Payment Card Industry

Standard de Sécurité des Données

Synthèse des Modifications du Standard PCI DSS Version 3.2.1 à 4.0

Révision 1

Mai 2022

Modifications Apportées au Document

Date	Révision	Description
Mars 2022		Synthèse des modifications apportées à la version initiale du standard PCI DSS v3.2.1 à v4.0.
Mai 2022	1	Mise à jour des errata pour corriger la description des modifications de l'exigence 8.3.9 du PCI DSS v4.0.

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

Ce document fournit un résumé de haut niveau et une description des modifications du standard *PCI DSS v3.2.1* au standard *PCI DSS v4.0* et ne détaille pas toutes les révisions du document. En raison de l'ampleur des modifications, le standard devrait être revu dans son intégralité plutôt que de se concentrer uniquement sur ce document de synthèse.

Ce résumé des modifications est organisé comme suit :

- *Types de modifications* - fournit un aperçu des types de modifications.
- *Résumé des modifications apportées aux sections d'introduction du standard PCI DSS* - résume les modifications apportées à chaque section concernée.
- *Résumé des modifications générales apportées aux exigences du standard PCI DSS* - résume les modifications apportées aux exigences, aux procédures de test et à l'orientation.
- *Modifications supplémentaires par exigence* - résume les modifications supplémentaires apportées aux exigences 1 à 12 et aux annexes.
- *Résumé des nouvelles exigences* - répertorie toutes les nouvelles exigences, l'entité à laquelle la nouvelle exigence s'applique (c'est-à-dire toutes les entités ou prestataires de services uniquement) et la date d'entrée en vigueur de la nouvelle exigence.

2 Types de Modification

Type de Modification	Définition
Evolution de l'exigence	Modifications pour s'assurer que le standard est à jour avec les menaces et les technologies émergentes, et les changements touchant l'industrie du paiement. Des exemples incluent des exigences ou des procédures de test nouvelles ou modifiées, ou la suppression d'une exigence.
Clarification ou orientation	Mises à jour de la formulation, des explications, des définitions, des conseils supplémentaires et/ou des instructions afin d'améliorer la compréhension ou fournir des informations ou des conseils supplémentaires sur un sujet particulier.
Structure ou format	Réorganisation du contenu, y compris la combinaison, la séparation et la renumérotation des exigences pour aligner le contenu.

3 Résumé des Modifications Apportées aux Sections D'introduction du Standard PCI DSS

Section		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Introduction et présentation de du standard de sécurité des données PCI	Introduction et présentation du standard de sécurité des données PCI	Ajout du sous-titre « Limitations » et clarification du fait que le standard PCI DSS ne remplace pas les lois nationales, étatiques ou locales. Développement de la liste des ressources du standard PCI DSS.	Clarification ou orientation
Informations sur les conditions d'applicabilité du standard PCI DSS	Informations sur les conditions d'applicabilité du standard PCI DSS	Ajout de sous-titres pour améliorer la lisibilité. Clarification du fait que certaines exigences du standard PCI DSS peuvent s'appliquer aux entités qui ne stockent, ne traitent ou ne transmettent pas de numéro de compte primaire (PAN). Clarification du fait que les termes données de compte, données d'authentification sensibles (SAD), données de titulaire de carte et PAN ne sont pas interchangeables et sont utilisés intentionnellement dans le standard PCI DSS. Clarification du tableau contenant les éléments couramment utilisés des données de titulaires de cartes et des SAD, si le stockage est autorisé et si les données doivent être rendues illisibles.	Clarification ou orientation
Relation entre le standard PCI DSS et le standard PA-DSS	Relation entre le standard PCI DSS et les standards logiciels du PCI SSC	Recentrage de la section sur la relation entre le standard PCI DSS et les standards logiciels du PCI SSC, avec mention du standard PA-DSS (qui ne sera plus effective à partir d'octobre 2022).	Evolution de l'exigence
Portée des exigences du standard PCI DSS	Portée des exigences du standard PCI DSS	Clarification de l'applicabilité des exigences du standard PCI DSS et définition de l'environnement des données de titulaires de cartes (CDE). Ajout des exemples de composants système auxquels le standard PCI DSS s'applique ; ajout du cloud et d'autres composants système. Ajout du diagramme « Comprendre la portée du standard PCI DSS ».	Clarification ou orientation
Portée des exigences du standard PCI DSS	Portée des exigences du standard PCI DSS : Confirmation annuelle de la portée du standard PCI DSS	Ajout de sous-titres et clarification du contenu existant.	Clarification ou orientation
Annexe D : Segmentation et échantillonnage des installations commerciales/composants système	Portée des exigences du standard PCI DSS : Segmentation	Déplacement du diagramme de segmentation précédemment dans l'annexe D, avec de légères modifications. Changement de titre de la sous-section mise à jour des références de « segmentation du réseau » à « segmentation » pour prendre en charge une gamme plus large de contrôles de segmentation.	Clarification ou orientation

Section		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Portée des exigences du standard PCI DSS : Technologie sans fil	Portée des exigences du standard PCI DSS : Technologie sans fil	Clarification du fait que la détection sans fil non autorisé (Exigence 11.2.1) doit être effectuée même si le réseau sans fil n'est pas utilisé dans le CDE et même si l'entité dispose d'une politique qui interdit son utilisation.	Clarification ou orientation
	Portée des exigences du standard PCI DSS : Données chiffrées des titulaires de carte et impact sur la portée du standard PCI DSS	Ajout d'une sous-section et contenu connexe.	Clarification ou orientation
	Portée des exigences du standard PCI DSS : Données chiffrées des titulaires de cartes et impact sur la portée du standard PCI DSS pour les prestataires de services tiers	Ajout d'une nouvelle sous-section et contenu connexe.	Clarification ou orientation
Portée des exigences du standard PCI DSS : Utilisation de prestataires de services tiers/Sous-traitance	Portée des exigences du standard PCI DSS : Utilisation de prestataires de services tiers	Changement de titre de sous-section, ajout de nouveau contenu et réorganisation du contenu existant sous de nouveaux sous-titres.	Clarification ou orientation
Meilleures pratiques pour la mise en œuvre du standard PCI DSS dans les processus des affaires courantes (Business-as-Usual ou « BAU »)	Meilleures pratiques pour la mise en œuvre du standard PCI DSS dans les processus des affaires courantes (Business-as-Usual ou « BAU »)	Ajout de conseils et de clarifications partout dans le document.	Clarification ou orientation
Pour les évaluateurs : Échantillonnage des installations commerciales/composants système	Pour les évaluateurs : Échantillonnage pour les évaluations du standard PCI DSS	Changement de titre de la section et mise à jour complète avec des conseils et des clarifications supplémentaires. Clarification du fait que les références d'échantillonnage ont été supprimées des procédures de test afin d'aider les évaluateurs à sélectionner des échantillons appropriés à la population testée.	Clarification ou orientation

