimables pour les enquêtes de criminalistique. Les clients doivent donc avoir accès à ces journaux. Cependant, les informations des journaux peuvent également être utilisées par un attaquant à des fins de reconnaissance. Par conséquent, les informations des journaux d'un consommateur ne doivent être accessibles que par le consommateur auquel les journaux se rapportent.	
<b>Exigences de L'approche Définie</b> <p><b>A1.2.2</b> Des processus ou des mécanismes sont mis en œuvre pour prendre en charge et/ou faciliter des enquêtes criminalistiques rapides en cas d'incident de sécurité soupçonné ou avéré pour tout consommateur.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>A1.2.2</b> Examiner les procédures documentées afin de vérifier que le prestataire dispose de processus ou de mécanismes pour prendre en charge et/ou faciliter une enquête criminalistique rapide sur les serveurs associés en cas d'incident de sécurité soupçonné ou avéré pour un consommateur.</p>	<b>Objectif</b> En cas de violation soupçonnée ou avérée de la confidentialité des données des titulaires de cartes, l'enquêteur criminalistique d'un consommateur vise à trouver la cause de la violation, à exclure l'attaquant de l'environnement et à s'assurer que tout accès non autorisé est supprimé. Des réponses rapides et efficaces aux demandes des enquêteurs criminalistiques peuvent réduire considérablement le temps nécessaire à l'enquêteur pour sécuriser l'environnement du consommateur.
<b>Objectif de L'approche Personnalisée</b> <p>L'enquête criminalistique est facilement accessible à tous les clients en cas d'incident de sécurité soupçonné ou avéré.</p>		

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A1.2.3</b> Des processus ou des mécanismes sont mis en œuvre pour signaler et traiter les incidents de sécurité et les vulnérabilités soupçonnés ou avérés, notamment :</p> <ul style="list-style-type: none"> <li>• Les clients peuvent en toute sécurité signaler les incidents de sécurité et les vulnérabilités au prestataire.</li> <li>• Le prestataire traite et corrige les incidents de sécurité et les vulnérabilités soupçonnés ou avérés conformément à l'exigence 6.3.1.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A1.2.3</b> Examiner les procédures documentées et interroger le personnel afin de vérifier que le prestataire dispose d'un mécanisme de signalement et de traitement des incidents de sécurité et des vulnérabilités soupçonnés ou avérés, conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Les incidents de sécurité ou les vulnérabilités soupçonnés ou avérés sont découverts et traités. Les clients sont informés le cas échéant.</p>	<p><b>Objectif</b></p> <p>Les vulnérabilités de sécurité dans les services fournis peuvent avoir une incidence sur la sécurité de tous les clients du prestataire de services et doivent donc être gérées conformément aux processus établis du prestataire de services, la priorité étant donnée à la résolution des vulnérabilités qui présentent la plus forte probabilité de compromission.</p> <p>Les clients sont susceptibles de remarquer des vulnérabilités et des erreurs de configuration de sécurité lors de l'utilisation du service.</p>
<p><b>Notes D'applicabilité</b></p> <p><i>Cette exigence reste une Bonne Pratique jusqu'au 31 mars 2025. Après cette date elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i></p>	<p>La mise en œuvre de méthodes sécurisées permettant aux clients de signaler les incidents de sécurité et les vulnérabilités encourage les clients à signaler les problèmes potentiels et permet au prestataire de se renseigner rapidement sur les problèmes potentiels dans leur environnement et de les résoudre.</p>

## Annexe A2 : Autres Exigences du Standard PCI DSS pour les Entités Utilisant SSL et/ou les Versions Obsolètes du Protocole TLS pour les Connexions de Terminaux POS POI Avec Carte

Sections
<b>A2.1</b> Les terminaux POI utilisant SSL et/ou les versions obsolètes du protocole TLS sont confirmés comme n'étant pas exposés aux exploits SSL/TLS connus.

### Aperçu

Cette annexe s'applique uniquement aux entités utilisant SSL et/ou les versions obsolètes de TLS pour sécuriser les données transmises par les terminaux POS POI. Elle s'applique également aux prestataires de services qui fournissent des connexions aux terminaux POS POI.

Les entités utilisant SSL et les versions obsolètes du protocole TLS pour les connexions des terminaux POS POI doivent travailler à la mise à niveau vers un protocole cryptographique fort dès que possible. De plus, SSL et/ou les versions obsolètes de TLS ne doivent pas être introduits dans des environnements où ces protocoles n'existent pas déjà. Au moment de la publication, les vulnérabilités connues sont difficiles à exploiter dans les terminaux de paiement POS POI. Cependant, de nouvelles vulnérabilités peuvent apparaître à tout moment, et il appartient à l'entreprise de rester à jour avec les tendances des vulnérabilités et de déterminer si elle est exposée à des exploits connus.

Les exigences du standard PCI DSS directement concernées sont :

- **Exigence 2.2.5** : Lorsque des services, protocoles ou démons non sécurisés sont présents ; la justification métier est documentée et des fonctionnalités de sécurité supplémentaires sont documentées et mises en œuvre pour réduire le risque d'utilisation de services, de protocoles ou de démons non sécurisés.
- **Exigence 2.2.7** : Tous les accès administratifs non-console sont chiffrés à l'aide d'une cryptographie robuste.
- **Exigence 4.2.1** : Des protocoles de chiffrement et de sécurité robustes sont mis en œuvre afin de protéger le PAN pendant la transmission sur des réseaux publics ouverts.

Les protocoles SSL et les versions obsolètes de TLS ne doivent pas être utilisés comme mesures de sécurité pour répondre à ces exigences, sauf dans le cas des connexions de terminaux POS POI, comme détaillé dans la présente annexe. Pour soutenir les entités travaillant à migrer de SSL et des versions obsolètes de TLS sur les terminaux POS POI, les dispositions suivantes sont incluses :

- Les nouvelles implémentations de terminaux POS POI ne doivent pas utiliser SSL ou les versions obsolètes de TLS comme mesure de sécurité.
- Tous les prestataires de services de terminaux POS POI doivent fournir une offre de service sécurisée.
- Les prestataires de services prenant en charge les mises en œuvre de terminaux POS POI existants qui utilisent SSL et/ou les versions obsolètes de TLS doivent avoir mis en place un plan de remédiation officiel permettant d'atténuer les risques et un plan de migration.
- Les terminaux POS POI dans des environnements de paiement en proximité qui peuvent être vérifiés comme n'étant pas exposés à des exploits connus pour SSL et/ou les versions obsolètes de TLS, **et les points de terminaison SSL/TLS auxquels ils se connectent**, peuvent continuer à utiliser SSL et/ou les versions obsolètes de TLS comme mesure de sécurité.

Les exigences de cette annexe ne sont pas admissibles à L'approche Personnalisée.

## Exigences et Procédures de Test

## Directives

**A2.1 Les terminaux POI utilisant SSL et/ou les versions obsolètes de TLS sont confirmées comme n'étant pas exposés aux exploits SSL/TLS connus.**

Exigences de L'approche Définie	Procédures de Test de L'approche Définie	Objectif
<p><b>A2.1.1</b> Lorsque les terminaux POS POI du commerçant ou du lieu d'acceptation des paiements utilisent SSL et/ou les versions obsolètes de TLS, l'entité confirme que les systèmes d'acceptation ne sont pas vulnérables et exposés à des exploits connus pour ces protocoles.</p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p> <p><b>Notes D'applicabilité</b></p> <p>Cette exigence est destinée à s'appliquer à l'entité disposant du terminal POS POI, telle qu'un commerçant. Cette exigence n'est pas destinée aux prestataires de services qui servent de point de terminaison ou de connexion à ces terminaux POS POI. Les exigences A2.1.2 et A2.1.3 s'appliquent aux prestataires de services POS POI.</p> <p>L'utilisation de SSL et/ou des versions obsolètes de TLS par les terminaux POS POI est tolérée sur la base des risques et exploits actuellement connus et sous condition que ces systèmes ne soient pas exposés à ces derniers.</p> <p>Si de nouveaux exploits sont introduits auxquels les terminaux POS POI sont exposés, les terminaux POS POI devront être mis à jour immédiatement.</p>	<p><b>A2.1.1</b> Pour les terminaux POS POI utilisant SSL et/ou les versions obsolètes de TLS, confirmer que l'entité dispose d'une documentation (par exemple, la documentation du fournisseur, les détails de la configuration du système/du réseau) qui vérifie que les systèmes d'acceptation ne sont pas exposés à des exploits connus pour les protocoles SSL et les versions obsolètes de TLS.</p>	<p><b>Objectif</b></p> <p>Les terminaux POS POI utilisés dans les environnements de paiement en proximité peuvent continuer à utiliser SSL et les versions obsolètes de TLS lorsqu'il peut être démontré que le terminal POS POI n'est pas exposé aux exploits actuellement connus.</p> <p><b>Bonne Pratique</b></p> <p>Cependant, le protocole SSL est une technologie obsolète ; de nouvelles vulnérabilités l'affectant pourront être identifiées à l'avenir. Il est donc fortement recommandé de mettre à niveau les terminaux POS POI vers un protocole sécurisé dès que possible. Si le protocole SSL et/ou les versions obsolètes de TLS ne sont pas nécessaires dans l'environnement, l'utilisation et le recours à ces versions doivent être désactivés.</p> <p><b>Informations Complémentaires</b></p> <p>Se reporter aux compléments d'informations du PCI SSC actuels sur SSL et les versions obsolètes de TLS pour plus d'informations.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A2.1.2 Exigence supplémentaire pour les prestataires de services uniquement :</b> Tous les prestataires de services disposant de points de connexion existants aux terminaux POS POI qui utilisent le protocole SSL et/ou les versions obsolètes de TLS tels que définis à l'annexe A2.1 ont mis en place un plan de remédiation permettant d'atténuer les risques et de migration qui comprend :</p> <ul style="list-style-type: none"> <li>Une description de l'utilisation, y compris les données transmises, les types et le nombre de systèmes qui utilisent et/ou prennent en charge le protocole SSL et/ou les versions obsolètes de TLS et le type d'environnement.</li> <li>Résultats de l'évaluation des risques et mesures de réduction des risques en place.</li> <li>Description des processus pour surveiller les nouvelles vulnérabilités associées à SSL et les versions obsolètes de TLS.</li> <li>Description des processus de gestion des changements qui sont mis en œuvre pour garantir que le protocole SSL et les versions obsolètes de TLS ne sont pas mis en œuvre dans de nouveaux environnements.</li> <li>Aperçu du plan de projet de migration pour remplacer SSL et les versions obsolètes de TLS à une date ultérieure.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A2.1.2 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner le plan d'atténuation des risques et de migration documentée afin de vérifier qu'il comprend tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Les points de terminaison POS POI, y compris, sans toutefois s'y limiter, les fournisseurs de services tels que les acquéreurs ou les processeurs des acquéreurs, peuvent continuer à utiliser le protocole SSL et les versions obsolètes de TLS lorsqu'il peut être démontré que le prestataire de services a mis en place des mesures de sécurité qui atténuent les risques liés au maintien de ces protocoles au sein de l'environnement du prestataire de services.</p> <p><b>Bonne Pratique</b> Les prestataires de services doivent communiquer à tous les clients utilisant le protocole SSL et les versions obsolètes de TLS les risques associés à leur utilisation et la nécessité de migrer vers un protocole sécurisé.</p> <p><b>Définitions</b> Le plan d'atténuation des risques et de migration, préparé par l'entité, détaille la migration vers un protocole sécurisé et décrit les mesures de sécurité mises en place afin de réduire le risque associé au protocole SSL et aux versions obsolètes de TLS.</p> <p><b>Informations Complémentaires</b> Se reporter aux suppléments d'information actuels du PCI SSC sur le protocole SSL et les versions obsolètes de TLS pour plus d'informations sur les plans d'atténuation des risques et de migration.</p>
<p><b>Notes D'applicabilité</b></p> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	

Exigences et Procédures de Test	Directives
<b>Exigences de L'approche Définie</b> <p><b>A2.1.3 Exigence supplémentaire pour les prestataires de services uniquement :</b> Tous les prestataires de services proposent une offre de services sécurisée.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>A2.1.3 Procédure de test supplémentaire pour les évaluations des prestataires de services uniquement :</b> Examiner les configurations du système et les documents justificatifs afin de vérifier que le prestataire de services offre une option de protocole sécurisé pour son service.</p>
<b>Objectif de L'approche Personnalisée</b> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	
<b>Notes D'applicabilité</b> <p>Cette exigence ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>	<b>Objectif</b> Les clients doivent pouvoir choisir de mettre à niveau leurs systèmes d'acceptation pour éliminer les vulnérabilités liées à l'utilisation de SSL et des versions obsolètes de TLS. Souvent, les clients auront préférence à adopter une approche progressive de migration de leur parc de POI POS, du protocole non sécurisé vers un protocole sécurisé. Pour ce faire, les clients exigeront que le prestataire de services propose une offre sécurisée. <b>Informations Complémentaires</b> Se reporter aux compléments d'informations du PCI SSC actuels sur SSL et les versions obsolètes de TLS initial pour plus d'informations.

## Annexe A3 : Validation Complémentaire des Entités Désignées (DESV)

### Sections

- A3.1** Un programme de conformité au standard PCI DSS est mis en œuvre.
- A3.2** La périphérie du standard PCI DSS est documentée et validée.
- A3.3** Le standard PCI DSS est intégrée aux activités courantes (BAU).
- A3.4** L'accès logique à l'environnement des données des titulaires de cartes est contrôlé et géré.
- A3.5** Les événements suspects sont identifiés et traités.

### Aperçu

Cette annexe s'applique uniquement aux entités désignées par un ou plusieurs des réseaux internationaux ou un acquéreur comme nécessitant une validation supplémentaire des exigences existantes du standard PCI DSS. Une entité est tenue de se soumettre à une évaluation conformément à la présente annexe **UNIQUEMENT** si elle lui est demandée par un acquéreur ou une marque de paiement. Voici des exemples d'entités auxquelles cette annexe pourrait s'appliquer :

- Ceux qui stockent, traitent et/ou transmettent de gros volumes de données de carte,
- Ceux qui fournissent des points d'agrégation pour les données de carte, ou
- Ceux qui ont subi des compromissions importantes ou répétées des données de carte.

De plus, d'autres standards PCI peuvent faire référence à la réalisation de cette annexe.

Ces étapes de validation supplémentaires visent à fournir une plus grande assurance que les mesures de sécurité du standard PCI DSS sont maintenues de manière efficace et continue en s'appuyant sur les processus de maintien des activités courantes (BAU). Ces étapes visent également à fournir l'assurance que les évolutions de périphérie sont prises en compte dans le cadre du programme de conformité au standard PCI DSS et que les processus de validation adaptés sont mis en œuvre en fonction de ces évolutions.

(suite à la page suivante)

**Remarque :** Certaines exigences PCI DSS dans cette Annexe ont défini des délais (par exemple, Avec une activité qui doit être réalisée au moins une fois tous les trois mois ou tous les six mois). Pour une évaluation initiale de ces exigences, il n'est pas nécessaire qu'une activité ait été effectuée pour chacune de ces périodes au cours de l'année précédente, si l'auditeur vérifie que :

- L'activité a été réalisée conformément à l'exigence applicable dans le délai le plus récent (par exemple, la période de trois ou six mois la plus récente), et
- L'entité a des politiques et des procédures documentées pour continuer à exercer l'activité dans le délai défini.

Pour les années suivantes après l'évaluation initiale, une activité doit avoir été réalisée dans chaque période requise (par exemple, une activité requise tous les trois mois doit avoir été réalisée au moins quatre fois au cours de l'année précédente à un intervalle ne dépassant pas 92 jours).

Se reporter à la section 7 Description des calendriers utilisés dans les exigences pour des instructions supplémentaires sur les évaluations initiales.

Toutes les exigences du standard PCI DSS ne s'appliquent pas à toutes les entités susceptibles de subir une évaluation. C'est pour cette raison que certaines exigences du standard PCI DSS sont dupliquées dans la présente annexe. Toute question concernant cette annexe doit être adressée aux acquéreurs ou aux réseaux internationaux.