Section		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Annexe D : Segmentation et échantillonnage des installations commerciales/composants système	Pour les évaluateurs : Échantillonnage pour les évaluations du standard PCI DSS	Déplacement du diagramme d'échantillonnage précédemment dans l'annexe D, avec de légères modifications.	Clarification ou orientation
	Description des délais utilisés dans les exigences PCI DSS	Nouvelle section pour clarifier les fréquences et les délais spécifiés dans le standard PCI DSS et les attentes associées. Ajout d'une explication de « changement significatif ».	Clarification ou orientation
	Approches pour la mise en œuvre et la validation du standard PCI DSS	Nouvelle section pour expliquer et illustrer les deux approches, définies et personnalisées, pour la mise en œuvre et la validation du standard PCI DSS.	Evolution de l'exigence
Contrôles compensatoires	Approches pour la mise en œuvre et la validation du standard PCI DSS	Déplacement du contenu vers cette section, à un sous-titre sous « Approche définie ».	Structure ou format
	Protéger les informations relatives à l'état de sécurité de l'entité	Nouvelle section pour décrire comment les entités peuvent gérer les artefacts sensibles de leur évaluation du standard PCI DSS.	Clarification ou orientation
	Méthodes de test pour les exigences du standard PCI DSS	Nouvelle section pour décrire les méthodes de test utilisées dans chaque procédure de test du standard PCI DSS et les activités correspondantes attendues d'être effectuées par l'évaluateur.	Clarification ou orientation
Processus d'évaluation du standard PCI DSS	Processus d'évaluation du standard PCI DSS	Comprend des clarifications mineures. Déplacement de la note commençant par « Les exigences du standard PCI DSS ne sont pas considérées comme étant en place… » ici, précédemment dans Exigences détaillées du standard PCI DSS et procédures d'évaluation de la sécurité.	Clarification ou orientation
	Autres références	Nouvelle section qui répertorie les organismes de standardisation externes référencés dans les exigences du standard PCI DSS ou les directives.	Clarification ou orientation
Exigences et procédures d'évaluation détaillées de la sécurité du standard PCI DSS	Exigences et procédures de test détaillées du standard PCI DSS	Remplacement du contenu de la première page de la section par une illustration expliquant tous les éléments de la colonne Exigences, de la colonne Procédures de test et de la colonne Directives. À la première page de la section, ajout d'une description pour les exigences notées par « Exigences supplémentaires pour les prestataires de services uniquement ». À la première page de la section, ajout d'un résumé des annexes qui incluent des exigences	Clarification ou orientation

Section		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
		supplémentaires du standard PCI DSS pour différents types d'entités.	

4 Résumé des Modifications Globales Apportées aux Exigences du Standard PCI DSS

Modifications Générales Mises en œuvre Dans l'ensemble des Exigences du Standard PCI DSS	Type de Modification
Remise en forme des sections d'aperçu et ajout d'un résumé des sections au début de chaque exigence principale.	Structure ou format
Mise à jour des sections d'aperçu et ajout de conseils au début de la section de chaque exigence.	Clarification ou orientation
Ajout de titres numérotés de description des exigences dans chaque exigence pour organiser et décrire les exigences qui en relèvent.	Structure ou format
Changement de numérotation des exigences et procédures de test et réorganisation des exigences en raison de l'ajout de titres numérotés de description des exigences.	Structure ou format
Reformulation des exigences des directives pour être objectives.	Evolution de l'exigence
Déplacement des exemples d'exigences ou de procédures de test dans la colonne Orientation.	Structure ou format
Suppression des références à l'échantillonnage des procédures de test.	Clarification ou orientation
Raccourcissement des procédures de test en clarifiant que les tests doivent être effectués « conformément à tous les éléments spécifiés dans la présente exigence » afin de minimiser la redondance entre les exigences et les procédures de test.	Clarification ou orientation
Mise à jour du langage dans les exigences et/ou les procédures de test correspondantes pour plus d'alignement et d'uniformité.	Clarification ou orientation
Amélioration des procédures de test afin de clarifier le niveau de validation escompté pour chaque exigence.	Clarification ou orientation
Remise en forme des exigences et des procédures de test, et légères modifications de la formulation pour une meilleure lisibilité - par exemple, le contenu des paragraphes transformés en puces.	Structure ou format
Combinaison des exigences qui soutiennent la même intention et des exigences séparées qui soutiennent différentes intentions.	Structure ou format
Séparation des exigences/procédures de test complexes et suppression des procédures de test redondantes ou qui se chevauchent.	Structure ou format
Déplacement des éléments obligatoires qui n'étaient inclus que dans les procédures de test vers les exigences afin de clarifier l'exigence et de faciliter le raccourcissement des procédures de test.	Clarification ou orientation
Déplacement et reformulation des exigences des politiques et des procédures de la fin au début de chaque exigence principale.	Structure ou format
Suppression des notes sur les protocoles SSL/TLS initial des colonnes d'orientation pour les exigences faisant référence à ces protocoles spécifiques.	Clarification ou orientation
Modification de « données de titulaire de carte » en « données de compte » selon les besoins pour s'aligner sur l'utilisation et l'intention.	Clarification ou orientation

Modifications Générales Mises en œuvre Dans l'ensemble des Exigences du Standard PCI DSS	Type de Modification
Modification de la terminologie utilisée pour faire référence à la fréquence dans toutes les exigences, conformément à la *Description des délais utilisés dans les exigences du standard PCI DSS.*	Clarification ou orientation
Ajout de titres et réorganisation du contenu de la colonne Orientation afin de faciliter la compréhension et fusionner des informations similaires.	Structure ou format