Exigences et Procédures de Test	Directives
<b>A3.1 Un programme de conformité au standard PCI DSS est mis en œuvre.</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.1.1</b> La responsabilité est établie par la direction générale pour la protection des données de carte et un programme de conformité au standard PCI DSS qui comprend :</p> <ul style="list-style-type: none"> <li>• Responsabilité globale pour le maintien de la conformité PCI DSS.</li> <li>• Définition d'une charte pour un programme de conformité au standard PCI DSS.</li> <li>• Fournir des mises à jour à la direction générale et au conseil d'administration sur les initiatives et les problèmes de conformité au standard PCI DSS, y compris les activités de correction, au moins une fois tous les 12 mois.</li> </ul> <p><b>Référence du standard PCI DSS : Exigence 12</b></p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.1.1.a</b> Examiner la documentation afin de vérifier que la direction générale a attribué la responsabilité globale du maintien de la conformité au standard PCI DSS de l'entité.</p> <p><b>A3.1.1.b</b> Examiner la charte du standard PCI DSS de l'entreprise afin de vérifier qu'elle décrit les conditions dans lesquelles le programme de conformité à le standard PCI DSS est organisé.</p> <p><b>A3.1.1.c</b> Examiner les procès-verbaux et/ou les présentations des réunions de la direction générale et du conseil d'administration pour s'assurer que les initiatives de conformité au standard PCI DSS et les activités correctives sont communiquées au moins une fois tous les 12 mois.</p> <p><b>Objectif</b></p> <p>L'attribution par la haute direction des responsabilités de conformité PCI DSS garantit une visibilité au niveau de la direction sur le programme de conformité PCI DSS, et permet de poser des questions appropriées pour déterminer l'efficacité du programme et influer sur les priorités stratégiques.</p> <p><b>Bonne Pratique</b></p> <p>La haute direction peut inclure des postes de niveau dirigeant, un conseil d'administration ou équivalent. Les titres spécifiques dépendront de la structure organisationnelle particulière.</p> <p>La responsabilité du programme de conformité PCI DSS peut être attribuée à des rôles individuels et/ou à des services/départements métier au sein de l'entreprise.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.1.2</b> Un programme formel de conformité au standard PCI DSS est en place et comprend :</p> <ul style="list-style-type: none"> <li>• Définition des activités de maintien et de surveillance de la conformité globale au standard PCI DSS, y compris les activités courantes.</li> <li>• Processus annuels d'évaluation vis-à-vis des exigences du standard PCI DSS</li> <li>• Processus de validation continue des exigences du standard PCI DSS (par exemple, quotidiennement, hebdomadairement, tous les trois mois, selon l'exigence).</li> <li>• Un processus permettant d'effectuer une analyse d'impact sur l'entreprise afin de déterminer les impacts potentiels du standard PCI DSS sur les décisions métier stratégiques.</li> </ul> <p><b>Référence du standard PCI DSS : Exigences 1 à 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.1.2.a</b> Examiner les politiques et procédures de sécurité des informations afin de vérifier que les processus sont définis pour un programme formel de conformité au standard PCI DSS qui comporte tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.1.2.b</b> Interroger le personnel et observer les activités de conformité afin de vérifier qu'un programme formel de conformité au standard PCI DSS est mis en œuvre conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Un programme de conformité formel permet à une entreprise de surveiller l'état de ses mesures et mesures de sécurité de sécurité, d'être proactive en cas de panne d'une mesure ou contrôle et de communiquer efficacement les activités et l'état de conformité dans toute l'entreprise.</p> <p><b>Bonne Pratique</b> Le programme de conformité à PCI DSS peut être un programme dédié ou faire partie d'un programme global de conformité et/ou de gouvernance, et doit inclure une méthodologie bien définie qui démontre une évaluation cohérente et efficace.</p> <p>Les décisions métier stratégiques qui doivent être analysées pour les impacts potentiels du standard PCI DSS peuvent inclure les fusions et acquisitions, les achats de nouvelles technologies ou les nouveaux canaux d'acceptation des paiements.</p> <p><b>Définitions</b> Le maintien et la surveillance de la conformité globale au standard PCI DSS d'une entreprise comprennent l'identification des activités à effectuer quotidiennement, hebdomadairement, mensuellement, tous les trois mois ou annuellement, et la garantie que ces activités sont exécutées en conséquence (par exemple, en utilisant une auto-évaluation de la sécurité ou une méthodologie PDCA).</p> <p><b>Exemples</b> Les méthodologies qui prennent en charge la gestion des programmes de conformité incluent Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC et Six Sigma.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.1.3</b> Les rôles et responsabilités de la conformité au standard PCI DSS sont spécifiquement définis et formellement attribués à un ou plusieurs membres du personnel, notamment :</p> <ul style="list-style-type: none"> <li>• La gestion des activités courantes du standard PCI DSS.</li> <li>• La gestion des évaluations annuelles du standard PCI DSS</li> <li>• La gestion de la validation continue des exigences du standard PCI DSS (par exemple, quotidiennement, hebdomadairement, tous les trois mois, selon l'exigence).</li> <li>• La gestion de l'analyse d'impact sur l'entreprise afin de déterminer les impacts potentiels du standard PCI DSS sur les décisions métier stratégiques.</li> </ul> <p><b>Référence du standard PCI DSS : Exigence 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.1.3.a</b> Examiner les politiques et procédures de sécurité des informations et interroger le personnel afin de vérifier que les rôles et responsabilités de la conformité au standard PCI DSS sont spécifiquement définis et officiellement attribués à un ou plusieurs membres du personnel conformément à tous les éléments de la présente exigence.</p> <p><b>A3.1.3.b</b> Interroger le personnel responsable et vérifier qu'il connaît et s'acquitte de ses responsabilités de conformité au standard PCI DSS.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> La définition formelle des rôles et responsabilités spécifiques de conformité au standard PCI DSS contribue à assurer la responsabilisation et la surveillance des efforts continus de conformité au standard PCI DSS.</p> <p><b>Bonne Pratique</b> La propriété devrait être attribuée aux personnes ayant le pouvoir de prendre des décisions fondées sur les risques et sur qui incombe la responsabilité de la fonction spécifique. Les tâches doivent être formellement définies et les propriétaires doivent être en mesure de démontrer une compréhension de leurs responsabilités et de leur comptabilité. Les rôles de conformité peuvent être attribués à un seul propriétaire ou à plusieurs propriétaires pour différents éléments de l'exigence.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.1.4</b> Une formation à jour sur le standard PCI DSS et/ou la sécurité des informations est dispensée au moins une fois tous les 12 mois au personnel ayant des responsabilités de conformité au standard PCI DSS (telles qu'identifiées en A3.1.3).</p> <p><b>Référence du standard PCI DSS : Exigence 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.1.4.a</b> Examiner les politiques et procédures de sécurité des informations afin de vérifier qu'une formation au standard PCI DSS et/ou à la sécurité des informations est requise au moins une fois tous les 12 mois pour chaque rôle ayant des responsabilités de conformité au standard PCI DSS.</p> <p><b>A3.1.4.b</b> Interroger le personnel et examiner les feuilles d'émarginement ou d'autres dossiers afin de vérifier que le personnel responsable de la conformité au standard PCI DSS reçoit une formation à jour sur le standard PCI DSS et/ou une formation similaire sur la sécurité des informations au moins une fois tous les 12 mois.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Le personnel responsable de la conformité au standard PCI DSS a des besoins de formation spécifiques dépassant ceux qui sont généralement fournis par la formation générale de sensibilisation à la sécurité afin de lui permettre de remplir son rôle.</p> <p><b>Bonne Pratique</b> Les personnes ayant des responsabilités de conformité au standard PCI DSS doivent recevoir une formation spécialisée qui, en plus d'une sensibilisation générale à la sécurité des informations, se concentre sur des sujets, des compétences, des processus ou des méthodologies de sécurité spécifiques qui doivent être suivis pour que ces personnes s'acquittent efficacement de leurs responsabilités de conformité.</p> <p>La formation peut être proposée par des tiers tels que le PCI SSC (par exemple, PCI Awareness, PCIP et ISA), les réseaux internationaux et les acquéreurs, ou la formation peut être en interne. Le contenu de la formation doit être applicable à la fonction de la personne, être à jour et inclure les dernières menaces de sécurité et/ou la version du standard PCI DSS.</p> <p><b>Informations Complémentaires</b> Pour plus d'informations, se reporter au <i>Complément d'informations : Meilleures pratiques pour la mise en œuvre d'un programme de sensibilisation à la sécurité</i>.</p>

Exigences et Procédures de Test	Directives	
<b>A3.2 Le périmètre soumis aux exigences de PCI DSS est documenté et validé.</b>		
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.1</b> Le périmètre soumis aux exigences de PCI DSS est documenté et son exactitude est confirmé au moins une fois tous les trois mois et en cas de modifications importantes de l'environnement. Au minimum, la validation du périmètre comprend :</p> <ul style="list-style-type: none"> <li>Identifier tous les flux de données pour les différentes étapes de paiement (par exemple, l'autorisation, la capture des règlements, les rétro facturations et les remboursements) et les canaux d'acceptation (par exemple, le paiement en proximité, le paiement à distance et le commerce électronique).</li> <li>Mettre à jour tous les diagrammes de flux de données conformément à l'exigence 1.2.4.</li> <li>Identifier tous les emplacements où les données carte sont stockées, traitées et transmises, y compris, sans toutefois s'y limiter, 1) tous les emplacements en dehors du CDE actuellement défini, 2) les applications qui traitent les CHD, 3) les transmissions entre systèmes et réseaux, et 4) les sauvegardes de fichiers.</li> <li>Pour toutes les données carte trouvées en dehors du CDE actuellement défini, soit 1) les supprimer de manière sécurisée, 2) les migrer dans le CDE actuellement défini, ou 3) étendre le CDE actuellement défini pour les inclure.</li> <li>Identifier tous les composants système dans le CDE, connectés au CDE, ou qui pourraient avoir une incidence sur la sécurité du CDE.</li> <li>Identifier toutes les mesures de sécurité de segmentation utilisés et le ou les environnements à partir desquels le CDE est segmenté, y compris la justification des environnements qui sont exclus du périmètre soumis à PCI DSS.</li> </ul> <p>(suite à la page suivante)</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.1.a</b> Examiner les résultats documentés des examens de la périmètre et interroger le personnel afin de vérifier que les examens sont effectués :</p> <ul style="list-style-type: none"> <li>Au moins une fois tous les trois mois.</li> <li>Après des modifications importantes de l'environnement dans la portée.</li> </ul> <p><b>A3.2.1.b</b> Examiner les résultats documentés des examens de la périmètre effectuées au moins une fois tous les trois mois afin de vérifier que la validation du périmètre comporte tous les éléments spécifiés dans cette exigence.</p>	<p><b>Objectif</b></p> <p>La validation fréquente du périmètre du standard PCI DSS permet de garantir que le périmètre du standard PCI DSS reste à jour et alignée sur les objectifs métiers changeants, et donc que les mesures de sécurité de sécurité protègent tous les composants systèmes appropriés.</p> <p><b>Bonne Pratique</b></p> <p>Une délimitation précise implique une évaluation critique du CDE et de tous les composants du système connecté afin de déterminer la couverture nécessaire pour les exigences du standard PCI DSS. Les activités de délimitation, y compris une analyse minutieuse et une surveillance continue, aident à garantir que les systèmes concernés sont correctement sécurisés. Lors de la documentation des emplacements des données de carte, l'entité peut envisager de créer un tableau ou une feuille de calcul contenant les informations suivantes :</p> <ul style="list-style-type: none"> <li>Les magasins de données (bases de données, fichiers, cloud, etc.), y compris la finalité du stockage des données et la durée de conservation,</li> <li>Quels éléments des CHD sont stockés (PAN, date d'expiration, nom du titulaire de la carte et/ou tout élément des SAD avant la fin de l'autorisation),</li> <li>Comment les données sont sécurisées (type de chiffrement et force, algorithme de hachage et force, troncature, tokenisation),</li> <li>Comment l'accès aux magasins de données est enregistré, y compris une description du ou des mécanismes de journalisation utilisés (solution d'entreprise, niveau de l'application, niveau de système d'exploitation, etc.).</li> </ul> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
<ul style="list-style-type: none"> <li>Identifier toutes les connexions aux entités tierces ayant accès au CDE.</li> <li>Confirmer que tous les flux de données identifiés, les données de carte, les composants système, les mesures de sécurité de segmentation et les connexions de tiers ayant accès au CDE sont inclus dans la portée.</li> </ul> <p><b>Référence du standard PCI DSS : Périmètre des exigences du standard PCI DSS, Exigence 12</b></p>	<p>En plus des systèmes et réseaux internes, toutes les connexions d'entités tierces ; par exemple, des partenaires commerciaux, des entités fournissant des services d'assistance à distance et d'autres prestataires de services, doivent être identifiées pour déterminer leur inclusion dans le périmètre du standard PCI DSS. Une fois que les connexions concernées ont été identifiées, les mesures de sécurité applicables du standard PCI DSS peuvent être mis en œuvre afin de réduire le risque qu'une connexion tierce soit utilisée pour compromettre le CDE d'une entité.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p>Un outil ou une méthodologie de découverte de données peut être utilisé pour faciliter l'identification de toutes les sources et emplacements des PAN, et pour rechercher des PAN qui résident sur des systèmes et des réseaux en dehors du CDE actuellement défini ou dans des endroits inattendus au sein du CDE défini ; par exemple, dans un journal d'erreurs ou un fichier de vidage de la mémoire. Cette approche peut aider à garantir que des emplacements de PAN précédemment inconnus sont détectés et que le PAN est soit éliminé, soit correctement sécurisé.</p> <p><b>Informations Complémentaires</b></p> <p>Se reporter au <i>Complément d'informations : Conseils pour le périmètre le standard PCI DSS et la segmentation du réseau</i> pour obtenir des conseils supplémentaires.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.2</b> L'impact du périmètre du standard PCI DSS pour toutes les modifications apportées aux systèmes ou aux réseaux est déterminé, y compris les ajouts de nouveaux systèmes et de nouvelles connexions réseau. Les processus comportent :</p> <ul style="list-style-type: none"> <li>• La réalisation d'une évaluation formelle de l'impact du standard PCI DSS.</li> <li>• L'identification des exigences du standard PCI DSS applicables au système ou au réseau.</li> <li>• La mise à jour du périmètre du standard PCI DSS, le cas échéant.</li> <li>• L'approbation documentée des résultats de l'évaluation d'impact par le personnel responsable (tel que défini en A3.1.3).</li> </ul> <p><b>Référence du standard PCI DSS :</b> <i>Périmètre des exigences du standard PCI DSS, Exigence 1 à 12</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.2</b> Examiner la documentation des modifications et interroger le personnel afin de vérifier que pour chaque modification du périmètre aux systèmes ou aux réseaux, l'impact du périmètre du standard PCI DSS est déterminé et comporte tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Les modifications apportées aux systèmes ou aux réseaux peuvent avoir un impact significatif sur le périmètre du standard PCI DSS. Par exemple, les modifications apportées aux ensembles de règles de contrôle de la sécurité du réseau peuvent amener des segments de réseau entiers dans la portée, ou de nouveaux systèmes peuvent être ajoutés au CDE qui doivent être protégés de manière adéquate.</p> <p>Une évaluation formelle de l'impact effectuée avant une modification donne à l'entité l'assurance que la modification n'aura aucune incidence négative la sécurité du CDE.</p> <p><b>Bonne Pratique</b> Les processus visant à déterminer l'impact potentiel que les modifications apportées aux systèmes et aux réseaux peuvent avoir sur le périmètre du standard PCI DSS d'une entité peuvent être exécutés dans le cadre d'un programme de conformité dédié au standard PCI DSS ou peuvent relever du programme global de conformité et/ou de gouvernance d'une entité.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.2.1</b> À la fin d'une modification, toutes les exigences pertinentes du standard PCI DSS sont confirmées comme étant mises en œuvre sur tous les systèmes et réseaux nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant.</p> <p><b>Référence du standard PCI DSS :</b> <i>Périmètre des exigences du standard PCI DSS, Exigences 1 à 12</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.2.1</b> Examiner les enregistrements des modifications et des systèmes/réseaux touchés, et, interroger le personnel afin de vérifier que toutes les exigences pertinentes du standard PCI DSS ont été confirmées comme étant mises en œuvre et que la documentation a été mise à jour dans le cadre de la modification.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Il est important de disposer de processus pour analyser toutes les modifications apportées aux systèmes ou aux réseaux, afin de garantir que tous les mesures de sécurité PCI DSS sont appliqués à tous les systèmes ou réseaux ajoutés à l'environnement dans le périmètre en raison d'une modification.</p> <p>L'intégration de cette validation dans les processus de gestion des changements permet de garantir que les inventaires des appareils et les standards de configuration sont tenus à jour et que des mesures de sécurité de sécurité sont appliqués, si nécessaire.</p> <p><b>Bonne Pratique</b> Un processus de gestion des changements doit comporter des justificatifs que les exigences du standard PCI DSS sont mises en œuvre ou préservées par le biais d'un processus itératif.</p> <p><b>Exemples</b> Les exigences du standard PCI DSS qui doivent être vérifiées comportent, sans toutefois s'y limiter :</p> <ul style="list-style-type: none"> <li>• Les diagrammes de réseau sont mis à jour pour refléter les modifications.</li> <li>• Les systèmes sont configurés selon les standards de configuration, avec tous les mots de passe par défaut modifiés et les services inutiles désactivés.</li> <li>• Les systèmes sont protégés par les mesures de sécurité requis, par exemple, la surveillance de l'intégrité des fichiers, anti-programmes malveillants, les correctifs et la journalisation des audits.</li> </ul> <p>(suite à la page suivante)</p>

Exigences et Procédures de Test	Directives
	<ul style="list-style-type: none"> <li>Les données d'authentification sensibles ne sont pas stockées et tout le stockage des données de carte est documenté et intégré à la politique et aux procédures de conservation des données.</li> <li>De nouveaux systèmes sont inclus dans le processus trimestriel de scan des vulnérabilités.</li> </ul>
<p><b>Exigences de l'approche définie</b></p> <p><b>A3.2.3</b> Les modifications apportées à la structure de l'entreprise entraînent un examen formel (interne) de l'impact sur le périmètre du standard PCI DSS et l'applicabilité des mesures de sécurité.</p> <p><b>Référence du standard PCI DSS : Exigence 12</b></p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.3</b> Examiner les politiques et les procédures afin de vérifier qu'une modification de la structure de l'entreprise entraîne un examen formel de l'impact sur le périmètre du standard PCI DSS et l'applicabilité des mesures de sécurité.</p> <p><b>Objectif</b>  La structure et la gestion d'une entreprise définissent les exigences et le protocole pour des opérations efficaces et sécurisées. Les modifications apportées à cette structure pourraient avoir des effets négatifs sur les mesures de sécurité et les cadres existants en réaffectant ou en supprimant des ressources qui prenaient autrefois en charge les mesures de sécurité du standard PCI DSS, ou en héritant de nouvelles responsabilités qui n'avaient peut-être pas établi de mesures de sécurité en place. Par conséquent, il est important de revoir le périmètre et les mesures de sécurité du standard PCI DSS lorsque des modifications sont apportées à la structure et à la gestion d'une entreprise afin de s'assurer que les mesures de sécurité sont en place et actifs.</p> <p><b>Exemples</b>  Les modifications apportées à la structure de l'entreprise comprennent, sans toutefois s'y limiter, les fusions ou acquisitions d'entreprises et les modifications ou réaffectations importantes du personnel responsable du contrôle de la sécurité.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.4</b> Si la segmentation est utilisée, le périmètre du standard PCI DSS est confirmée comme suit :</p> <ul style="list-style-type: none"> <li>• Selon la méthodologie de l'entité définie à l'exigence 11.4.1.</li> <li>• Des tests d'intrusion sont effectués sur les mesures de sécurité de segmentation au moins une fois tous les six mois et après toute modification des mesures de sécurité/méthodes de segmentation.</li> <li>• Les tests d'intrusion couvrent tous les mesures de sécurité/méthodes de segmentation utilisés.</li> <li>• Le test d'intrusion vérifie que les mesures de sécurité ou méthodes de segmentation sont opérationnels et efficaces, et isoler le CDE de tous les systèmes hors de portée.</li> </ul> <p>Référence du standard PCI DSS : Exigence 11</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.4</b> Examiner les résultats du test d'intrusion le plus récent afin de vérifier que le test a été effectué conformément à tous les éléments spécifiés dans cette exigence.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Le standard PCI DSS exige normalement que les mesures de sécurité de segmentation soient vérifiées par des tests d'intrusion tous les douze mois.</p> <p>La validation plus fréquente des mesures de sécurité de segmentation est susceptible de découvrir des défaillances dans la segmentation avant qu'elles ne puissent être exploitées par un attaquant tentant de basculer latéralement d'un réseau non fiable hors de périmètre vers le CDE.</p> <p><b>Bonne Pratique</b> Bien que l'exigence précise que cette validation du périmètre est effectuée au moins une fois tous les six mois et après une modification importante, cet exercice doit être effectué aussi fréquemment que possible afin de s'assurer qu'il reste efficace pour isoler le CDE des autres réseaux.</p> <p><b>Informations Complémentaires</b> Se reporter au <i>Complément d'informations : Conseils pour des tests d'intrusion</i> pour des conseils supplémentaires.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.5</b> Une méthodologie de découverte de données est mise en œuvre qui :</p> <ul style="list-style-type: none"> <li>Confirme le périmètre du standard PCI DSS.</li> <li>Localise toutes les sources et tous les emplacements des PAN en texte clair au moins une fois tous les trois mois et lors de modifications importantes du CDE ou des processus.</li> <li>Traite de la possibilité que le PAN en texte clair réside sur des systèmes et des réseaux en dehors du CDE actuellement défini.</li> </ul> <p><b>Référence du standard PCI DSS : Périmètre des exigences du standard PCI DSS</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.5.a</b> Examiner la méthodologie de découverte de données documentée afin de vérifier qu'elle comporte tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.2.5.b</b> Examiner les résultats des récents efforts de découverte de données et interroger le personnel responsable afin de vérifier que la découverte de données est effectuée au moins une fois tous les trois mois et lors de modifications importantes du CDE ou des processus.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée</p>	<p><b>Objectif</b> Le standard PCI DSS exige que, dans le cadre de l'exercice de la portée, les entités évaluées identifient et documentent l'existence de tous les PAN en texte clair dans leurs environnements. La mise en œuvre d'une méthodologie de découverte de données qui identifie toutes les sources et tous les emplacements des PAN en texte clair et recherche des PAN en texte clair sur des systèmes et des réseaux en dehors du CDE actuellement défini, ou à des endroits imprévus au sein du CDE défini ; par exemple, dans un journal d'erreurs ou un fichier de vidage de mémoire, aide à garantir que les emplacements précédemment inconnus des PAN en texte clair sont détectés et correctement sécurisés.</p> <p><b>Exemples</b> Un processus de découverte de données peut être effectué via une variété de méthodes, y compris, sans toutefois s'y limiter, 1) un logiciel de découverte de données disponible dans le commerce, 2) un programme de découverte de données développé en interne ou 3) une recherche manuelle. Une combinaison de méthodologies peut également être utilisée selon les besoins.</p> <p>Indépendamment de la méthode utilisée, le but de l'effort est de trouver toutes les sources et tous les emplacements des PAN en texte clair (pas uniquement dans le CDE défini).</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.5.1</b> Les méthodes de découverte de données sont confirmées comme suit :</p> <ul style="list-style-type: none"> <li>• L'efficacité des méthodes est testée.</li> <li>• Les méthodes sont capables de découvrir le PAN en texte clair sur tous les types de composants système et les formats de fichiers utilisés.</li> <li>• L'efficacité des méthodes de découverte de données est confirmée au moins une fois tous les 12 mois.</li> </ul> <p><b>Référence du standard PCI DSS</b> : <i>Périmètre des exigences du standard PCI DSS</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.5.1.a</b> Interroger le personnel et examiner la documentation afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• L'entité a mis en place un processus pour tester l'efficacité des méthodes utilisées pour la découverte des données.</li> <li>• Le processus comprend la vérification que les méthodes sont capables de découvrir le PAN en texte clair sur tous les types de composants système et les formats de fichiers utilisés.</li> </ul> <p><b>A3.2.5.1.b</b> Examiner les résultats des tests d'efficacité afin de vérifier que l'efficacité des méthodes de découverte des données est confirmée au moins une fois tous les 12 mois.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Un processus de test de l'efficacité des méthodes utilisées pour la découverte des données garantit l'exhaustivité et l'exactitude de la détection des données de carte.</p> <p><b>Bonne Pratique</b> Pour l'exhaustivité, les composants du système dans les réseaux couverts et les systèmes dans les réseaux hors de périmètre doivent être inclus dans le processus de découverte des données. Le processus de découverte des données doit être efficace sur tous les systèmes d'exploitation et les plates-formes utilisés. L'exactitude peut être testée en plaçant des PAN de test sur les composants système et les formats de fichiers utilisés, et en confirmant que la méthode de découverte des données a détecté les PAN de test.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.5.2</b> Des procédures de réponse sont mises en œuvre pour être lancées lors de la détection d'un PAN en texte clair en dehors du CDE pour inclure :</p> <ul style="list-style-type: none"> <li>• Déterminer ce qu'il faut faire si le PAN en texte clair est découvert en dehors du CDE, y compris sa récupération, sa suppression sécurisée et/ou sa migration vers le CDE actuellement défini, selon le cas.</li> <li>• Déterminer comment les données se sont retrouvées en dehors du CDE.</li> <li>• Corriger les fuites de données ou les lacunes des processus qui ont fait que les données se trouvaient en dehors du CDE.</li> <li>• Identifier la source des données.</li> <li>• Identifier si des données de suivi sont stockées avec les PAN.</li> </ul>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.5.2.a</b> Examiner les procédures de réponse documentées afin de vérifier que les procédures de réponse à la détection d'un PAN en texte clair en dehors du CDE sont définies et incluent tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.2.5.2.b</b> Interroger le personnel et examiner les enregistrements des actions de réponse afin de vérifier que les activités correctives sont effectuées lorsqu'un PAN en texte clair est détecté en dehors du CDE.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Avoir des procédures de réponse documentées qui sont suivies dans le cas où un PAN en texte clair est trouvé en dehors du CDE aide à identifier les mesures correctives nécessaires et à prévenir de futures fuites.</p> <p><b>Bonne Pratique</b> Si le PAN a été trouvé en dehors du CDE, une analyse doit être effectuée pour 1) déterminer s'il a été enregistré indépendamment d'autres données ou avec des données d'authentification sensibles, 2) identifier la source des données et 3) identifier les lacunes de contrôle qui ont entraîné que les données soient en dehors du CDE.</p> <p>Les entités doivent déterminer si des facteurs contributifs, tels que des processus professionnels, le comportement des utilisateurs, des configurations système inappropriées, etc. ont entraîné le stockage du PAN dans un emplacement imprévu. Si de tels facteurs contributifs sont présents, ils doivent être traités conformément à cette exigence afin d'éviter qu'ils ne se reproduisent.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.6</b> Des mécanismes sont mis en œuvre pour détecter et empêcher les PAN en texte clair de quitter le CDE via un canal, une méthode ou un processus non autorisé, y compris des mécanismes qui :</p> <ul style="list-style-type: none"> <li>• Sont en cours d'exécution.</li> <li>• Sont configurés pour détecter et empêcher les PAN en texte clair de quitter le CDE via un canal, une méthode ou un processus non autorisé.</li> <li>• Génèrent des journaux d'audit et d'alertes lors de la détection d'un PAN en texte clair quittant le CDE via un canal, une méthode ou un processus non autorisé.</li> </ul> <p><b>Référence du standard PCI DSS</b> : <i>Périmètre des exigences du standard PCI DSS, Exigence 12</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.6.a</b> Examiner la documentation et observer les mécanismes mis en œuvre afin de vérifier que les mécanismes sont conformes à tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.2.6.b</b> Examiner les journaux d'audit et les alertes, et interroger le personnel responsable afin de vérifier que les alertes font l'objet d'une enquête.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> L'utilisation de mécanismes pour détecter et empêcher les PAN non autorisés de quitter le CDE permet à une entreprise de détecter et de prévenir les situations pouvant entraîner une perte de données.</p> <p><b>Bonne Pratique</b> La couverture des mécanismes devrait comprendre, sans toutefois s'y limiter, les courriels, les téléchargements sur des supports amovibles et les sorties vers des imprimantes.</p> <p><b>Exemples</b> Les mécanismes de détection et de prévention de la perte non autorisée de PAN en texte clair peuvent inclure l'utilisation d'outils appropriés tels que des solutions de prévention des pertes de données (DLP) ainsi que des processus et procédures manuels.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.2.6.1</b> Des procédures de réponse sont mises en œuvre pour être lancées lors de la détection de tentatives de suppression de PAN en texte clair du CDE via un canal, une méthode ou un processus non autorisé. Les procédures de réponse comprennent :</p> <ul style="list-style-type: none"> <li>• Des procédures d'examen rapide des alertes par le personnel responsable.</li> <li>• Des procédures pour corriger les fuites de données ou les lacunes des processus, si nécessaire, afin d'éviter toute perte de données.</li> </ul> <p>Référence du standard PCI DSS : Exigence 12</p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.2.6.1.a</b> Examiner les procédures de réponse documentées afin de vérifier que les procédures de réponse à la tentative de suppression de PAN en texte clair du CDE via un canal, une méthode ou un processus non autorisé comportent tous les éléments spécifiés dans cette exigence :</p> <ul style="list-style-type: none"> <li>• Des procédures d'examen rapide des alertes par le personnel responsable.</li> <li>• Des procédures pour corriger les fuites de données ou les lacunes des processus, si nécessaire, afin d'éviter toute perte de données.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b></p> <p>Les tentatives de suppression des PAN en texte clair via un canal, une méthode ou un processus non autorisé peuvent indiquer une intention malveillante de voler des données, ou peuvent être les actions d'un employé autorisé qui ne connaît pas ou ne suit tout simplement pas les méthodes adéquates. Une enquête rapide sur ces événements peut identifier les endroits où des mesures correctives doivent être appliquées, et fournit des informations précieuses pour aider à comprendre l'origine des menaces.</p>

Exigences et Procédures de Test	Directives
<b>A3.3 Le standard PCI DSS est intégrée aux activités courantes (BAU).</b>	
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.3.1</b> Les défaillances des systèmes de contrôle de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances :</p> <ul style="list-style-type: none"> <li>• Des mesures de sécurité réseau</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Des solutions anti-programmes malveillants</li> <li>• Les mesures de sécurité d'accès physiques</li> <li>• Les mesures de sécurité d'accès logiques</li> <li>• Des mécanismes de journalisation des audits</li> <li>• Des mesures de segmentation (le cas échéant)</li> <li>• Des mécanismes automatisés d'examen des Journaux d'audit <i>Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</i></li> <li>• Outils automatisés d'examen du code (le cas échéant). <i>Ce point est une Bonne Pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes D'applicabilité ci-dessous pour plus de détails.</i></li> </ul> <p><b>Référence du standard PCI DSS : Exigences 1 à 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.3.1.a</b> Examiner les politiques et procédures documentées afin de vérifier que les processus sont définis pour détecter, alerter et résoudre rapidement les défaillances critiques des mesures de sécurité de sécurité conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.3.1.b</b> Examiner les processus de détection et d'alerte, et interroger le personnel afin de vérifier que les processus sont mis en œuvre pour tous les mesures de sécurité de sécurité critiques spécifiés dans cette exigence et que chaque défaillance d'un contrôle de sécurité critique entraîne la génération d'une alerte.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p> <p>(suite à la page suivante)</p>	<p><b>Objectif</b></p> <p>Sans processus formels pour la détection rapide (dès que possible), l'alerte et le traitement des défaillances critiques des mesures de sécurité de sécurité, les défaillances peuvent passer inaperçues ou rester non résolues pendant de longues périodes. De plus, sans processus formalisés limités dans le temps, les attaquants auront amplement le temps de compromettre les systèmes et de voler les données de carte du CDE.</p> <p><b>Bonne Pratique</b></p> <p>Les types spécifiques de pannes peuvent varier selon la fonction du composant système de l'appareil et de la technologie utilisée. Les défaillances typiques incluent un système cessant d'exécuter sa fonction de sécurité ou ne fonctionnant pas de la manière prévue, tel un pare-feu effaçant toutes ses règles ou se déconnectant.</p>