5 Autres Modifications par Exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Exigence 1			
Exigence 1- Généralité		Mise à jour du titre de l'exigence principale pour refléter l'accent mis sur les « contrôles de sécurité du réseau ». Remplacement de « pare-feu » et de « routeurs » par « contrôles de sécurité réseau » afin de prendre en charge une gamme plus large de technologies utilisées pour répondre aux objectifs de sécurité traditionnellement atteints par les pare-feu.	Evolution de l'exigence
1.1.5	1.1.2	Remplacement de l'exigence relative à la « Description des groupes, des rôles et des responsabilités pour la gestion des composants réseau » par l'exigence générale relative aux rôles et aux responsabilités pour l'Exigence 1.	Evolution de l'exigence
1.1	1.2.1	Recentrage de l'ancienne exigence « nulle » (tout le contenu pointait vers d'autres exigences) sur la définition, la mise en œuvre et la maintenance des normes de configuration pour les ensembles de règles de contrôle de la sécurité du réseau.	Clarification ou orientation
1.1.1	1.2.2	Clarification du fait que les modifications sont gérées conformément au processus de contrôle des modifications défini à l'exigence 6.5.1.	Clarification ou orientation
1.1.4		Suppression de l'exigence redondante.	Clarification ou orientation
1.1.6	1.2.5 1.2.6	Scindée en deux exigences afin de clarifier l'intention de chacune.	Clarification ou orientation
1.1.7	1.2.7	Clarification de l'intention d'examiner les configurations des contrôles de sécurité du réseau au moins une fois tous les six mois.	Clarification ou orientation
1.2		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
1.2.2	1.2.8	Clarification de l'intention de sécuriser les fichiers de configuration.	Clarification ou orientation
1.2.1 1.3.4	1.3.1 1.3.2	Exigence 1.2.1 scindée en deux exigences afin de clarifier l'intention de chacune. Suppression de l'exigence redondante 1.3.4.	Clarification ou orientation
1.2.3	1.3.3	Clarification de l'intention de mettre en œuvre des contrôles de sécurité du réseau entre les réseaux sans fil et le CDE.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
1.3	1.4.1	Recentrage d'une ancienne exigence nulle (tout le contenu pointait vers d'autres exigences). Clarification du fait que l'intention est de mettre en œuvre des contrôles entre les réseaux approuvés et non approuvés.	Clarification ou orientation
1.3.1 1.3.2 1.3.5	1.4.2	Fusion des exigences afin de clarifier que l'intention est de restreindre le trafic entrant provenant de réseaux non approuvés.	Clarification ou orientation
1.3.6	1.4.4	Clarification du fait que les composants système qui stockent les données des titulaires de cartes ne sont pas directement accessibles à partir de réseaux non fiables.	Clarification ou orientation
1.4	1.5.1	Clarification du fait que l'intention est de mettre en œuvre des contrôles de sécurité sur tout appareil informatique qui se connecte à la fois à des réseaux non approuvés et au CDE.	Clarification ou orientation
Exigence 2			
Exigence 2- Généralité		Mise à jour du titre de l'exigence principale pour indiquer que l'accent est mis sur les configurations sécurisées en général, et pas seulement sur les valeurs par défaut fournies par le fournisseur.	Clarification ou orientation
	2.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
2.1	2.2.2	Clarification du fait que l'intention est de comprendre si les comptes par défaut des fournisseurs sont utilisés et de les gérer en conséquence.	Clarification ou orientation
2.2.1	2.2.3	Clarification de l'intention de l'exigence de gestion des fonctions principales qui nécessitent différents niveaux de sécurité.	Clarification ou orientation
2.2.2 2.2.5	2.2.4	Combinaison des exigences pour aligner des sujets similaires.	Structure ou format
2.2.3	2.2.5	Clarification du fait que l'intention de l'exigence est de savoir *si* des services, des protocoles ou des démons non sécurisés sont présents.	Clarification ou orientation
2.1.1	2.3.1 2.3.2	Division de l'exigence relative à la modification de toutes les valeurs par défaut des prestataires de services sans fil en deux exigences afin de clarifier l'objectif de chacune.	Clarification ou orientation
2.4	12.5.1	Déplacement de l'exigence afin d'aligner le contenu connexe.	Structure ou format
2.6		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Exigence 3			
Exigence 3 - Généralité		Mise à jour du titre de l'exigence principale pour qu'elle reflète l'accent mis sur les données de compte.	Clarification ou orientation
	3.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
3.1	3.2.1	**Nouvelle puce de l'exigence** pour traiter les SAD stockées avant l'achèvement de l'autorisation grâce à la mise en œuvre de politiques, de procédures et de processus de conservation et d'élimination des données. *Cette puce est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	3.3.2	**Nouvelle exigence** pour crypter les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
3.2.a 3.2.b	3.3.3	Ajout d'une exigence afin de répondre aux anciennes procédures de test selon lesquelles tout stockage de SAD par les émetteurs est limité à ce qui est nécessaire pour un besoin professionnel légitime de l'émetteur, et est sécurisé.	Clarification ou orientation
3.3	3.4.1	Clarification que le PAN est masqué lorsqu'il est affiché de telle sorte que seul le personnel ayant un besoin professionnel puisse voir plus que le BIN / les quatre derniers chiffres du PAN.	Evolution de l'exigence
12.3.10	3.4.2	**Nouvelle exigence** de contrôles techniques afin d'empêcher la copie et/ou la relocalisation du PAN lors de l'utilisation de technologies d'accès à distance. Développement de l'ancienne exigence 12.3.10. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
3.4	3.5.1	Suppression des clés répertoriées de la puce « tokens d'index et clés répertoriés » pour rendre le PAN illisible.	Evolution de l'exigence
	3.5.1.1	**Nouvelle exigence** pour les hachages cryptographiques à clé lorsque le hachage est utilisé pour rendre le PAN illisible. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	3.5.1.2	**Nouvelle exigence** selon laquelle le cryptage au niveau du disque ou de la partition n'est utilisé que pour rendre le PAN illisible sur un support électronique amovible ou, s'il est utilisé sur un support électronique non amovible, le PAN est également rendu illisible via un mécanisme qui satisfait à l'exigence 3.5.1. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
3.5.1	3.6.1.1	**Nouvelle puce d'exigence pour les prestataires de services uniquement**, à inclure dans la description documentée de l'architecture cryptographique qui empêche l'utilisation des mêmes clés cryptographiques dans les environnements de production et de test. *Cette puce est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
Exigence 4			
Exigence 4 - Généralité		Mise à jour du titre de l'exigence principale pour qu'elle reflète l'accent mis sur la « cryptographie robuste » pour protéger les transmissions de données de titulaires de cartes.	Clarification ou orientation
	4.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
4.1	4.2.1	**Nouvelle puce de l'exigence** pour confirmer que les certificats utilisés pour les transmissions des PAN sur des réseaux publics ouverts sont valides et non expirés ou révoqués. *Cette puce est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	4.2.1.1	**Nouvelle exigence** pour maintenir un inventaire de clés et de certificats de confiance. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Exigence 5			
Exigence 5 - Généralité		Mise à jour du titre de l'exigence principale pour refléter l'accent mis sur la protection de tous les systèmes et réseaux contre les logiciels malveillants.	Clarification ou orientation
		Remplacement complet de « antivirus » par « anti-programmes malveillants » pour prendre en charge une gamme plus large de technologies utilisées pour répondre aux objectifs de sécurité traditionnellement atteints par les logiciels antivirus.	Evolution de l'exigence
	5.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
5.1.2	5.2.3	Clarification de l'exigence en mettant l'accent sur les « composants système qui ne sont pas à risque pour les programmes malveillants ».	Clarification ou orientation
	5.2.3.1	**Nouvelle exigence** pour définir la fréquence des évaluations périodiques des composants système qui ne sont pas à risque pour les programmes malveillants dans l'analyse ciblée des risques de l'entité. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
5.2	5.3.1 5.3.2 5.3.4	Division d'une exigence en trois pour concentrer chaque exigence sur un domaine : • Maintien à jour de la solution anti-programmes malveillants via des mises à jour automatiques, • Exécution d'analyses périodiques et d'analyses actives ou en temps réel (avec une nouvelle option pour l'analyse comportementale en continu), • Génération de journaux d'audit par la solution anti-programmes malveillants.	Clarification ou orientation
	5.3.2.1	**Nouvelle exigence** pour définir la fréquence des scans périodiques de logiciels malveillants dans l'analyse de risque ciblée de l'entité. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	5.3.3	**Nouvelle exigence** pour une solution anti-programmes malveillants sur supports électroniques amovibles. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	5.4.1	**Nouvelle exigence** pour détecter et protéger le personnel contre les attaques d'hameçonnage. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
Exigence 6			
Exigence 6 - Généralité		Mise à jour du titre de l'exigence principale pour inclure « logiciel » plutôt que « applications ». Clarification que l'exigence 6 s'applique à tous les composants système, à l'exception de l'exigence 6.2 qui s'applique uniquement aux logiciels sur mesure et personnalisés.	Clarification ou orientation
	6.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
6.3	6.2.1	Déplacement sous l'exigence 6.2 de l'exigence relative au développement sécurisé de logiciels afin d'aligner tout le contenu de développement de logiciels.	Structure ou format
		Remplacement de logiciel « interne et externe » par logiciel « sur mesure et personnalisé ». Clarification que cette exigence s'applique aux logiciels développés pour ou par l'entité pour son propre usage et ne s'applique pas aux logiciels tiers.	Clarification ou orientation
6.5	6.2.2	Déplacement sous l'exigence 6.2 des éléments de l'exigence 6.5 pour la formation des développeurs de logiciels afin d'aligner tout le contenu de développement de logiciels. Clarification de l'exigence relative à la formation du personnel de développement de logiciels.	Clarification ou orientation
6.3.2	6.2.3 6.2.3.1	Déplacement sous l'exigence 6.2 de l'exigence relative à l'examen des logiciels personnalisés avant leur publication afin d'aligner tout le contenu de développement logiciel. Division de l'exigence pour séparer les pratiques générales de révision du code de celles nécessaires si des révisions manuelles du code sont effectuées.	Clarification ou orientation
6.5.1 – 6.5.10	6.2.4	Déplacement sous l'exigence 6.2 des exigences pour traiter les vulnérabilités de codage courantes afin d'aligner tout le contenu de développement logiciel. Combinaison des méthodes pour prévenir ou atténuer les attaques logicielles courantes en une seule exigence, et généralisation du langage décrivant chaque type d'attaque.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
6.1 6.2	6.3	Déplacement sous l'exigence 6.3 de l'exigence pour l'identification des vulnérabilités de sécurité et la protection des composants système contre les vulnérabilités via l'application de correctifs.	Structure ou format
6.1	6.3.1	Ajout d'une puce pour clarifier l'applicabilité aux vulnérabilités des logiciels sur mesure, personnalisés et tiers.	Clarification ou orientation
	6.3.2	**Nouvelle exigence** pour maintenir un inventaire de logiciels sur mesure et personnalisés. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
6.6	6.4.1	Déplacement sous l'exigence 6.4 de l'exigence relative à la gestion des nouvelles menaces et vulnérabilités pour les applications Web destinées au public.	Structure ou format
	6.4.2	**Nouvelle exigence** pour le déploiement d'une solution technique automatisée pour les applications Web destinées au public qui détecte et empêche en permanence les attaques Web. Cette nouvelle exigence élimine l'option de l'exigence 6.4.1 d'examiner les applications Web via des outils ou des méthodes d'évaluation manuelle ou automatisée de la vulnérabilité des applications. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	6.4.3	**Nouvelle exigence** pour la gestion de tous les scripts de page de paiement qui sont chargés et exécutés dans le navigateur du consommateur. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
6.3.1 6.4 6.4.1 – 6.4.6	6.5.1 – 6.5.6	Déplacement sous l'exigence 6.5 et combinaison des exigences pour les modifications apportées aux composants système.	Structure ou format
6.4	6.5.3 6.5.4 6.5.5 6.5.6	Suppression de l'exigence relative aux procédures documentées spécifiques, et ajout de procédures de test pour vérifier les politiques et les procédures de chaque exigence connexe.	Clarification ou orientation
6.4.1	6.5.3	Modification des termes « développement/test et production » en « environnements de production et de pré-production ».	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
6.4.2	6.5.4	Modification des termes « développement/test et production » en « environnements de production et de pré-production ». Modification du terme « séparation des tâches » et clarification du fait que la séparation des rôles et des fonctions entre la production et la pré-production vise à assurer la responsabilité afin que seules les modifications approuvées soient déployées.	Clarification ou orientation
6.4.3	6.5.5	Modification du terme de « test ou développement » en environnements de « pré-production ». Clarification du fait que les PAN actifs ne sont pas utilisés dans les environnements de pré-production, sauf lorsque toutes les exigences applicables du standard PCI DSS sont en place.	Clarification ou orientation
Exigence 7			
Exigence 7 - Généralité		Mise à jour du titre de l'exigence principale pour inclure les composants système et les données de titulaires de cartes.	Clarification ou orientation
	7.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
7.1	7.2.1 7.2.2 7.2.3	Suppression de l'exigence relative aux procédures documentées spécifiques, et ajout de procédures de test pour vérifier les politiques et les procédures de chaque exigence connexe.	Clarification ou orientation
7.1.1	7.2.1	Clarification que l'exigence concerne la définition d'un modèle de contrôle d'accès.	Clarification ou orientation
7.1.2 7.1.3	7.2.2	Combinaison des exigences pour l'attribution de l'accès en fonction de la classification et de la fonction du poste, et des moindres privilèges.	Structure ou format
7.1.4	7.2.3	Clarification que l'exigence concerne l'approbation des privilèges requis par le personnel autorisé.	Clarification ou orientation
	7.2.4	**Nouvelle exigence** pour l'examen de tous les comptes d'utilisateurs et des privilèges d'accès associés. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	7.2.5	**Nouvelle exigence** pour l'attribution et la gestion de tous les comptes d'applications et système et des privilèges d'accès associés. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	7.2.5.1	**Nouvelle exigence** pour l'examen de tous les accès par les comptes d'applications et système et les privilèges d'accès associés. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
8.7	7.2.6	Déplacement de l'exigence car elle correspond mieux au contenu de l'exigence 7.	Structure ou format
7.2		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
Exigence 8			
Exigence 8 - Généralité		Normalisation sur les termes « facteur d'authentification » et « identifiants d'authentification ». Suppression des « utilisateurs non consommateurs » et clarification dans l'aperçu que les exigences ne s'appliquent pas aux comptes utilisés par les consommateurs (titulaires de cartes).	Clarification ou orientation