Exigences et Procédures de Test	Directives
<p><b>Notes D'applicabilité</b></p> <p><i>Les puces ci-dessus (pour les mécanismes automatisés d'examen des journaux et les outils automatisés d'examen du code (le cas échéant)) constituent de meilleures pratiques jusqu'au 31 mars 2025. Après cette date elles seront obligatoires dans le cadre de l'exigence A3.3.1 et doivent être pleinement prises en compte lors d'une évaluation du standard PCI DSS.</i></p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.3.1.1</b> Les défaillances de tout système de contrôle de sécurité critique sont traitées rapidement. Les processus de réponse aux défaillances des systèmes de contrôle de sécurité comprennent :</p> <ul style="list-style-type: none"> <li>Restauration des fonctions de sécurité.</li> <li>Identifier et documenter la durée (date et heure du début à la fin) de la défaillance de sécurité.</li> <li>Identifier et documenter la ou les causes de la défaillance, y compris la cause profonde, et documenter les mesures correctives nécessaires pour traiter la cause profonde.</li> <li>Identifier et résoudre tous les problèmes de sécurité survenus lors de la défaillance.</li> <li>Déterminer si d'autres mesures sont nécessaires à la suite de la défaillance de sécurité.</li> <li>Mettre en œuvre des mesures afin d'éviter que la cause de la défaillance ne se reproduise.</li> <li>Reprendre la surveillance des mesures de sécurité.</li> </ul> <p><b>Référence du standard PCI DSS : Exigences 1 à 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.3.1.1.a</b> Examiner les politiques et procédures documentées et interroger le personnel afin de vérifier que les processus sont définis et mis en œuvre pour répondre rapidement à une défaillance des mesures de sécurité de sécurité conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.3.1.1.b</b> Examiner les enregistrements afin de vérifier que les défaillances des mesures de sécurité de sécurité sont documentées pour inclure :</p> <ul style="list-style-type: none"> <li>L'identification de la ou des causes de la défaillance, y compris la cause profonde.</li> <li>La durée (date et heure de début et de fin) de la défaillance de sécurité.</li> <li>Les détails des correctifs nécessaires pour traiter la cause profonde.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Si les alertes de défaillances des systèmes de contrôle de sécurité critiques ne sont pas traitées rapidement et efficacement, les attaquants peuvent utiliser ce temps pour insérer des logiciels malveillants, prendre le contrôle d'un système ou voler des données dans l'environnement de l'entité.</p> <p><b>Bonne Pratique</b> Des preuves documentées (par exemple, des enregistrements dans un système de gestion des problèmes) doivent appuyer les processus et les procédures en place qui répondent aux défaillances de sécurité. De plus, le personnel doit être conscient de ses responsabilités en cas de défaillance. Les actions et les réponses à l'échec doivent être consignées dans les preuves documentées.</p>

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.3.2</b> Les technologies matérielles et logicielles sont examinées au moins une fois tous les 12 mois pour confirmer si elles continuent de répondre aux exigences du standard PCI DSS de l'entreprise.</p> <p><b>Référence du standard PCI DSS :</b> <i>Exigences 2, 6, 12.</i></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.3.2.a</b> Examiner les politiques et procédures documentées et interroger le personnel afin de vérifier que les processus sont définis et mis en œuvre pour examiner les technologies matérielles et logicielles afin de confirmer si elles continuent de répondre aux exigences du standard PCI DSS de l'entreprise.</p> <p><b>A3.3.2.b</b> Examiner les résultats des examens récents des technologies matérielles et logicielles afin de vérifier que les examens sont effectués au moins une fois tous les 12 mois.</p> <p><b>A3.3.2.c</b> Examiner la documentation afin de vérifier que, pour toutes les technologies qui ont été déterminées comme ne répondant plus aux exigences du standard PCI DSS de l'entreprise, un plan est en place pour corriger la technologie.</p>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Les technologies matérielles et logicielles évoluent constamment, et les entreprises doivent être conscientes des changements apportés aux technologies qu'elles utilisent, ainsi que des menaces en constante évolution qui pèsent sur ces technologies. La réalisation d'examens appropriés de ces technologies garantit qu'elles peuvent se préparer à, et gérer les vulnérabilités du matériel et des logiciels qui ne seront pas corrigées par le fournisseur ou le développeur.</p> <p><b>Bonne Pratique</b> Les entreprises doivent également envisager d'examiner les versions du micrologiciel afin de s'assurer qu'elles restent à jour et prises en charge par les fournisseurs.</p> <p>Les entreprises doivent également être conscientes des modifications apportées par les fournisseurs de technologies à leurs produits ou processus pour comprendre la manière dont ces modifications peuvent avoir une incidence sur l'utilisation de la technologie par l'entreprise.</p> <p>Des examens réguliers des technologies qui ont un impact ou une influence sur les mesures de sécurité du standard PCI DSS peuvent aider à l'achat, à l'utilisation et aux stratégies de déploiement, et garantir que les mesures de sécurité qui reposent sur ces technologies restent efficaces. Ces examens comportent, sans toutefois s'y limiter, l'examen des technologies qui ne sont plus prises en charge par le fournisseur et/ou qui ne répondent plus aux besoins de sécurité de l'entreprise.</p>
<p><b>Notes D'applicabilité</b></p> <p>Le processus comprend un plan de correction des technologies qui ne répondent plus aux exigences du standard PCI DSS de l'entreprise, jusqu'au remplacement de la technologie, le cas échéant.</p>	

Exigences et Procédures de Test	Directives
<p><b>Exigences de L'approche Définie</b></p> <p><b>A3.3.3</b> Des examens sont effectués au moins une fois tous les trois mois afin de vérifier que les activités BAU sont suivies. Des examens sont effectués par le personnel affecté au programme de conformité au standard PCI DSS (tel qu'identifié en A3.1.3) et comprennent :</p> <ul style="list-style-type: none"> <li>La confirmation que toutes les activités BAU, y compris A3.2.2, A3.2.6 et A3.3.1, sont effectuées.</li> <li>La confirmation que le personnel suit les politiques de sécurité et les procédures opérationnelles (par exemple, examens quotidiens des journaux, examens des ensembles de règles pour les mesures de sécurité du réseau, standards de configuration pour les nouveaux systèmes).</li> <li>La documentation de la façon dont les examens ont été effectués, y compris la façon dont toutes les activités BAU ont été vérifiées comme étant en place.</li> <li>La collecte de preuves documentées requises pour l'évaluation annuelle du standard PCI DSS.</li> <li>Examen et approbation des résultats par le personnel affecté à la responsabilité du programme de conformité PCI DSS, tel qu'identifié en A3.1.3.</li> <li>La conservation des enregistrements et de la documentation pendant au moins 12 mois, couvrant toutes les activités BAU.</li> </ul> <p><b>Référence du standard PCI DSS : Exigences 1 à 12</b></p>	<p><b>Procédures de Test de L'approche Définie</b></p> <p><b>A3.3.3.a</b> Examiner les politiques et procédures afin de vérifier que des processus sont définis pour examiner et vérifier les activités BAU conformément à tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.3.3.b</b> Interroger le personnel responsable et consulter les enregistrements des examens afin de vérifier que :</p> <ul style="list-style-type: none"> <li>Des examens sont effectués par le personnel affecté au programme de conformité au standard PCI DSS.</li> <li>Des examens sont effectués au moins une fois tous les trois mois.</li> </ul>
<p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<p><b>Objectif</b> Une confirmation régulière que les politiques et procédures de sécurité sont suivies donne l'assurance que les mesures de sécurité attendue sont actives et fonctionnent comme prévu. L'objectif de ces examens n'est pas d'effectuer à nouveau d'autres exigences PCI DSS, mais de confirmer que les activités de sécurité sont effectuées de manière continue.</p> <p><b>Bonne Pratique</b> Ces examens peuvent également être utilisés afin de vérifier que les preuves appropriées sont conservées (par exemple, journaux d'audit, rapports d'analyse de vulnérabilités, examens des ensembles de règles de contrôle de sécurité réseau) pour aider l'entité à préparer sa prochaine évaluation du standard PCI DSS.</p> <p><b>Exemples</b> Prenant l'exigence 1.2.7 comme exemple, l'exigence A3.3.3 est satisfaite en confirmant, au moins une fois tous les trois mois, que les examens des configurations des mesures de sécurité de sécurité réseau ont eu lieu à la fréquence requise. D'autre part, l'exigence 1.2.7 est satisfaite en examinant ces configurations comme spécifié dans l'exigence.</p>

Exigences et Procédures de Test	Directives
<b>A3.4 L'accès logique à l'environnement des données des titulaires de cartes est contrôlé et géré.</b>	
<b>Exigences de L'approche Définie</b> <p><b>A3.4.1</b> Les comptes d'utilisateurs et les priviléges d'accès aux composants système dans le périmètre sont examinés au moins une fois tous les six mois pour s'assurer que les comptes d'utilisateurs et les priviléges d'accès restent appropriés selon la fonction, et que tous les accès sont autorisés.</p> <p><b>Référence du standard PCI DSS : Exigence 7</b></p> <p><b>Objectif de L'approche Personnalisée</b></p> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<b>Procédures de Test de L'approche Définie</b> <p><b>A3.4.1</b> Interroger le personnel responsable et examiner les documents justificatifs afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• Les comptes d'utilisateurs et les priviléges d'accès sont examinés au moins tous les six mois.</li> <li>• Les examens confirment que l'accès est approprié selon la fonction et que tous les accès sont autorisés.</li> </ul>
	<b>Objectif</b> <p>L'examen régulier des droits d'accès permet de détecter les droits d'accès excessifs restants après le changement des responsabilités professionnelles de l'utilisateur, le changement des fonctions du système ou autres changements. Si des droits excessifs d'un utilisateur ne sont pas révoqués en temps utile, ils peuvent être exploités par des utilisateurs malveillants pour un accès non autorisé.</p> <p>Cet examen offre une autre possibilité de s'assurer que les comptes de tous les utilisateurs ayant terminé leurs tâches ont été supprimés (le cas échéant, au moment de la fin de leurs tâches), ainsi que de s'assurer que tout tiers qui n'a plus besoin d'accès a vu son accès suspendu.</p>

Exigences et Procédures de Test	Directives
<b>A3.5 Les événements suspects sont identifiés et traités.</b>	
<b>Exigences de L'approche Définie</b> <p><b>A3.5.1</b> Une méthodologie est mise en œuvre pour l'identification rapide des modèles d'attaque et des comportements indésirables sur les systèmes, qui comprend :</p> <ul style="list-style-type: none"> <li>• L'identification des anomalies ou des activités suspectes au fur et à mesure qu'elles se produisent.</li> <li>• L'émission d'alertes rapides lors de la détection d'une activité suspecte ou d'une anomalie au personnel responsable.</li> <li>• Une réponse aux alertes conformément aux procédures de réponse documentées.</li> </ul> <p><b>Référence du standard PCI DSS : Exigences 10, 12</b></p>	<b>Procédures de Test de L'approche Définie</b> <p><b>A3.5.1.a</b> Examiner la documentation et interroger le personnel afin de vérifier qu'une méthodologie est définie et mise en œuvre pour identifier rapidement les modèles d'attaque et les comportements indésirables sur les systèmes, et comporte tous les éléments spécifiés dans cette exigence.</p> <p><b>A3.5.1.b</b> Examiner les procédures de réponse aux incidents et interroger le personnel responsable afin de vérifier que :</p> <ul style="list-style-type: none"> <li>• Le personnel en service de garde reçoit des alertes rapides.</li> <li>• Les alertes sont traitées conformément aux procédures de réponse documentées.</li> </ul>
<b>Objectif de L'approche Personnalisée</b> <p>Cette exigence n'est pas admissible pour l'approche personnalisée.</p>	<b>Objectif</b> <p>La capacité d'identifier les modèles d'attaque et les comportements indésirables sur l'ensemble des systèmes ; par exemple, à l'aide d'outils de corrélation de journaux gérés de manière centralisée ou automatisés, est essentielle afin de prévenir, détecter ou minimiser l'impact d'une compromission des données. La présence de journaux dans tous les environnements permet un suivi, une alerte et une analyse approfondis en cas de problème. Il est très difficile, voire impossible, de déterminer la cause d'une compromission sans un processus permettant de corroborer les informations des composants système critiques et des systèmes qui exécutent des fonctions de sécurité, telles que les mesures de sécurité de réseau, IDS/IPS et les systèmes de surveillance de l'intégrité des fichiers (FIM). Ainsi, les journaux de tous les composants système critiques et des systèmes qui exécutent des fonctions de sécurité doivent être recueillis, corrélatifs et conservés. Cela peut inclure l'utilisation de produits logiciels et de méthodologies de service afin de fournir des analyses, des alertes et des rapports en temps réel, tels que la gestion des informations et des événements de sécurité (SIEM), FIM ou la détection des modifications.</p>

## Annexe B Mesures de Sécurité Compensatoires

Des mesures de sécurité peuvent être envisagées lorsqu'une entité ne peut pas répondre à une exigence du standard PCI DSS explicitement comme indiqué, en raison de contraintes techniques ou métier légitimes et documentées, mais a suffisamment atténué le risque associé à la non satisfaction à l'exigence en mettant en œuvre d'autres mesures ou des mesures compensatoires.

Les mesures compensatoires doivent répondre aux critères suivants :

1. Répondre à l'intention et la rigueur de l'exigence d'origine du standard PCI DSS.
2. Fournir un niveau de défense similaire à celui de l'exigence d'origine du standard PCI DSS, de sorte que la mesure compensatoire compense suffisamment le risque contre lequel l'exigence d'origine du standard PCI DSS était conçue pour se défendre. Pour comprendre l'intention d'une exigence, se reporter à *l'objectif d'approche personnalisée* pour la plupart des exigences du standard PCI DSS. Si une exigence n'est pas éligible à l'approche personnalisée et n'a donc pas d'objectif d'approche personnalisée, se reporter à **l'Objectif** dans la colonne Conseils pour cette exigence.
3. Être « au-dessus et au-delà » des autres exigences du standard PCI DSS. (Le simple fait d'être en conformité avec d'autres exigences du standard PCI DSS n'est pas recevable en tant que mesure compensatoire.)
4. Lors de l'évaluation « au-dessus et au-delà » pour les mesures compensatoires, tenez compte des éléments suivants :
  - a) Les exigences existantes du standard PCI DSS NE PEUVENT PAS être considérées comme des mesures compensatoires si elles sont déjà obligatoires pour l'élément en cours d'examen. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être envoyés chiffrés pour atténuer le risque d'interception des mots de passe administratifs en texte clair. Une entité ne peut pas utiliser d'autres exigences de mot de passe du standard PCI DSS (verrouillage anti-intrusion, mots de passe complexes, etc.) pour compenser l'absence de mots de passe chiffrés, car ces autres exigences relatives aux mots de passe n'atténuent pas le risque d'interception des mots de passe en texte clair. En outre, les autres mesures de renforcement de mot de passe sont déjà des exigences du standard PCI DSS pour l'élément en cours d'examen (mots de passe).
  - b) Les exigences existantes du standard PCI DSS PEUVENT être considérées comme des mesures compensatoires si elles sont obligatoires pour un autre domaine mais ne sont pas obligatoires pour l'élément en cours d'examen.