		Suppression de la note dans l'aperçu qui énumérait les exigences qui ne s'appliquent pas aux comptes d'utilisateurs ayant accès à un seul numéro de carte à la fois pour faciliter une seule transaction, et ajout de cette note à chaque exigence connexe.	Structure ou format
	8.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
8.1.1	8.2.1	Ajout d'une note indiquant que 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.	Clarification ou orientation
8.5	8.2.2	Modification de l'objectif de l'exigence pour permettre l'utilisation d'identifiants d'authentification partagés, mais uniquement sur une base exceptionnelle.	Evolution de l'exigence
		Ajout d'une note indiquant que 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.	Clarification ou orientation
8.5 8.5.1	8.2.2 8.2.3	Déplacement sous l'exigence 8.2 de l'exigence relative aux comptes de groupe, partagés ou génériques et aux prestataires de services ayant un accès à distance aux locaux des clients.	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
8.1.8	8.2.8	Ajout d'une note indiquant que 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.	Structure ou format
8.2	8.3.1	Ajout d'une note indiquant que 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.	Structure ou format
8.1.6 8.1.7	8.3.4	Fusion des exigences et leur déplacement sous l'exigence 8.3. Ajout d'une note indiquant que 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.	Structure ou format
		Augmentation du nombre de tentatives d'authentification non valides avant le verrouillage d'un ID utilisateur de six à 10 tentatives.	Evolution de l'exigence
8.2.6	8.3.5	Clarification que cette exigence ne s'applique que si des mots de passe/phrases secrètes sont utilisés comme facteur d'authentification pour satisfaire à l'exigence 8.3.1.	Clarification ou orientation
8.2.3	8.3.6	**Nouvelle exigence** pour augmenter la longueur du mot de passe d'une longueur minimale de sept caractères à une longueur minimale de 12 caractères (ou si le système ne prend pas en charge 12 caractères, une longueur minimale de huit caractères). *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.* Clarification que, jusqu'au 31 mars 2025, les mots de passe doivent avoir une longueur minimale d'au moins sept caractères conformément à l'exigence 8.2.3 de la version v3.2.1. Clarification que cette exigence ne s'applique que si des mots de passe/phrases secrètes sont utilisés comme facteur d'authentification pour satisfaire à l'exigence 8.3.1. Ajout d'une note indiquant que 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.	Evolution de l'exigence
8.2.5	8.3.7	Ajout d'une note indiquant que 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.	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
8.4	8.3.8	Déplacement sous l'exigence 8.3 du contenu sur la communication des politiques et procédures d'authentification des utilisateurs.	Structure ou format
8.2.4	8.3.9	Clarification que cette exigence s'applique si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès des utilisateurs (c'est-à-dire, dans toute implémentation d'authentification à facteur unique). Ajout d'une note indiquant que 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. Ajout d'une note indiquant que l'exigence ne s'applique pas aux comptes clients des prestataires de services mais s'applique aux comptes du personnel des prestataires de services.	Clarification ou orientation
8.2.4	8.3.9	Ajout de l'option permettant de déterminer automatiquement l'accès aux ressources en analysant dynamiquement la posture de sécurité des comptes, au lieu de changer les mots de passe/phrases secrètes au moins une fois tous les 90 jours.	Evolution de l'exigence
8.2.4.b	8.3.10	Déplacement du contenu d'une ancienne procédure de test vers une exigence pour les prestataires de services de fournir des conseils aux clients sur la modification des mots de passe/phrases secrètes. Ajout d'une note indiquant que cette exigence sera remplacée par l'exigence 8.3.10.1 une fois que l'exigence 8.3.10.1 entre en vigueur.	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	8.3.10.1	**Nouvelle exigence pour les prestataires de services uniquement** - si les mots de passe/phrases secrètes sont le seul facteur d'authentification pour l'accès des utilisateurs clients, alors les mots de passe/phrases secrètes sont soit modifiés au moins une fois tous les 90 jours, soit l'accès aux ressources est automatiquement déterminé en analysant dynamiquement la posture de sécurité des comptes. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.* Ajout d'une note indiquant que cette exigence ne s'applique pas aux comptes des utilisateurs consommateurs accédant à leurs informations de carte de paiement. Ajout d'une note indiquant que cette exigence remplacera l'exigence 8.3.10 une fois qu'elle entrera en vigueur, et jusqu'à cette date, les prestataires de services peuvent satisfaire à l'exigence 8.3.10 ou 8.3.10.1.	Evolution de l'exigence
8.6	8.3.11	Déplacement sous l'exigence 8.3 de l'exigence relative aux facteurs d'authentification tels que les tokens de sécurité physiques ou logiques, les cartes à puce et les certificats.	Structure ou format
8.3		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
	8.4.2	**Nouvelle exigence** pour mettre en œuvre l'authentification à plusieurs facteurs (MFA) pour tous les accès au CDE. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.* Ajout d'une note pour clarifier que la MFA est requise pour les deux types d'accès spécifiés dans les exigences 8.4.2 et 8.4.3 ; et que l'application de la MFA à un type d'accès ne remplace pas la nécessité d'appliquer une autre instance de MFA à l'autre type d'accès.	Evolution de l'exigence
	8.5.1	**Nouvelle exigence** pour la mise en œuvre sécurisée des systèmes d'authentification à plusieurs facteurs. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	8.6.1	**Nouvelle exigence** pour la gestion des systèmes ou des comptes d'applications pouvant être utilisés pour la connexion interactive. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	8.6.2	**Nouvelle exigence** pour ne pas coder en dur les mots de passe/phrases secrètes dans des fichiers ou des scripts pour toutes les applications et tous les comptes système pouvant être utilisés pour une connexion interactive. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	8.6.3	**Nouvelle exigence** pour la protection des mots de passe/phrases secrètes pour les comptes d'applications et système contre les abus. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
8.7	7.2.6	Déplacement de l'exigence car elle correspond mieux au contenu de l'exigence 7.	Structure ou format
Exigence 9			
Exigence 9 - Généralité		Dans l'aperçu, clarification des trois différents domaines couverts par l'exigence 9 (zones sensibles, CDE et installations). Partout, clarification apportée pour préciser si chaque exigence s'applique au CDE, aux zones sensibles ou aux sites.	Clarification ou orientation
	9.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
9.1	9.2.4	Ajout d'une exigence pour adresser un ancien point de procédure de test afin de restreindre l'accès aux consoles dans les zones sensibles via le verrouillage lorsqu'elles ne sont pas utilisées.	Clarification ou orientation
9.2	9.3.1 9.3.2	Division de l'exigence d'identification du personnel et des visiteurs en exigences distinctes, exigences 9.3.1 et 9.3.2, respectivement.	Structure ou format
9.4 9.4.1 9.4.2	9.3.2	Combinaison des exigences pour autoriser et gérer l'accès des visiteurs ensemble dans l'exigence 9.3.2.	Structure ou format
9.5 9.5.1	9.4.1 9.4.1.1 9.4.1.2	Suppression de l'exigence relative aux procédures de sécurisation physique des supports (9.5) et fusion des procédures dans les exigences associées. Division en 2 exigences de l'exigence relative au stockage des sauvegardes de médias dans un emplacement sécurisé et à l'examen de la sécurité de l'emplacement de sauvegarde hors ligne au moins tous les 12 mois.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	**PCI DSS v4.0**		