**Remarque :** Toutes les mesures compensatoires doivent être examinées et validées pour leur suffisance par l'auditeur qui effectue l'évaluation du standard PCI DSS. L'efficacité d'une mesure compensatoire dépend des spécificités de l'environnement dans lequel la mesure est mise en œuvre, des autres mesures de sécurité au sein de périmètre concerné et de la configuration de la mesure. Les entités doivent être conscientes qu'une mesure compensatoire donnée ne sera pas efficace dans tous les environnements.

- c) Les exigences existantes du standard PCI DSS peuvent être combinées avec de nouvelles mesures pour devenir une mesure compensatoire. Par exemple, si une entreprise est incapable de résoudre une vulnérabilité exploitable via une interface réseau, car une mise à jour de sécurité n'est pas encore disponible auprès d'un fournisseur, une mesure compensatoire peut consister en des mesures qui incluent tous les éléments suivants : 1) une segmentation du réseau interne, 2) une limitation de l'accès réseau à l'interface vulnérable aux seuls périphériques requis (filtrage d'adresse IP ou d'adresse MAC) et 3) surveillance IDS/IPS de tout le trafic destiné à l'interface vulnérable.
- 5. Traiter le risque supplémentaire imposé par le non-respect de l'exigence du standard PCI DSS.
- 6. Traiter à l'exigence actuelle et future. Une mesure compensatoire ne peut pas satisfaire à une exigence qui a été ignorée dans le passé (par exemple, lorsque l'exécution d'une tâche était requise il y a deux trimestres, mais que cette tâche n'a pas été effectuée).

L'auditeur est tenu d'évaluer minutieusement les mesures compensatoires lors de chaque évaluation annuelle du standard PCI DSS afin de confirmer que chaque mesure compensatoire traite de manière adéquate le risque que l'exigence d'origine du standard PCI DSS a été conçue pour traiter, conformément aux éléments 1 à 5 ci-dessus.

Pour maintenir la conformité, des processus et des mesures de sécurité réguliers doivent être en place pour s'assurer que les mesures compensatoires restent efficaces une fois l'évaluation terminée. De plus, les résultats des mesures compensatoires doivent être documentés dans le rapport applicable pour l'évaluation (par exemple, un rapport sur la conformité ou un questionnaire d'auto-évaluation) dans la section correspondante des exigences du standard PCI DSS, et inclus lorsque le rapport applicable est soumis à l'entreprise requérante.

## Annexe C Fiche D'Identification des Mesures Compensatoires

L'entité doit utiliser cette fiche d'identification pour définir des mesures compensatoires pour toute exigence où des mesures compensatoires sont utilisées pour satisfaire à une exigence du standard PCI DSS. À noter que les mesures compensatoires doivent également être documentées conformément aux instructions du rapport de conformité dans la section correspondante des exigences du standard PCI DSS.

**Remarque :** Seules les entités qui ont des contraintes techniques ou métier légitimes et documentées peuvent envisager l'utilisation de mesures compensatoires pour satisfaire à la conformité.

### Numéro et Définition de L'exigence :

	Informations Requises	Explication
<b>1. Contraintes</b>	Documenter les contraintes techniques ou métier légitimes empêchant la conformité à l'exigence d'origine.	
<b>2. Définition des Mesures Compensatoires</b>	Définir les mesures compensatoires : expliquer comment elles répondent aux objectifs de la mesure d'origine et au risque accru, le cas échéant.	
<b>3. Objectif</b>	Définir l'objectif de la mesure de sécurité d'origine (par exemple, l'objectif de l'approche personnalisée).	
	Identifier l'objectif atteint par la mesure compensatoire ( <i>remarque : cela peut être, sans que toutefois ce ne soit obligatoire, l'objectif d'approche personnalisée déclaré pour l'exigence du standard PCI DSS</i> ).	
<b>4. Risque Identifié</b>	Identifier tout risque supplémentaire posé par l'absence de la mesure de sécurité d'origine.	
<b>5. Validation des Mesures Compensatoires</b>	Définir la manière dont les mesures compensatoires ont été validées et testées.	
<b>6. Maintenance</b>	Définir le ou les processus et les mesures en place pour maintenir les mesures compensatoires.	

## Annexe D Approche Personnalisée

Cette approche est destinée aux entités qui décident de satisfaire à l'objectif de l'approche personnalisée d'une exigence du standard PCI DSS d'une manière qui ne suit pas strictement l'exigence définie. L'approche personnalisée permet à une entité d'adopter une approche stratégique pour satisfaire à l'objectif de l'approche personnalisée d'une exigence, afin qu'elle puisse déterminer et concevoir les mesures de sécurité nécessaires pour atteindre l'objectif d'une manière unique pour cette entreprise.

**L'entité** mettant en œuvre une approche personnalisée doit répondre aux critères suivants :

- Documenter et conserver des preuves sur chaque mesure de sécurité personnalisée, y compris toutes les informations spécifiées dans le modèle de matrice de mesures de sécurité dans *PCI DSS v4.x : Exemples de Modèles pour Prendre en Charge l'Approche Personnalisée* sur le site Web du PCI SSC.
- Effectuer et documenter une analyse ciblée de risques (exigence 12.3.2 du standard PCI DSS) pour chaque mesure de sécurité personnalisée, y compris toutes les informations spécifiées dans le modèle d'analyse ciblée de risques dans *PCI DSS v4.x : Exemples de Modèles pour Prendre en Charge l'Approche Personnalisée* sur le site Web du PCI SSC.
- Effectuer des tests de chaque mesure de sécurité personnalisée pour prouver l'efficacité, et documenter les tests effectués, les méthodes utilisées, les éléments testés, les dates auxquels les tests ont été effectués et les résultats des tests dans la matrice des mesures de sécurité.
- Surveiller et conserver des preuves de l'efficacité de chaque mesure de sécurité personnalisée.
- Fournir à son auditeur la ou les matrices de mesures de sécurité remplies, l'analyse ciblée de risques, les justificatifs du test et les preuves de l'efficacité des mesures de sécurité personnalisées.

**L'auditeur** effectuant une évaluation des mesures de sécurité personnalisées doit satisfaire aux critères suivants :

- Examiner la ou les matrices de mesures de sécurité de l'entité, l'analyse ciblée de risques et les preuves de l'efficacité des mesures de sécurité afin de bien comprendre la ou les mesures de sécurité personnalisées et de vérifier que l'entité réponde à toutes les exigences en matière de documentation et de preuves de l'approche personnalisée.
- Obtenir et documenter les procédures de test appropriées nécessaires afin d'effectuer des tests approfondis de chaque mesure de sécurité personnalisée.
- Tester chaque mesure de sécurité personnalisée afin de déterminer si la mise en œuvre de l'entité 1) répond à l'objectif de l'approche personnalisée de l'exigence et 2) aboutit à des résultats « en place » pour l'exigence.
- À tout moment, les QSA maintiennent les exigences d'indépendance définies dans les exigences de qualification des QSA. Cela signifie que si un QSA est impliqué dans la conception ou la mise en œuvre d'une mesure de sécurité personnalisée, ce QSA n'obtient pas également de procédures de test pour, n'évalue pas ou n'aide pas à l'évaluation de cette mesure de sécurité personnalisée.

L'entité et son auditeur doivent collaborer pour s'assurer 1) qu'ils conviennent que la ou les mesures de sécurité personnalisées répondent pleinement à l'objectif de l'approche personnalisée, 2) que l'auditeur comprend parfaitement la mesure de sécurité personnalisée et 3) que l'entité comprend les tests dérivés que l'auditeur effectuera.

L'utilisation de l'approche personnalisée doit être documentée par un QSA ou un ISA conformément aux instructions du modèle de rapport de conformité (ROC) et en suivant les instructions de la *FAQ à utiliser avec le modèle ROC du standard PCI DSS v4.x* disponible sur le site Internet PCI SSC.

Les entités qui remplissent un questionnaire d'auto-évaluation ne sont pas éligibles pour utiliser une approche personnalisée ; cependant, ces entités peuvent choisir de demander à un QSA ou à un ISA d'effectuer son évaluation et de la documenter dans un modèle ROC.

L'utilisation de l'approche personnalisée peut être réglementée par les entreprises qui gèrent les programmes de conformité (par exemple, les réseaux internationaux de paiement et les acquéreurs). Par conséquent, les questions concernant l'utilisation d'une approche personnalisée doivent être adressées à ces entreprises, y compris, par exemple, si une entité est tenue d'utiliser un QSA ou peut utiliser un ISA pour effectuer une évaluation en utilisant l'approche personnalisée.

**Remarque :** *Les mesures compensatoires ne sont pas une option avec l'approche personnalisée. Étant donné que l'approche personnalisée permet à une entité de déterminer et de concevoir les mesures de sécurité nécessaires afin de satisfaire à l'objectif de l'approche personnalisée d'une exigence, l'entité est censée mettre en œuvre efficacement les mesures qu'elle a conçues pour cette exigence sans avoir à mettre également en œuvre d'autres mesures compensatoires.*

## Annexe E Exemples de Modèles pour Soutenir une Approche Personnalisée

Cette annexe contient des exemples de modèles de matrice de mesures de sécurité et d'analyse ciblée de risques, à documenter par l'entité dans le cadre de l'approche personnalisée. Ces modèles sont des exemples de formats qui pourraient être utilisés. *Bien qu'il ne soit pas nécessaire que les entités suivent les formats spécifiques fournis dans cette annexe, la matrice de mesure de sécurité et l'analyse ciblée de risques de l'entité doivent inclure toutes les informations telles que définies dans ces modèles.*

Ces exemples de modèles sont disponibles sur le site Web du PCI SSC.

## Annexe F Utiliser le Cadre de Sécurité Logicielle PCI pour Répondre à L'exigence 6

L'exigence 6 du standard PCI DSS définit les exigences pour le développement et la maintenance de systèmes et de logiciels sécurisés. Étant donné que le standard PCI SSC Secure Software et le standard Secure SLC (collectivement, le cadre de sécurité logicielle appelé "Secure Software Framework") comportent des exigences de sécurité logicielle rigoureuses, l'utilisation de logiciels sur mesure et personnalisés développés et maintenus conformément à l'une ou l'autre des standards peut aider l'entité à satisfaire à plusieurs exigences de l'exigence 6 du standard PCI DSS sans avoir à effectuer de tests détaillés supplémentaires, et peut également prendre en charge l'utilisation de l'approche personnalisée pour d'autres exigences. Pour plus de détails, voir le tableau 7.

**Remarque :** *Cette prise en charge pour satisfaire à l'exigence 6 s'applique uniquement aux logiciels qui sont spécifiquement développés et maintenus conformément à le standard Secure Software Standard ou à le standard Secure SLC ; elle ne s'étend pas aux autres composants logiciels ou système dans le cadre de l'exigence 6.*

**Tableau 7. Exploiter le Cadre de Sécurité Logicielle PCI pour Prendre en Charge L'exigence 6**

Exigences du Standard PCI DSS	Comment les Exigences PCI DSS S'appliquent aux Logiciels Développés et Maintenus Conformément à le Standard Secure Software Standard	Comment les Exigences PCI DSS S'appliquent aux Logiciels Développés et Maintenus Conformément à le Standard SLC
6.1 Les processus et mécanismes d'exécution des activités de l'Exigence 6 sont définis et compris.	Les exigences/objectifs du standard PCI DSS s'appliquent comme d'habitude.	
6.2 Les logiciels sur mesure et personnalisés sont développés de manière sécurisée.	L'exigence 6.2.4 du standard PCI DSS peut être considérée comme en place pour les logiciels développés et maintenus conformément au standard SLC.	L'exigence 6.2 du standard PCI DSS peut être considérée comme en place pour les logiciels développés et maintenus conformément au standard SLC.
6.3 Les vulnérabilités de sécurité sont identifiées et corrigées.	Les exigences/objectifs du standard PCI DSS s'appliquent comme d'habitude. Les logiciels développés et maintenus conformément à le standard Secure SLC peuvent prendre en charge l'approche personnalisée pour les objectifs de l'exigence 6.3. Alors que l'utilisation de logiciels développés et maintenus conformément à le standard Secure SLC fournit l'assurance que le fournisseur met à disposition les correctifs de sécurité et les mises à jour logicielles en temps opportun, <b>l'entité conserve la responsabilité</b> de s'assurer que les correctifs et les mises à jour sont installés conformément aux exigences du standard PCI DSS.	

Exigences du Standard PCI DSS	Comment les Exigences PCI DSS S'appliquent aux Logiciels Développés et Maintenus Conformément à le Standard Secure Software Standard	Comment les Exigences PCI DSS S'appliquent aux Logiciels Développés et Maintenus Conformément à le Standard SLC
<b>6.4</b> Les applications Web destinées au public sont protégées contre les attaques.	Les exigences/objectifs du standard PCI DSS s'appliquent comme d'habitude.	
<b>6.5</b> Les modifications apportées à tous les composants système sont gérées de manière sécurisée.	Les exigences/objectifs du standard PCI DSS s'appliquent comme d'habitude. Les logiciels développés et maintenus conformément à le standard Secure SLC peuvent prendre en charge l'approche personnalisée pour les objectifs de l'exigence 6.5. Alors que l'utilisation de logiciels développés et maintenus conformément à le standard Secure SLC fournit l'assurance que le fournisseur suit les procédures de gestion des changements lors du développement des logiciels et des mises à jour associées, <b>l'entité conserve la responsabilité</b> de s'assurer que les logiciels et les autres modifications apportées aux composants système sont mises en œuvre dans son environnement de production conformément aux exigences du standard PCI DSS.	

### ***L'utilisation de Logiciels sur Mesure et Personnalisés Développés et Maintenus par un Fournisseur Qualifié Secure SLC***

Lors de la validation de l'utilisation d'un logiciel développé et maintenu par un fournisseur qualifié Secure SLC pour satisfaire à l'exigence 6.2 du standard PCI DSS et prendre en charge l'approche personnalisée pour les exigences 6.3 et 6.5, l'auditeur doit confirmer que les éléments suivants sont satisfaits :

- Le fournisseur de logiciels figure actuellement sur la liste du PCI SSC des fournisseurs qualifiés Secure SLC, c'est-à-dire que la validation est toujours en vigueur.
- Le logiciel a été développé et est maintenu à l'aide de pratiques de gestion du cycle de vie du logiciel qui ont été évaluées dans le cadre de la validation du fournisseur du logiciel.
- L'entité suit les directives de mise en œuvre fournies par le fournisseur qualifié Secure SLC.

### ***L'utilisation de Logiciels sur Mesure et Personnalisés Développés Conformément à le Standard Secure SLC***

Les entités qui développent en interne des logiciels uniquement pour leur usage ou qui développent des logiciels pour une utilisation par une seule entité peuvent choisir d'engager un auditeur Secure SLC afin d'évaluer leurs pratiques de gestion du cycle de vie des logiciels par rapport à le standard Secure SLC. L'auditeur Secure SLC documentera les résultats de l'évaluation dans un rapport de conformité Secure SLC (ROC) et une attestation de conformité Secure SLC (AOC).

Les logiciels développés et maintenus conformément aux pratiques de gestion du cycle de vie des logiciels fournissent la même prise en charge pour l'exigence 6 du standard PCI DSS que les logiciels développés et maintenus par un fournisseur qualifié Secure SLC, si ces pratiques ont été évaluées par un auditeur Secure SLC et confirmées comme conformes aux exigences du standard Secure SLC, avec les résultats documentés dans un ROC et une AOC Secure SLC.