9.6 9.6.1 9.6.2 9.6.3	9.4.2 9.4.3 9.4.4	Suppression de l'exigence relative aux procédures de distribution interne et externe des médias (9.6) et fusion des procédures dans les exigences associées.	Clarification ou orientation
9.7 9.7.1	9.4.5 9.4.5.1	Suppression de l'exigence relative aux procédures de contrôle strict du stockage et de l'accessibilité des supports (9.7) et fusion des procédures dans les exigences associées. Division en 2 exigences de l'exigence relative à la tenue des journaux d'inventaire des médias et à la réalisation d'inventaires des médias sur une base annuelle.	Clarification ou orientation
9.8 9.8.1 9.8.2	9.4.6 9.4.7	Suppression de l'exigence relative aux procédures de destruction des supports lorsque les supports ne sont plus nécessaires (9.8) et fusion des procédures dans les exigences associées. Clarification du fait que les options pour la destruction des supports lorsqu'ils ne sont plus nécessaires comprennent soit la destruction des supports électroniques, soit le fait de rendre les données des titulaires de cartes irrécupérables.	Clarification ou orientation
9.9	9.5.1	Clarification de l'objectif de l'exigence sur les équipements “Point-of-interaction (POI) qui capturent les données de carte de paiement via une interaction physique directe avec le facteur de forme de la carte de paiement.” Clarification du fait que l'exigence s'applique aux équipements POI déployés utilisés dans les transactions avec carte présente.	Clarification ou orientation
	9.5.1.2.1	**Nouvelle exigence** pour définir la fréquence des inspections périodiques des dispositifs POI sur la base de l'analyse de risque ciblée de l'entité. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l’exigence
Exigence 10			
Exigence 10 - Généralité		Mise à jour du titre de l'exigence principale pour refléter l'accent mis sur les journaux d'audit, les composants système et les données des titulaires de cartes. Clarification du fait que les exigences ne s'appliquent pas à l'activité d'utilisateur des consommateurs (titulaires de cartes). Remplacement partout de « Pistes d'audit » par « Journaux d'audit ».	Clarification ou orientation
	10.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l’exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
10.2		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
10.5		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
10.5.1 – 10.5.5	10.3.1 – 10.3.4	Déplacement sous l'exigence 10.3 des exigences relatives à la protection des journaux d'audit.	Structure ou format
10.5.3 10.5.4	10.3.3	Combinaison des exigences pour aligner des sujets similaires.	Structure ou format
10.6		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
10.6.1 – 10.6.3	10.4.1 – 10.4.3	Déplacement sous l'exigence 10.4 des exigences relatives aux examens des journaux d'audit.	Structure ou format
	10.4.1.1	**Nouvelle exigence** pour l'utilisation de mécanismes automatisés pour effectuer les examens des journaux d'audit. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	10.4.2.1	**Nouvelle exigence** pour une analyse de risque ciblée afin de définir la fréquence des examens périodiques des journaux pour tous les autres composants système (non définie dans l'exigence 10.4.1) *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
10.7	10.5.1	Déplacement vers 10.5.1 de l'exigence relative à l'historique des journaux d'audit.	Structure ou format
10.4 10.4.1 – 10.4.3	10.6.1 – 10.6.3	Déplacement sous 10.6 et réorganisation des exigences pour la synchronisation temporelle.	Structure ou format
10.8	10.7.1	Déplacement vers l'exigence 10.7.1 de l'exigence *pour les prestataires de services* de détecter, d'alerter et de traiter rapidement les défaillances des systèmes de contrôle critiques.	Structure ou format
	10.7.2	**Nouvelle exigence** *pour toutes les entités* de détecter, d'alerter et de traiter rapidement les défaillances des systèmes critiques de contrôle de sécurité. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.* Cette nouvelle exigence s'applique à *toutes les entités* - elle comprend deux contrôles de sécurité critiques supplémentaires non inclus dans l'exigence 10.7.1 pour les prestataires de services.	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
10.8.1	10.7.3	**Nouvelle exigence** pour répondre rapidement aux défaillances de tout contrôle de sécurité critique. Pour les prestataires de services : il s'agit de l'exigence actuelle du standard PCI DSS v3.2.1. Pour toutes les autres entités (non-prestataires de services) : il s'agit d'une nouvelle exigence. *Cette exigence est une bonne pratique (pour les non-prestataires de services) jusqu'au 31 mars 2025.*	Evolution de l'exigence
Exigence 11			
Exigence 11 - Généralité		Mise à jour mineure du titre de l'exigence principale.	Clarification ou orientation
	11.1.2	**Nouvelle exigence** pour les rôles et les responsabilités. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
11.1	11.2.1	Clarification du fait que l'intention de l'exigence est de gérer les points d'accès sans fil autorisés et non autorisés. Clarification du fait que cette exigence s'applique même lorsqu'il existe une politique interdisant l'utilisation de la technologie sans fil.	Clarification ou orientation
	11.3.1.1	**Nouvelle exigence** pour gérer toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme à haut risque ou critiques) trouvées lors des scans de vulnérabilité internes. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	11.3.1.2	**Nouvelle exigence** pour effectuer des scans de vulnérabilité internes via un scan authentifié. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
11.2.3	11.3.1.3 11.3.2.1	Séparation de l'exigence d'effectuer des scans de vulnérabilité internes et externes et des scans de vérification après tout changement significatif en une exigence de scans internes (11.3.1.3) et une exigence de scans externes (11.3.2.1).	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
11.3	11.4.1	Clarification des éléments suivants : • La méthodologie est définie, documentée et mise en œuvre par l'entité. • Les résultats des tests d'intrusion sont conservés pendant au moins 12 mois. • La méthodologie comprend 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. • La signification des tests depuis l'intérieur du réseau (tests d'intrusion internes) et depuis l'extérieur du réseau (tests d'intrusion externes).	Clarification ou orientation
11.3.3	11.4.4	Clarification du fait que les résultats des tests d'intrusion sont corrigés conformément à l'évaluation par l'entité du risque posé par le problème de sécurité.	Clarification ou orientation
	11.4.7	**Nouvelle exigence pour les prestataires de services mutualisés** pour assister leurs clients dans les tests d'intrusion externes. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	11.5.1.1	**Nouvelle exigence pour les fournisseurs de services** d'utiliser les techniques de détection et/ou de prévention des intrusions afin de détecter, alerter/prévenir et traiter les canaux secrets de communication des logiciels malveillants. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	11.6.1	**Nouvelle exigence** pour le déploiement d'un mécanisme de détection de modifications et de falsification pour alerter des modifications non autorisées des en-têtes HTTP et du contenu des pages de paiement tel que reçu par le navigateur du consommateur. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
11.2		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
11.1.2	12.10.5	Déplacement de l'exigence pour les procédures de réponse aux incidents si des points d'accès sans fil non autorisés sont détectés afin de s'aligner sur d'autres éléments de réponse aux incidents.	Structure ou format
11.5.1	12.10.5	Déplacement de l'exigence relative à la réponse aux alertes générées par la solution de détection de modification afin de s'aligner sur les autres éléments de réponse aux incidents.	Structure ou format