### **Validation de L'utilisation du Standard Secure SLC**

Lors de la validation de l'utilisation d'un logiciel développé et maintenu conformément à le standard Secure SLC pour répondre à l'exigence 6.2 du standard PCI DSS et prendre en charge une approche personnalisée pour les exigences 6.3 et 6.5, l'auditeur doit confirmer que les conditions suivantes sont remplies :

- Les pratiques de gestion du cycle de vie des logiciels ont été évaluées par un auditeur Secure SLC et confirmées comme conformes à toutes les exigences du standard Secure SLC, les résultats étant documentés dans un rapport de conformité Secure SLC (ROC) et une attestation de conformité Secure SLC (AOC).
- Le logiciel a été développé et maintenu à l'aide des pratiques de gestion du cycle de vie des logiciels couvertes par l'évaluation du standard Secure SLC.
- Une évaluation Secure SLC complète des pratiques de gestion du cycle de vie des logiciels a été réalisée au cours des 36 derniers mois. De plus, si la dernière évaluation Secure SLC complète a eu lieu il y a plus de 12 mois, une attestation annuelle a été fournie par le développeur/fournisseur au cours des 12 mois précédents qui confirme le respect continu du standard Secure SLC pour les pratiques de gestion du cycle de vie des logiciels utilisées.

### **Validation de L'utilisation du Standard Secure SLC**

Lors de la validation de l'utilisation d'un logiciel développé et maintenu conformément à le standard Secure SLC pour répondre à l'exigence 6.2.4 du standard PCI DSS et prendre en charge une approche personnalisée pour les exigences 6.3 et 6.5, l'auditeur doit confirmer que les conditions suivantes sont remplies :

- L'évaluation du logiciel sécurisé a été effectuée par un auditeur de logiciels sécurisés et a confirmé qu'elle répondait à toutes les exigences du standard Secure SLC avec les résultats documentés dans un rapport de validation de logiciel sécurisé (ROV) et une attestation de validation de logiciel sécurisé (AOV).
- Le logiciel a été développé et est maintenu à l'aide des pratiques de gestion du cycle de vie des logiciels couvertes par l'évaluation des logiciels sécurisés.
- Une évaluation complète du logiciel sécurisé a été réalisée au cours des 36 derniers mois. De plus, si la dernière évaluation complète du logiciel sécurisé a eu lieu il y a plus de 12 mois, une attestation annuelle a été fournie par le développeur/fournisseur au cours des 12 mois précédents qui confirme le respect continu du standard des logiciels sécurisés.

## Annexe G Glossaire des Termes, Abréviations et Acronymes du Standard PCI DSS

Terme	Définition
<b>Accès à Distance</b>	Accès au réseau d'une entité à partir d'un emplacement en dehors de ce réseau. Un exemple de technologie d'accès à distance est un VPN.
<b>Accès D'administration</b>	Privilèges élevés ou accrus accordés à un compte pour que ce compte puisse gérer des systèmes, des réseaux et/ou des applications. L'accès administratif peut être attribué à un compte individuel ou à un compte système intégré. Les comptes disposant d'un accès administratif sont souvent appelés « superuser », « root », « administrateur », « admin », « administrateur système » ou « état du superviseur », selon le système d'exploitation et la structure organisationnelle.
<b>Accès Non Console</b>	Accès logique à un composant système qui se produit via une interface réseau plutôt que via une connexion physique directe au composant système. L'accès non console comprend l'accès à partir de réseaux locaux/internes ainsi que l'accès à partir de réseaux externes ou distants.
<b>Acquéreur</b>	Également appelée « banque du commerçant », « banque acquéreur » ou « établissement financier acquéreur ». Entité, généralement un établissement financier, qui traite les transactions par carte de paiement pour les commerçants et est définie par une marque de paiement comme un acquéreur. Les acquéreurs sont soumis aux règles et procédures de la marque de paiement concernant la conformité des commerçants. Voir Processeur de paiement.
<b>AES</b>	Acronyme de « Advanced Encryption Standard ». Voir Cryptographie robuste.
<b>Algorithme Cryptographique</b>	Également appelé « algorithme de chiffrement ». Processus mathématique réversible clairement spécifié utilisé pour transformer des données en texte clair en données chiffrées, et vice versa. Voir Cryptographie robuste.
<b>Algorithme de Chiffrement</b>	Voir Algorithme cryptographique.

Terme	Définition
<b>Analyse Ciblée de Risques</b>	Aux fins du standard PCI DSS, une analyse de risques qui se concentre sur une ou plusieurs exigences spécifiques d'intérêt du standard PCI DSS, soit parce que l'exigence permet une flexibilité (par exemple, quant à la fréquence) ou, pour l'approche personnalisée, pour expliquer comment l'entité a évalué le risque et déterminé que la mesure de sécurité personnalisée répond à l'objectif d'une exigence du standard PCI DSS.
<b>ANSI</b>	Acronyme de « American National Standards Institute. »
<b>Anti-Programmes Malveillants</b>	Logiciel conçu pour détecter, supprimer, bloquer ou contenir diverses formes de logiciels malveillants.
<b>AOC</b>	Acronyme de « Attestation de Conformité. » L'AOC est le formulaire officiel du PCI SSC permettant aux commerçants et aux prestataires de services d'attester des résultats d'une évaluation du standard PCI DSS, comme documenté dans un questionnaire d'auto-évaluation (SAQ) ou un rapport de conformité (ROC).
<b>Application</b>	Comprend tous les programmes logiciels ou groupes de programmes achetés, personnalisés et sur mesure, y compris les applications internes et externes (par exemple, les applications Web).
<b>Application Web</b>	Une application généralement accessible via un navigateur Web ou via des services Web. Les applications Web peuvent être disponibles via Internet ou un réseau interne privé.
<b>Approche Personnalisée</b>	Voir « Approches pour la mise en œuvre et la validation du standard PCI DSS » dans Exigences du standard PCI DSS et procédures d'évaluation de la sécurité.
<b>ASV</b>	Acronyme de « Fournisseur d'analyse approuvé ». Entreprise agréée par le PCI SSC pour mener des services externes de scan de vulnérabilités.
<b>Authentification</b>	Processus de vérification de l'identité d'une personne, d'un appareil ou d'un processus. L'authentification se produit généralement avec un ou plusieurs facteurs d'authentification. Voir Compte, Identifiants d'authentification, et Facteur d'authentification.

Terme	Définition
<b>Authentification à Plusieurs Facteurs</b>	Méthode d'authentification d'un utilisateur par laquelle au moins deux facteurs sont vérifiés. Ces facteurs comportent quelque chose que l'utilisateur possède (comme une carte à point ou un dongle), quelque chose que l'utilisateur connaît (comme un mot de passe, une phrase secrète ou un code PIN) ou quelque chose que l'utilisateur est ou fait (comme des empreintes digitales et d'autres éléments biométriques).
<b>Authentification résistant à l'hameçonnage</b>	Authentification conçue pour empêcher la divulgation et l'utilisation de secrets d'authentification à toute partie autre que le système légitime auprès duquel l'utilisateur tente de s'authentifier (par exemple, via des attaques par le procédé in-the-middle (ITM) ou par usurpation d'identité). Les systèmes résistants à l'hameçonnage mettent souvent en œuvre la cryptographie asymétrique comme mesure de sécurité principal. Les systèmes qui s'appuient uniquement sur des facteurs basés sur la connaissance ou limités dans le temps, tels que les mots de passe ou les mots de passe à usage unique (OTP), ne sont pas considérés comme résistants à l'hameçonnage, pas plus que les SMS ou les liens magiques. FIDO2 est un exemple d'authentification résistant au l'hameçonnage.
<b>Autorisation</b>	<p>Dans le contexte du contrôle d'accès, l'autorisation est l'octroi d'un accès ou d'autres droits à un utilisateur, un programme ou un processus. L'autorisation définit ce qu'une personne ou un programme peut faire après une authentification réussie.</p> <p>Dans le contexte d'une transaction par carte de paiement, l'autorisation fait référence au processus d'autorisation, qui se termine lorsqu'un commerçant reçoit une réponse de transaction (par exemple, une approbation ou un refus).</p>
<b>BAU</b>	Acronyme pour « Business as Usual. » (Activités courantes)
<b>Bloc PIN</b>	Bloc de données utilisé pour encapsuler un code PIN lors du traitement. Le format du bloc PIN définit le contenu du bloc PIN et la manière dont il est traité pour récupérer le PIN. Le bloc PIN est composé du PIN, de la longueur du PIN et peut contenir le PAN (ou une troncature de celui-ci) selon le format du bloc PIN ISO approuvé utilisé.
<b>Cadre de Sécurité</b>	Personne principale responsable de la sécurité d'une entité.
<b>Canal de Paiement</b>	Méthodes utilisées par les commerçants pour accepter les paiements des clients. Les canaux de paiement courants incluent la carte présente (en personne) et la carte non présente (commerce électronique et MO/TO).
<b>Cartes de Paiement</b>	Aux fins du standard PCI DSS, tout facteur de forme de carte de paiement portant le logo de toute marque de paiement participante du PCI SSC.

Terme	Définition
<b>CDE</b>	<p>Acronyme pour « Cardholder Data Environment. » (Environnement de données des titulaires de cartes) Le CDE se compose de :</p> <ul style="list-style-type: none"> <li>• Les composants système, aux personnes et aux processus qui stockent, traitent et transmettent les données de titulaires de cartes et/ou des données d'authentification sensibles, et</li> <li>• Les composants système qui ne doivent pas stocker, traiter ou transmettre des CHD/SAD mais qui ont une connectivité illimitée aux composants système qui stockent, traitent ou transmettent les CHD/SAD.</li> </ul>
<b>CERT</b>	Acronyme pour « Computer Emergency Response Team. » (Équipe de réponse d'urgence informatique)
<b>Chiffrement</b>	La transformation (réversible) des données par un algorithme cryptographique pour produire un texte chiffré, c'est-à-dire pour masquer le contenu informatif des données. Voir Cryptographie robuste.
<b>Chiffrement au Niveau des Fichiers</b>	Technique ou technologie (logicielle ou matérielle) permettant de chiffrer l'intégralité du contenu de fichiers spécifiques. Vous pouvez également consulter Chiffrement de disque et Chiffrement des bases de données au niveau des colonnes.
<b>Chiffrement de Bases de Données au Niveau Colonne</b>	Technique ou technologie (logicielle ou matérielle) pour chiffrer le contenu d'une colonne spécifique dans une base de données par rapport au contenu complet de la base de données entière. Vous pouvez également consulter Chiffrement du disque et Chiffrement au niveau des fichiers.
<b>Chiffrement de Disques</b>	Technique ou technologie (logicielle ou matérielle) permettant de chiffrer toutes les données stockées sur un appareil (par exemple, un disque dur ou une clé USB). Alternativement, le chiffrement au niveau des fichiers ou le chiffrement de la base de données au niveau de la colonne est utilisé pour chiffrer le contenu de fichiers ou de colonnes spécifiques.
<b>CIS</b>	Acronyme pour « Center for Internet Security »
<b>Classement des Risques</b>	Processus de classification des risques pour identifier, prioriser et traiter les éléments par ordre d'importance.

Terme	Définition
<b>Clé Cryptographique</b>	<p>Paramètre utilisé conjointement avec un algorithme cryptographique utilisé pour des opérations telles que :</p> <ul style="list-style-type: none"> <li>• Transformer des données en texte clair en données chiffrées,</li> <li>• Transformer des données chiffrées en données en texte clair,</li> <li>• Une signature numérique calculée à partir de données,</li> <li>• Vérifier une signature numérique calculée à partir de données,</li> <li>• Un code d'authentification calculé à partir de données, ou</li> <li>• Un accord d'échange d'un secret partagé.</li> </ul> <p><i>Voir Cryptographie robuste.</i></p>
<b>Codage Sécurisé</b>	<p>Processus de création et de mise en œuvre d'applications résistantes à l'altération et/ou à la compromission.</p>
<b>Code de Service</b>	<p>Valeur à trois ou quatre chiffres dans la piste magnétique qui suit la date d'expiration de la carte de paiement sur les données de piste. Il est utilisé pour diverses choses, telles que la définition des attributs de service, la différenciation entre les échanges internationaux et nationaux ou l'identification des restrictions d'utilisation.</p>
<b>Code de Vérification de la Carte</b>	<p>Également appelé cryptogramme visuel, code ou valeur de validation de la carte ou code de sécurité de la carte. Aux fins du standard PCI DSS, il s'agit de la valeur à trois ou quatre chiffres imprimés au recto ou au verso d'une carte de paiement. Peut être appelé CAV2, CVC2, CVN2, CVV2 ou CID selon les marques individuelles de paiement participantes. Pour plus d'informations, contactez les réseaux internationaux participantes.</p>
<b>Commerçant</b>	<p>Aux fins du standard PCI DSS, un commerçant est défini comme toute entité qui accepte les cartes de paiement portant les logos de toute marque de paiement participante du PCI SSC comme moyen de paiement pour des biens et/ou des services.</p> <p>Un commerçant qui accepte les cartes de paiement pour le paiement de biens et/ou de services peut également être un prestataire de services, si les services vendus entraînent le stockage, le traitement ou la transmission de données de titulaires de cartes pour le compte d'autres commerçants ou prestataires de services. Par exemple, un ISP est un commerçant qui accepte les cartes de paiement pour la facturation mensuelle, mais est également un fournisseur de services s'il héberge des commerçants en tant que clients.</p>
<b>Composants Système</b>	<p>Tous les périphériques réseau, serveurs, périphériques informatiques, composants virtuels ou logiciels inclus dans ou connectés au CDE, ou qui pourraient avoir une incidence sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles.</p>

Terme	Définition
<b>Compromission</b>	Également appelée « compromission des données » ou « violation des données ». Intrusion dans un système informatique où la divulgation/le vol, la modification ou la destruction non autorisée des données de titulaires de cartes est suspectée.
<b>Compte</b>	Également appelé « ID d'utilisateur », « ID de compte » ou « ID d'application ». Utilisé pour identifier une personne ou un processus sur un système informatique. Voir Identifiants d'authentification et Facteur d'authentification.
<b>Compte par Défaut</b>	Compte de connexion prédéfini dans un système, une application ou un appareil pour permettre l'accès initial lors de la première mise en service du système. Des comptes par défaut supplémentaires peuvent également être générés par le système dans le cadre du processus d'installation.
<b>Comptes Système et D'applications</b>	Également appelés « comptes de service ». Des comptes qui exécutent des processus ou effectuent des tâches sur un système informatique ou dans une application. Ces comptes ont généralement des priviléges élevés qui sont nécessaires pour effectuer des tâches ou des fonctions spécialisées et ne sont généralement pas des comptes utilisés par une personne.
<b>Connexion Interactive</b>	Processus par lequel une personne fournit des identifiants d'authentification pour se connecter directement à une application ou à un compte système. L'utilisation d'une connexion interactive signifie qu'il n'y a aucune responsabilité ou traçabilité des actions entreprises par cette personne.
<b>Connexion Réseau</b>	Voie de communication logique, physique ou virtuel entre des appareils qui permet la transmission et la réception de paquets de couche réseau.
<b>Console</b>	Écran et/ou clavier directement connectés qui permettent l'accès et le contrôle d'un serveur, d'un ordinateur central ou d'un autre type de système. Voir Accès non console.
<b>Consommateur</b>	Titulaire de carte individuel achetant des biens, des services ou les deux.
<b>Contrôle D'accès Logique</b>	Mécanismes qui limitent la disponibilité des informations ou des ressources de traitement de l'information uniquement aux personnes ou applications autorisées. Voir Contrôle d'accès physique.

Terme	Définition
<b>Contrôle D'accès Physique</b>	Mécanismes qui limitent l'accès à un espace physique ou à un environnement aux seules personnes autorisées. Voir Contrôle d'accès logique.
<b>Contrôle des Modifications</b>	Processus et procédures pour examiner, tester et approuver les modifications apportées aux systèmes et aux logiciels avant leur mise en œuvre.
<b>Correctif</b>	Mise à jour du logiciel existant pour ajouter une fonction ou pour corriger un défaut.
<b>Credentials</b>	Combinaison de l'ID utilisateur ou de l'ID de compte plus le ou les facteurs d'authentification utilisés pour authentifier une personne, un appareil ou un processus. Voir Compte et Facteur d'authentification.
<b>Criminalistique</b>	Appelé également « criminalistique informatique ». En ce qui concerne la sécurité des informations, l'application d'outils d'enquête et de techniques d'analyse pour recueillir des preuves à partir de ressources informatiques afin de déterminer la cause des compromissions des données. Les enquêtes sur la compromission des données de paiement sont généralement menées par un PCI Forensic Investigator (PFI).
<b>Cryptographie Robuste</b>	<p>La cryptographie est une méthode de protection des données via un processus de chiffrement réversible et est d'une primitive fondamentale utilisée dans de nombreux protocoles et services de sécurité. La cryptographie robuste est basée sur des algorithmes testés et acceptés par l'industrie, ainsi que sur des longueurs de clé qui fournissent un minimum de 112 bits de force de clé effective et des pratiques appropriées de gestion des clés. La force effective de la clé peut être plus courte que la longueur réelle en "bits" de la clé, ce qui peut conduire à des algorithmes avec des clés plus grandes offrant une protection moindre que des algorithmes avec des tailles de clé réelles plus petites, mais avec des tailles de clé effectives plus grandes. Il est recommandé que toutes les nouvelles mises en œuvre utilisent un minimum de 128 bits de force de clé effective. Ci-dessous des exemples de références de l'industrie sur les algorithmes cryptographiques et les longueurs de clé :</p> <ul style="list-style-type: none"> <li>• Publication spéciale 800-57 du NIST, Partie 1,</li> <li>• BSI TR-02102-1,</li> <li>• ECRYPT-CSA D5.4 Rapport sur les algorithmes, la taille des clés et les protocoles (2018), et</li> <li>• Algorithmes de chiffrement ISO/IEC 18033, et</li> <li>• ISO/IEC 14888-3:2-81 Techniques de sécurité informatique – Signatures numériques avec annexe – Partie 3 : Mécanismes basés sur le logarithme discret.</li> </ul>

Terme	Définition
<b>Cryptopériode</b>	La durée pendant laquelle une clé cryptographique peut être utilisée pour son but défini. Souvent définie en termes de période pendant laquelle la clé est active et/ou la quantité de texte chiffré qui a été produite par la clé, et selon les meilleures pratiques et directives de l'industrie (par exemple, NIST Special Publication 800-57).
<b>CVSS</b>	Acronyme de « Common Vulnerability Scoring System » (Système commun de notation des vulnérabilités). Se reporter au Guide du programme ASV pour plus d'informations.
<b>Diagramme de Flux de Données</b>	Un diagramme montrant comment et où les données circulent dans les applications, les système ou les réseau de l'entité, et vers/depuis les parties externes.
<b>Diagramme Réseau</b>	Un diagramme montrant les composants système et les connexions dans un environnement en réseau.
<b>DMZ</b>	Abréviation de « demilitarized zone » (Zone démilitarisée). Sous-réseau physique ou logique qui fournit une couche de sécurité supplémentaire au réseau privé interne d'une entreprise.
<b>DNS</b>	Acronyme pour « Domain Name System. »
<b>Données D'authentification Sensibles (SAD)</b>	Informations liées à la sécurité utilisées pour authentifier les titulaires de cartes et/ou autoriser les transactions par carte de paiement. Ces informations incluent, sans toutefois s'y limiter, les codes de vérification de la carte, les données de piste complètes (à partir d'une piste magnétique ou équivalente sur une puce), les codes PIN et les blocs PIN.
<b>Données de Carte</b>	Les données de carte consistent en des données de titulaires de cartes et/ou des données d'authentification sensibles. Voir Données de titulaires de cartes et Données d'authentification sensibles.
<b>Données de Piste</b>	Également appelées « données de piste complètes » ou « données de piste magnétique ». Données encodées dans la piste magnétique ou le point utilisées pour l'authentification et/ou l'autorisation lors des transactions de paiement. Il peut s'agir de l'image de la piste magnétique sur un point ou des données de piste sur la piste magnétique.
<b>Données de Piste Magnétique</b>	Voir Données de suivi.

Terme	Définition
<b>Données en Texte Clair</b>	Données non chiffrées.
<b>Données Relatives au Titulaire de Carte (CHD)</b>	<p>Au minimum, les données du titulaire de carte consistent en le PAN complet. Les données du titulaire de carte peuvent également apparaître sous la forme du PAN complet plus l'un des éléments suivants : nom du titulaire de la carte, date d'expiration et/ou code de service.</p> <p>Voir Données d'authentification sensibles pour les éléments de données supplémentaires qui peuvent être transmis ou traités (mais non stockés) dans le cadre d'une transaction de paiement.</p>
<b>Double Contrôle</b>	Processus consistant à utiliser deux ou plusieurs entités distinctes (généralement des personnes) agissant de concert pour protéger des fonctions ou des informations sensibles. Les deux entités sont également responsables de la protection physique du matériel impliqué dans les transactions vulnérables. Aucune personne n'est autorisée à accéder ou à utiliser le matériel (par exemple, la clé cryptographique). Pour la génération, le transport, le chargement, le stockage et la récupération manuels des clés, le double contrôle nécessite de répartir la connaissance de la clé entre les entités. Voir Fractionnement des connaissances.
<b>ECC</b>	Acronyme de « Elliptic Curve Cryptography » (cryptographie à courbe elliptique). Voir Cryptographie robuste.
<b>E-commerce (web) Serveur de Redirection</b>	Serveur qui redirige le navigateur d'un consommateur du site Web d'un marchand vers un emplacement différent pour le traitement des paiements lors d'une transaction de commerce électronique.
<b>Émetteur</b>	Également appelée « banque émetteur » ou « établissement financier émetteur ». Entité qui émet des cartes de paiement ou exécute, facilite ou prend en charge des services d'émission, y compris, sans toutefois s'y limiter, les banques émettrices et les processeurs émetteurs.
<b>Entité</b>	Dans le contexte de l'évaluation PCI DSS, un terme utilisé pour représenter la société, l'organisation ou l'entreprise qui fait l'objet d'une évaluation du standard PCI DSS.
<b>Évaluation des Risques</b>	Processus à l'échelle de l'entreprise qui identifie les ressources système précieuses et les menaces ; quantifie les expositions aux pertes (c'est-à-dire les pertes potentielles) en fonction des fréquences et des coûts d'occurrence estimés ; et (éventuellement) recommande la manière d'allouer des ressources aux contre-mesures pour minimiser l'exposition totale. Voir Analyse de risques ciblée.

Terme	Définition
<b>Événement de Sécurité</b>	<p>Événement considéré par une entreprise comme ayant des implications potentielles sur la sécurité d'un système ou de son environnement. Dans le contexte du standard PCI DSS, les événements de sécurité identifient des activités suspectes ou anormales.</p>
<b>Exception Légale</b>	<p>Une restriction légale due à une loi, une réglementation ou une exigence réglementaire locale ou régionale, dans laquelle le respect d'une exigence PCI DSS violerait cette loi, cette réglementation ou cette exigence réglementaire. Les obligations contractuelles ou les conseils juridiques ne constituent pas des restrictions légales.</p> <p>Consulter les documents PCI DSS v4.x suivants pour plus d'informations sur la déclaration des exceptions légales :</p> <ul style="list-style-type: none"> <li>• Le modèle de rapport de conformité (ROC) et les attestations de conformité associées.</li> <li>• Les questionnaires d'auto-évaluation (SAQ) et les attestations de conformité associées.</li> </ul> <p>Remarque : Lorsqu'une entité opère sur plusieurs sites, une exception légale ne peut être invoquée que pour les sites régis par la loi, la réglementation ou l'exigence réglementaire, et ne peut pas être invoquée pour les sites dans lesquels cette loi, cette réglementation ou cette exigence réglementaire est inapplicable.</p>
<b>Facteur D'authentification</b>	<p>L'élément utilisé pour prouver ou vérifier l'identité d'une personne ou d'un processus sur un système informatique. L'authentification se produit généralement avec le ou les facteurs d'authentification suivant :</p> <ul style="list-style-type: none"> <li>• Quelque chose que vous connaissez, comme un mot de passe ou une phrase de secrète</li> <li>• Un objet que vous possédez, tel qu'un dispositif à jeton ou une carte à puce</li> <li>• Quelque chose que vous êtes, comme un élément biométrique.</li> </ul> <p>L'ID (ou le compte) et le facteur d'authentification sont considérés ensemble comme des identifiants d'authentification. Voir Compte et Identifiant d'authentification.</p>
<b>Facteur de Forme des Cartes de Paiement</b>	<p>Comprend les cartes de paiement physiques ainsi que les appareils dotés d'une fonctionnalité qui émule une carte de paiement pour initier une transaction de paiement. Des exemples de tels appareils comportent, sans toutefois s'y limiter, les smartphones, les montres intelligentes, les bracelets de fitness, les porte-clés et les objets portables tels que les bijoux.</p>
<b>FTP</b>	<p>Acronyme pour « File Transfer Protocol. » Protocole réseau utilisé pour transférer des données d'un ordinateur à un autre via un réseau public tel qu'Internet. Le protocole FTP est largement considéré comme un protocole non sécurisé car les mots de passe et le contenu des fichiers sont envoyés sans protection et en texte clair. Le protocole FTP peut être mis en œuvre en toute sécurité via SSH ou une autre technologie.</p>

Terme	Définition
<b>Génération de Clé Cryptographique</b>	<p>La génération de clés est l'une des fonctions de la gestion des clés. Les documents suivants fournissent des conseils reconnus sur la génération appropriée de clés :</p> <ul style="list-style-type: none"> <li>Publication spéciale 800-133 du NIST : Recommandation pour la génération de clés cryptographiques</li> <li>ISO 11568-2 Service financiers — Gestion des clés (détail) — Partie 2 : Les chiffrements symétriques, leur gestion des clés et leur cycle de vie <ul style="list-style-type: none"> <li>4.3 Génération des clés</li> </ul> </li> <li>ISO 11568-4 Service financiers — Gestion des clés (détail) — Partie 4 : Cryptosystèmes asymétriques — Gestion des clés et du cycle de vie <ul style="list-style-type: none"> <li>6.2 Principales étapes du cycle de vie — Génération</li> </ul> </li> <li>Conseil Européen des Paiements EPC 342-08 Directives sur l'utilisation des algorithmes et la gestion des clés <ul style="list-style-type: none"> <li>4.1.1 Génération des clés [pour les algorithmes symétriques]</li> <li>4.2.1 Génération des clés [pour les algorithmes asymétriques]</li> </ul> </li> </ul>
<b>Gestion des Clés Cryptographiques</b>	<p>L'ensemble des processus et des mécanismes qui prennent en charge l'établissement et la maintenance des clés cryptographiques, y compris le remplacement des anciennes clés par de nouvelles clés si nécessaire.</p>
<b>Hachage</b>	<p>Méthode de protection des données qui convertit les données en un résumé de message de longueur fixe. Le hachage est une fonction unidirectionnelle (mathématique) dans laquelle un algorithme non secret prend en entrée n'importe quel message de longueur arbitraire et produit une sortie de longueur fixe (généralement appelée « code de hachage » ou « résumé de message »). Les fonctions de hachage doivent avoir les propriétés suivantes :</p> <ul style="list-style-type: none"> <li>Il est informatiquement impossible de déterminer l'entrée d'origine avec uniquement le code de hachage,</li> <li>Il est informatiquement impossible de trouver deux entrées qui donnent le même code de hachage.</li> </ul>
<b>Hachage Cryptographique à Clé</b>	<p>Une fonction de hachage qui incorpore une clé secrète générée de manière aléatoire pour offrir une résistance aux attaques par force brute et une intégrité d'authentification secrète.</p> <p>Les algorithmes de hachage cryptographique (ou de scellement) à clé appropriés incluent, sans toutefois s'y limiter : HMAC, CMAC et GMAC, avec une force cryptographique effective d'au moins 128 bits (NIST SP 800-131Ar2). Se reporter à ce qui suit pour plus d'informations sur HMAC, CMAC et GMAC, respectivement : NIST SP 800-107r1, NIST SP 800-38B, et NIST SP 800-38D).</p> <p>Voir NIST SP 800-107 (Révision 1) : Recommandation pour les applications utilisant des algorithmes de hachage approuvés §5.3.</p>

Terme	Définition
<b>HSM</b>	Acronyme de « module de sécurité matériel » ou « module de sécurité hôte ». Dispositif matériel physiquement et logiquement protégé qui fournit un ensemble sécurisé de services cryptographiques, utilisé pour les fonctions de gestion des clés cryptographiques et/ou le déchiffrement des données de carte.
<b>IDS</b>	Acronyme de « intrusion-detection system » (système de détection d'intrusions).
<b>Indépendance Organisationnelle</b>	Une structure organisationnelle qui garantit qu'il n'y a pas de conflit d'intérêts entre la personne ou le service exécutant l'activité et la personne ou le service évaluant l'activité. Par exemple, les personnes qui effectuent des évaluations sont organisationnellement distinctes de la gestion de l'environnement évalué.
<b>IPS</b>	Acronyme de « intrusion prevention system » (système de prévention des intrusions).
<b>ISO</b>	Acronyme pour « International Organization for Standardization. »
<b>Journal</b>	Voir Journal d'audit.
<b>Journal D'audit</b>	Également appelé « suivi d'audit ». Enregistrement chronologique des activités du système. Fournit une piste vérifiable de manière indépendante, suffisante pour permettre la reconstruction, la révision et l'examen de la séquence des environnements et des activités entourant ou menant à une opération, une procédure ou un événement dans une transaction, du début jusqu'aux résultats finaux.
<b>L'approche Définie</b>	Voir « Section PCI DSS : 8 approches pour la mise en œuvre et la validation du standard PCI DSS » dans Exigences et procédures d'évaluation de la sécurité du PCI DSS.
<b>LAN</b>	Acronyme de « local area network » (réseau local)
<b>LDAP</b>	Acronyme de « Lightweight Directory Access Protocol ».
<b>Logiciel Tiers</b>	Logiciel acheté par une entité, mais non développé expressément pour elle. Il peut être open source, freeware, shareware ou acheté.

Terme	Définition
<b>Logiciels Sur Mesure et Personnalisés</b>	Un logiciel sur mesure est développé pour l'entité par un tiers au nom de l'entité et selon les spécifications de l'entité. Le logiciel personnalisé est développé par l'entité pour son propre usage.
<b>MAC</b>	En cryptographie, acronyme de « code d'authentification de message ». Voir Cryptographie robuste.
<b>Marque de Paiement</b>	Une entreprise avec des cartes de paiement de marque ou d'autres facteurs de forme de carte de paiement. Les réseaux internationaux réglementent où et comment les cartes de paiement ou autres facteurs de forme portant leur marque ou leur logo sont utilisés. Une marque de paiement peut être une marque de paiement participante du PCI SSC ou une autre marque, système ou réseau de paiement mondial ou régional.
<b>Marque de Paiement Participante</b>	Également appelée « marque de paiement ». Une marque de carte de paiement qui, à l'époque en question, est alors officiellement admise en tant que membre (ou affiliée à) du PCI SSC conformément à ses documents constitutifs. Au moment de la rédaction du présent document, les réseaux internationaux participantes incluent les membres fondateurs et les membres stratégiques du PCI SSC.
<b>Masquage</b>	Méthode de dissimulation d'un segment du PAN lorsqu'il est affiché ou imprimé. Le masquage est utilisé lorsqu'il n'est pas nécessaire pour l'entreprise de visualiser l'intégralité du PAN. Le masquage concerne la protection du PAN lorsqu'il est affiché sur les écrans, les reçus papier, les impressions, etc. Voir Troncature pour la protection du PAN lorsqu'il est stocké, traité ou transmis électroniquement.
<b>Mesures de Sécurité Compensatoires</b>	Voir les annexes B et C du standard PCI DSS dans les exigences et les procédures d'évaluation de la sécurité du PCI DSS.
<b>Mesures de Sécurité Réseau (NSC)</b>	Pare-feu et autres technologies de sécurité réseau qui agissent comme des points d'application de la politique réseau. Les NSC contrôlent généralement le trafic réseau entre deux ou plusieurs segments de réseau logiques ou physiques (ou sous-réseaux) en fonction de politiques ou de règles prédéfinies.
<b>MO/TO</b>	Acronyme de « Mail-Order/Telephone-Order ».
<b>Moindres Priviléges</b>	Le niveau minimum de priviléges nécessaires pour assumer les rôles et responsabilités de la fonction.