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Exigence 12			
Exigence 12 - Généralité		Mise à jour du titre de l'exigence principale pour indiquer que l'accent est mis sur les politiques et les programmes organisationnels qui appuient la sécurité des informations.	Clarification ou orientation
12.2		Suppression de l'exigence relative à une évaluation formelle des risques à l'échelle de l'entreprise et son remplacement par des analyses de risques ciblées spécifiques (12.3.1 et 12.3.2).	Evolution de l'exigence
12.4	12.1.3	Ajout d'une reconnaissance formelle par le personnel de ses responsabilités.	Evolution de l'exigence
12.5 12.5.1 – 12.5.5	12.1.4	Clarification du fait que les responsabilités sont officiellement attribuées à un responsable de la sécurité du système d'informations (RSSI) ou à un autre membre compétent de la direction. Fusion des exigences relatives à l'attribution officielle de la responsabilité de la sécurité de l'information.	Clarification ou orientation
12.3 12.3.1 – 12.3.9	12.2.1	Clarification de l'intention de l'exigence relative aux politiques d'utilisation acceptable pour les technologies d'utilisateur final. Fusion et suppression d'exigences pour se focaliser sur l'approbation explicite de la direction, les utilisations acceptables des technologies et une liste de produits matériels et logiciels approuvés par l'entreprise pour l'utilisation par les employés.	Clarification ou orientation
12.3.10	3.4.2	Suppression de l'exigence et ajout de la nouvelle exigence 3.4.2 pour les contrôles techniques afin d'empêcher la copie et/ou la relocalisation du PAN lors de l'utilisation de technologies d'accès à distance.	Evolution de l'exigence
	12.3.1	**Nouvelle exigence** pour effectuer une analyse ciblée des risques pour toute exigence du standard PCI DSS qui offre une flexibilité quant à la fréquence de son exécution. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	12.3.2	**Nouvelle exigence pour les entités utilisant une approche personnalisée** d'effectuer une analyse de risque ciblée pour chaque exigence du standard PCI DSS que l'entité satisfait avec l'approche personnalisée. *Cette exigence est effective immédiatement pour toutes les entités subissant une évaluation de la version v4.0 et utilisant une approche personnalisée.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	12.3.3	**Nouvelle exigence** pour documenter et examiner les suites et protocoles de chiffrement cryptographiques utilisés au moins une fois tous les 12 mois. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	12.3.4	**Nouvelle exigence** pour examiner les technologies matérielles et logicielles utilisées au moins une fois tous les 12 mois. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
12.11 12.11.1	12.4.2 12.4.2.1	Déplacement des exigences relatives aux examens pour confirmer que le personnel exécute les tâches du standard PCI DSS conformément aux politiques et procédures de l'exigence 12.4, afin de s'aligner sur les autres exigences relatives à la gestion des activités de conformité du standard PCI DSS.	Structure ou format
2.4	12.5.1	Déplacement sous l'exigence 12.5 afin de s'aligner sur d'autres exigences de documentation et de validation du périmètre PCI DSS.	Structure ou format
	12.5.2	**Nouvelle exigence** pour documenter et confirmer le périmètre PCI DSS au moins tous les 12 mois et en cas de changement significatif de l'environnement à l'intérieur du périmètre PCI DSS. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
	12.5.2.1	**Nouvelle exigence pour les fournisseurs de services** pour documenter et confirmer le périmètre PCI DSS au moins une fois tous les six mois et en cas de changement significatif de l'environnement à l'intérieur du périmètre PCI DSS. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	12.5.3	**Nouvelle exigence pour les fournisseurs de services** pour un examen documenté de l'impact sur le périmètre PCI DSS et de l'applicabilité des contrôles lors des changements significatifs de structure organisationnelle. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
12.6	12.6.1	Clarification du fait que l'intention est que tout le personnel connaisse la politique de sécurité de l'information de l'entité et son rôle dans la protection des données des titulaires de cartes.	Clarification ou orientation
	12.6.2	**Nouvelle exigence** pour examiner et mettre à jour (au besoin) le programme de sensibilisation à la sécurité au moins une fois tous les 12 mois. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
12.6.1 12.6.2	12.6.3	Fusion des exigences relatives à la sensibilisation à la sécurité.	Structure ou format
	12.6.3.1	**Nouvelle exigence** pour la sensibilisation à la sécurité pour inclure la sensibilisation aux menaces et aux vulnérabilités qui pourraient avoir une incidence sur la sécurité du CDE. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	12.6.3.2	**Nouvelle exigence** concernant la sensibilisation à la sécurité pour inclure la sensibilisation à l'utilisation acceptable des technologies de l'utilisateur final conformément à l'exigence 12.2.1. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
12.8		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
12.8.1 – 12.8.5	12.8.1 – 12.8.5	Remplacement de « Fournisseur de services » par Prestataire de services tiers (TPSP). Clarification du fait que 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.	Clarification ou orientation
12.8.2	12.8.2	Remplacement de « Fournisseur de services » par Prestataire de services tiers (TPSP).	Clarification ou orientation
12.8.3	12.8.3	Remplacement de « Fournisseur de services » par Prestataire de services tiers (TPSP).	Clarification ou orientation
12.8.4	12.8.4	Remplacement de « Fournisseur de services » par Prestataire de services tiers (TPSP). Clarification du fait que lorsqu'une entité passe un accord avec un TPSP pour satisfaire aux exigences du standard PCI DSS au nom de l'entité, l'entité doit collaborer avec le TPSP pour s'assurer que les exigences applicables du standard 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.	Clarification ou orientation
12.8.5	12.8.5	Remplacement de « Fournisseur de services » par Prestataire de services tiers (TPSP). Clarification du fait que les informations sur les exigences du standard PCI DSS gérées par le TPSP et l'entité doivent inclure celles qui sont partagées entre le TPSP et l'entité.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	12.9.2	**Nouvelle exigence pour les fournisseurs de services** pour prendre en charge les demandes d'informations de leurs clients pour satisfaire aux exigences 12.8.4 et 12.8.5. *Cette exigence est effective immédiatement pour toutes les évaluations de la v4.0.*	Evolution de l'exigence
12.10		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
12.10.1	12.10.1	Remplacement de « violation du système » et « compromission » par « incident de sécurité soupçonné ou confirmé ».	Clarification ou orientation
12.10.3	12.10.3	Remplacement de « alertes » par « incidents de sécurité soupçonnés ou confirmés ».	Clarification ou orientation
12.10.4	12.10.4	Remplacement de « violation du système » par « incidents de sécurité soupçonnés ou confirmés ».	Clarification ou orientation
	12.10.4.1	**Nouvelle exigence** pour effectuer une analyse de risque ciblée afin de définir la fréquence des formations périodiques du personnel intervenant en cas d'incident. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
12.10.5 11.1.2 11.5.1	12.10.5	Fusion des exigences et mise à jour des systèmes de surveillance de la sécurité à suivre et à traiter dans le cadre du plan de réponse aux incidents pour inclure les éléments suivants : • Détection des points d'accès sans fil non autorisés (ancienne 11.1.2), • Mécanisme de détection des modifications pour les fichiers critiques (ancienne 11.5.1), • **Nouvelle puce d'exigence** concernant l'utilisation d'un mécanisme de détection des modifications et de falsification pour les pages de paiement (se rapporte à la nouvelle exigence 11.6.1). *Cette puce est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	12.10.7	**Nouvelle exigence** pour que les procédures de réponse aux incidents soient en place et lancées lors de la détection d'un PAN stocké partout où il n'est pas censé l'être. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	**PCI DSS v4.0**		
Annexe A1			
Annexe A1 - Généralité		Mise à jour du titre des exigences principales afin de refléter l'accent mis sur les prestataires de services mutualisés. Mise à jour de l'aperçu des exigences pour décrire les prestataires de services mutualisés et leurs environnements, et pour clarifier les responsabilités entre les prestataires de services mutualisés et leurs clients. Mise à jour globale de « fournisseur d'hébergement partagé » en « fournisseur d'hébergement mutualisé ».	Clarification ou orientation
A1		Suppression de l'exigence « nulle » (tout le contenu pointait vers d'autres exigences).	Structure ou format
	A1.1.1	**Nouvelle exigence** pour la mise en œuvre d'une séparation logique entre les environnements des prestataires et les environnements des clients. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	A1.1.4	**Nouvelle exigence** pour confirmer, via des tests d'intrusion, l'efficacité des contrôles de séparation logique utilisés pour séparer les environnements des clients. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
	A1.2.3	**Nouvelle exigence** pour la mise en œuvre de processus et de mécanismes de signalement et de traitement des incidents de sécurité et des vulnérabilités soupçonnés ou confirmés. *Cette exigence est une bonne pratique jusqu'au 31 mars 2025.*	Evolution de l'exigence
A1.4	A1.2.2	Remplacement de « compromission » par « incident de sécurité soupçonné ou confirmé ».	Clarification ou orientation
Annexe A2			
Les seules modifications apportées à l'Annexe A2 consistaient à ajouter l'en-tête de description de l'exigence à A2.1 et à renuméroter les trois exigences en A2.1.1, A2.1.2 et A2.1.3.			Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Annexe A3			
Annexe A3 - Généralité		Clarification du fait que d'autres standards PCI peuvent faire référence à la réalisation de la présente annexe. Clarification du fait que toutes les exigences du standard PCI DSS ne s'appliquent pas à toutes les entités qui subissent une évaluation du standard PCI DSS, c'est la raison pour laquelle certaines exigences du standard PCI DSS sont dupliquées dans la présente annexe. Toute question concernant la présente annexe doit être adressée aux acquéreurs ou aux marques de paiement.	Clarification ou orientation
A3.2.1	A3.2.1	Mise à jour des éléments inclus pour la documentation et la confirmation du champ d'application du standard PCI DSS afin de s'aligner sur la nouvelle exigence 12.5.2 du standard PCI DSS.	Evolution de l'exigence
	A3.3.1	**Nouvelle puce d'exigence** pour détecter, alerter et signaler les défaillances des mécanismes d'examen automatisé des journaux. **Nouvelle puce d'exigence** pour détecter, alerter et signaler les défaillances des outils d'examen automatisé du code. Ces puces sont des meilleures pratiques jusqu'au 31 mars 2025.	Evolution de l'exigence
Annexe B : Contrôles compensatoires	Annexe B : Contrôles compensatoires	Clarification du fait que des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas satisfaire explicitement à une exigence du standard PCI DSS telle qu'elle est rédigée, en raison de « contraintes techniques ou commerciales légitimes et documentées ». Mise à jour de l'élément 2 pour mentionner l'objectif de l'approche personnalisée et son utilisation afin de comprendre l'intention de la plupart des exigences du standard PCI DSS. Clarification du fait que l'intention de l'élément 4 est de traiter le risque imposé par le non-respect de l'exigence du standard PCI DSS. Ajout de l'élément 6 afin de clarifier que les contrôles compensatoires sont utilisés pour répondre aux exigences actuelles et à venir, et qu'ils ne peuvent pas être utilisés pour satisfaire à une exigence manquée dans le passé.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
Annexe C : Feuille de travail des contrôles compensatoires	Annexe C : Feuille de travail des contrôles compensatoires	Clarification du fait que l'intention est que l'entité utilise la feuille de travail pour définir ses contrôles compensatoires. Mise à jour de l'élément 1 « Documenter les contraintes techniques ou commerciales légitimes empêchant la conformité à l'exigence d'origine. » Réorganisation des éléments de la feuille de travail pour déplacer l'élément 4 vers l'élément 2. Mise à jour de l'élément 3 pour mentionner l'objectif de l'approche personnalisée, et division de l'élément en deux parties : « Définir l'objectif du contrôle d'origine » et « Identifier l'objectif atteint par le contrôle compensatoire ». Suppression de la feuille de travail des contrôles compensatoires - développement de l'exemple. Mise à jour d'un exemple élaboré et son inclusion dans un document d'orientation distinct.	Clarification ou orientation
	Annexe D : Approche personnalisée	**Nouvelle annexe** pour expliquer et fournir des instructions concernant l'approche personnalisée.	Clarification ou orientation
	Annexe E : Exemples de modèles pour soutenir une approche personnalisée	**Une nouvelle annexe** pour des exemples de modèles de matrice de contrôles et d'analyse ciblée de risques, à documenter par l'entité dans le cadre de l'approche personnalisée. Clarification du fait que les entités ne sont pas tenues de suivre les formats de modèle spécifiques mais doivent fournir toutes les informations telles que définies dans chaque modèle. Comprend deux modèles : • E1 Exemple de modèle de matrice de contrôles • E2 Exemple de modèle d'analyse ciblée des risques.	Clarification ou orientation
	Annexe F : Exploiter le cadre de sécurité logicielle PCI pour prendre en charge l'exigence 6	**Nouvelle annexe** pour décrire comment une entité peut satisfaire à plusieurs exigences de l'exigence 6 en utilisant un logiciel sur mesure ou personnalisé, développé et maintenu conformément à l'un des standards de logiciel sécurisé (Secure Software Standards) du PCI SSC.	Clarification ou orientation