Terme	Définition
<b>Mot de Passe / Phrase Secrète</b>	Chaîne de caractères servant de facteur d'authentification pour un utilisateur ou un compte.
<b>Mot de Passe par Défaut</b>	Mot de passe sur l'administration système, les comptes d'utilisateurs ou de services prédéfinis dans un système, une application ou un appareil ; généralement associé au compte par défaut. Les comptes et mots de passe par défaut sont publiés et bien connus, et donc facilement devinés.
<b>NAC</b>	Acronyme de « Network Access Control » (Contrôle d'accès au réseau).
<b>NAT</b>	Acronyme de « Network Address Translation » (Traduction d'adresses réseau).
<b>NIST</b>	Acronyme de « National Institute of Standards and Technology. » Agence fédérale non réglementaire au sein de la Technology Administration du département américain du Commerce.
<b>NTP</b>	Acronyme de « Network Time Protocol ».
<b>Objet de Niveau Système</b>	Tout élément d'un composant système nécessaire à son fonctionnement, y compris, sans toutefois s'y limiter, les exécutables d'applications et les fichiers de configuration, les fichiers de configuration système, les bibliothèques et DLL statiques et partagées, les exécutables système, les pilotes de périphérique et les fichiers de configuration de périphérique, et les composants tiers.
<b>Opérateur des Clés</b>	Rôle dans lequel une ou plusieurs personnes se voient confier et sont responsables de l'exécution de tâches de gestion de clés impliquant des clés secrètes et/ou privées, des partages de clés ou des composants clés pour le compte d'une entité.
<b>OWASP</b>	Acronyme de « Open Web Application Security Project »

Terme	Définition
<b>Page de Paiement</b>	<p>Interface utilisateur Web contenant un ou plusieurs éléments de formulaire destinés à capturer les données de carte d'un consommateur ou à soumettre les données de carte capturées à des fins de traitement et d'autorisation des transactions de paiement. La page de paiement peut être rendue comme l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Un document ou une instance unique,</li> <li>• Un document ou un composant affiché dans un cadre inséré dans une page de non-paiement,</li> <li>• Plusieurs documents ou composants contenant chacun un ou plusieurs éléments de formulaire contenus dans plusieurs cadres en ligne au sein d'une page de non-paiement.</li> </ul>
<b>PAN</b>	<p>Acronyme de « Numéro de compte primaire. » Numéro de carte de paiement unique (cartes de crédit, de débit ou prépayées, etc.) qui identifie l'émetteur et le compte du titulaire de la carte.</p>
<b>Pare-feu</b>	<p>Technologie matérielle et/ou logicielle qui protège les ressources du réseau contre tout accès non autorisé. Un pare-feu autorise ou refuse le trafic informatique entre des réseaux avec différents niveaux de sécurité en fonction d'un ensemble de règles et d'autres critères.</p>
<b>PCI DSS</b>	<p>Acronyme de « Payment Card Industry Data Security Standard » (Standard de sécurité des données de l'industrie des cartes de paiement).</p>
<b>Personnel</b>	<p>Employés à temps plein et à temps partiel, employés temporaires, sous-traitants et consultants ayant des responsabilités de sécurité pour la protection des données de carte ou pouvant avoir un impact sur la sécurité des données de titulaires de carte et/ou des données d'authentification sensibles.</p>
<b>PIN</b>	<p>Acronyme de « personal identification number » (numéro d'identification personnel).</p>
<b>POI</b>	<p>Acronyme de "Point of Interaction" (Point d'interaction), le point initial où les données sont lues à partir d'une carte.</p>
<b>Portée</b>	<p>Processus d'identification de tous les composants, personnes et processus du système à inclure dans une évaluation du standard PCI DSS. Voir la section 4 du PCI DSS : Portée des exigences du standard PCI DSS.</p>

Terme	Définition
<b>Prestataire de Services</b>	<p>Entité commerciale qui n'est pas une marque de paiement, directement impliquée dans le traitement, le stockage ou la transmission de données de titulaires de cartes (CHD) et/ou des données d'authentification sensibles pour le compte d'une autre entité. Cela inclut les passerelles de paiement, les prestataires de services de paiement (PSP) et les entreprises de vente indépendantes (ISO). Cela inclut également les entreprises qui fournissent des services qui contrôlent ou pourraient avoir un impact sur la sécurité des CHD et/ou des SAD. Les exemples incluent les prestataires de services gérés qui fournissent des pare-feu gérés, des IDS et d'autres services, ainsi que des fournisseurs d'hébergement et d'autres entités.</p> <p>Si une entité fournit un service qui implique uniquement la fourniture d'un accès au réseau public, telle une entreprise de télécommunications fournissant uniquement la liaison de communication, l'entité ne serait pas considérée comme un prestataire de services pour ce service (bien qu'elle puisse être considérée comme un prestataire de services pour d'autres services). <i>Consulter les rubriques Prestataire de services mutualisés et Prestataire de services tiers.</i></p>
<b>Prestataire de Services Mutualisés</b>	<p>Un type de fournisseur de services tiers qui offre divers services partagés aux commerçants et autres fournisseurs de services, où les clients partagent les ressources système (telles que les serveurs physiques ou virtuels), l'infrastructure, les applications (y compris le logiciel en tant que service (SaaS)), et/ou des bases de données, l'accès à ces ressources ou services étant logiquement contrôlé ou partitionné pour maintenir les ressources contenues et les données isolées entre les clients. Les services peuvent inclure, sans toutefois s'y limiter, l'hébergement de plusieurs entités sur un seul serveur partagé, la fourniture de services de commerce électronique et/ou de "panier d'achat", des services d'hébergement Web, des applications de paiement, diverses applications et services cloud, et des connexions à des passerelles de paiement et des processeurs. Voir Prestataire de services et Prestataire de services tiers.</p>
<b>Prestataire de Services Tiers (TPSP)</b>	<p>Tout tiers agissant en tant que prestataire de services pour le compte d'une entité. Consulter la rubrique Prestataire de services mutualisés et Prestataire de services.</p>
<b>Processeur de Paiement</b>	<p>Parfois appelée « passerelle de paiement » ou « Prestataire de services de paiement (PSP) ». Entité engagée par un commerçant ou une autre entité pour gérer les transactions par carte de paiement en son nom. Voir Acquéreurs.</p>
<b>Produit Vendu sur Étagère (COTS)</b>	<p>Description des produits qui sont des articles en stock disponibles dans le commerce et non spécifiquement personnalisés ou conçus pour un consommateur ou un utilisateur spécifique et qui sont facilement disponibles pour utilisation.</p>

Terme	Définition
<b>QIR</b>	Acronyme de « Qualified Integrator or Reseller » (Intégrateur ou revendeur qualifié). Se reporter au Guide du programme QIR sur le site Web du PCI SSC pour plus d'informations.
<b>QSA</b>	Acronyme de « Qualified Security Assessor » (auditeur de sécurité qualifié). Les entreprises QSA sont qualifiées par le PCI SSC pour valider le respect par les entités des exigences PCI DSS des évaluations sur place du standard PCI DSS. Se reporter aux exigences de qualification des QSA pour plus de détails sur les exigences pour les entreprises et employés QSA.
<b>Réseau de Confiance</b>	Réseau d'une entité qui est dans la capacité de contrôle ou de gestion de l'entité et qui répond aux exigences applicables du standard PCI DSS.
<b>Réseau sans Relation de Confiance</b>	Tout réseau qui ne répond pas à la définition d'un « réseau de confiance ».
<b>ROC</b>	Acronyme de « Report on Compliance » (Rapport sur la conformité). Outil de reporting utilisé pour documenter les résultats détaillés de l'évaluation du standard PCI DSS d'une entité.
<b>RSA</b>	Algorithme de chiffrement à clé publique. Voir Cryptographie robuste.
<b>SAD</b>	Acronyme de « Sensitive Authentication Data » (Données d'authentification sensibles).
<b>SAQ</b>	Acronyme de « Self-Assessment Questionnaire » (Questionnaire d'auto-évaluation). Outil de reporting utilisé pour documenter les résultats de l'auto-évaluation du standard PCI DSS d'une entité.
<b>Scripts de Page de Paiement</b>	Toutes commandes ou instructions de langage de programmation sur une page de paiement qui sont traitées et/ou interprétées par le navigateur d'un consommateur, y compris les commandes ou instructions qui interagissent avec le modèle d'objet de document d'une page. Des exemples de langages de programmation sont JavaScript et VB script ; ni les langages de balisage (par exemple, HTML) ni les règles de style (par exemple, CSS) ne sont des langages de programmation.

Terme	Définition
<b>Segmentation</b>	Également appelée « segmentation du réseau » ou « isolation ». La segmentation isole les composants système qui stockent, traitent ou transmettent les données des titulaires de cartes des systèmes qui ne le font pas. Voir « Segmentation » dans la section 4 : Portée des exigences du standard PCI DSS.
<b>Séparation des Connaissances</b>	Une méthode par laquelle deux ou plusieurs entités ont séparément des composants de clés ou des partages de clés qui ne transmettent individuellement aucune connaissance de la clé cryptographique résultante.
<b>Séparation des Tâches</b>	Pratique consistant à diviser les étapes d'une fonction entre plusieurs individus, pour empêcher un seul individu de subvertir le processus.
<b>Services D'émission</b>	Les exemples de services d'émission comportent, sans toutefois s'y limiter, l'autorisation et la personnalisation de la carte.
<b>Skimmer de Cartes</b>	Un appareil physique, souvent relié à un lecteur de carte légitime, conçu pour capturer et/ou stocker de manière illégitime les informations d'une carte de paiement.
<b>SNMP</b>	Acronyme de « Simple Network Management Protocol » (Protocole simplifié de gestion de réseau).
<b>SQL</b>	Acronyme de « Structured Query Language ».
<b>SSH</b>	Abréviation de « Secure Shell ».
<b>SSL</b>	Acronyme de « Secure Sockets Layer ».
<b>Supports</b>	Matériel physique, y compris, sans toutefois s'y limiter, les dispositifs de stockage électroniques, les supports électroniques amovibles et les rapports papier.
<b>Supports Électroniques Amovibles</b>	Supports qui stockent des données numérisées qui peuvent être facilement supprimées et/ou transportées d'un système informatique à un autre. Des exemples de supports électroniques amovibles comprennent les CD-ROM, les DVD-ROM, les clés USB et les disques durs externes/portables. Dans ce contexte, les supports électroniques amovibles n'incluent pas les lecteurs remplaçables à chaud, les lecteurs de bande utilisés pour les sauvegardes en bloc ou d'autres supports qui ne sont généralement pas utilisés pour transporter des données d'un emplacement à un autre.

Terme	Définition
<b>Surveillance de L'intégrité des Fichiers (FIM)</b>	Une solution de détection des changements qui vérifie les modifications, les ajouts et les suppressions de fichiers critiques et avertit lorsque de telles modifications sont détectées.
<b>Système de Gestion des Clés</b>	Une combinaison de matériel et de logiciels qui fournit une approche intégrée pour générer, distribuer et/ou gérer des clés cryptographiques pour les appareils et les applications.
<b>Système de Point de Vente (POS)</b>	Matériel et logiciels utilisés par les commerçants pour accepter les paiements des clients. Peut inclure des dispositifs POI, des claviers NIP, des caisses enregistreuses électroniques, etc.
<b>Systèmes Critiques</b>	Un système ou une technologie que l'entité juge d'une importance particulière. Par exemple, un système critique peut être essentiel à l'exécution d'une opération commerciale ou au maintien d'une fonction de sécurité. Les exemples de systèmes critiques comportent souvent les systèmes de sécurité, les appareils et systèmes destinés au public, les bases de données et les systèmes qui stockent, traitent ou transmettent les données des titulaires de cartes.
<b>TDES</b>	Acronyme de « Triple Data Encryption Standard » (Standard de chiffrement triple des données). Aussi appelée « 3DES » ou « Triple DES ».
<b>Telnet</b>	Abréviation de « telephone network protocol » (protocole de réseau téléphonique).
<b>Terminal de Paiement Virtuel</b>	Dans le cadre du questionnaire d'auto-évaluation (SAQ) C-VT, un terminal de paiement virtuel est un accès basé sur un navigateur Web au site Web d'un acquéreur, d'un processeur ou d'un prestataire de services tiers pour autoriser les transactions par carte de paiement, où le commerçant saisit manuellement les données de la carte de paiement via un navigateur Web. Contrairement aux terminaux physiques, les terminaux de paiement virtuels ne lisent pas directement les données d'une carte de paiement. Étant donné que les transactions par carte de paiement sont saisies manuellement, les terminaux de paiement virtuels sont généralement utilisés à la place des terminaux physiques dans les environnements marchands avec de faibles volumes de transactions.
<b>Titulaire de Carte</b>	Client auquel une carte de paiement est émise ou toute personne autorisée à utiliser la carte de paiement. <i>Voir le visiteur.</i>
<b>TLS</b>	Acronyme de « Transport Layer Security » (Sécurité de la couche de transport).

Terme	Définition
<b>Token (Jeton)</b>	Dans le contexte de l'authentification et du contrôle d'accès, un jeton est une valeur fournie par un matériel ou un logiciel qui fonctionne avec un serveur d'authentification ou un VPN pour effectuer une authentification dynamique ou à plusieurs facteurs.
<b>Token D'index</b>	Une valeur aléatoire d'un tableau de valeurs aléatoires qui correspond à un PAN donné.
<b>Troncature</b>	Méthode pour rendre un PAN complet illisible en supprimant un segment des données du PAN. La troncature concerne la protection du PAN lorsqu'il est stocké, traité ou transmis électroniquement. Voir <i>Masquage</i> pour la protection du PAN lorsqu'il est affiché sur les écrans, les reçus papier, etc.
<b>Utilisateur Privilégié</b>	Tout compte utilisateur avec des priviléges d'accès plus élevés que les priviléges d'accès de base. Généralement, ces comptes ont des priviléges élevés ou accrus avec plus de droits qu'un compte d'utilisateur standard. Cependant, l'étendue des priviléges sur différents comptes privilégiés peut varier considérablement en fonction de l'entreprise, de la fonction ou du rôle et de la technologie utilisée.
<b>Virtualisation</b>	L'abstraction logique des ressources informatiques des contraintes physiques et/ou logiques. Une abstraction courante est appelée machines virtuelles ou VM, qui prend le contenu d'une machine physique et lui permet de fonctionner sur un matériel physique différent et/ou avec d'autres machines virtuelles sur le même matériel physique. D'autres abstractions courantes comprennent, sans toutefois s'y limiter, les conteneurs, l'informatique sans serveur ou les microservices.
<b>Visiteur</b>	Un fournisseur, un invité de tout membre du personnel, un employé de service ou un membre du personnel qui n'a normalement pas accès à la zone concernée. Les titulaires de carte présents dans un point de vente au détail pour acheter des biens ou des services ne sont pas considérés comme des « visiteurs ». Voir <i>Titulaire de carte et Personnel</i> .
<b>VPN</b>	Acronyme de « virtual private network » (réseau privé virtuel).
<b>Vulnérabilité</b>	Défaut ou faiblesse qui, s'ils sont exploités, peuvent entraîner une compromission intentionnelle ou non d'un système.

Terme	Définition
<b>Zone Sensible</b>	<p>Une zone sensible est généralement un sous-ensemble du CDE et correspond à toute zone qui abrite des systèmes considérés comme critiques pour le CDE. Cela inclut les centres de données, les salles de serveurs, les salles de back-office dans les points de vente et toute zone qui concentre ou agrège le stockage, le traitement ou la transmission des données des titulaires de cartes. Les zones sensibles comprennent également les zones hébergeant des systèmes qui gèrent ou maintiennent la sécurité du CDE (par exemple, ceux qui fournissent des mesures de sécurité de sécurité du réseau ou qui gèrent la sécurité physique ou logique).</p> <p>Cela exclut les zones où seuls les terminaux de point de vente sont présents, tels que les zones de caisse dans un magasin de détail ou les centres d'appels où les agents acceptent les paiements.</p>