Exigence		Description de la Modification	Type de Modification
PCI DSS v3.2.1	PCI DSS v4.0		
	Annexe G : Glossaire des termes, abréviations et acronymes du standard PCI DSS	**Nouvelle annexe** pour le glossaire du standard PCI DSS v4.0. Les mises à jour générales du glossaire comprennent : • Ajout de nouveaux termes basés sur des exigences mises à jour ou sur la base de commentaires, • Suppression des termes communs qui peuvent être facilement trouvés avec d'autres sources, • Suppression des termes non utilisés dans le standard PCI DSS v4.0, • Abrégement des définitions des acronymes.	Clarification ou orientation
Annexe D : Segmentation et échantillonnage des installations commerciales/composants système		Suppression de l'annexe et déplacement de l'ancien contenu vers les sections intitulées « Segmentation » et « Pour les évaluateurs : Échantillonnage pour les évaluations du standard PCI DSS. »	Clarification ou orientation

6 Résumé des Nouvelles Exigences

Comme indiqué dans le tableau ci-dessous, les nouvelles exigences incluses dans le standard PCI DSS v4.0 sont soit :

- En vigueur immédiatement pour toutes les évaluations PCI DSS v4.0.

  OU

- Des bonnes pratiques jusqu'au 31 mars 2025, après quoi elles entrent en vigueur.

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
2.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 2 sont documentés, attribués et compris.	✓		✓	
3.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 3 sont documentés, attribués et compris.	✓		✓	
3.2.1	Les SAD stockées avant l'achèvement de l'autorisation sont réduites au minimum via la mise en œuvre de politiques, de procédures et de processus de conservation et d'élimination des données.	✓			✓
3.3.2	Les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation sont cryptées à l'aide d'une cryptographie robuste.	✓			✓
3.3.3	Les SAD stockées par les émetteurs sont cryptées à l'aide d'une cryptographie robuste.		✓[1]		✓
3.4.2	Des contrôles techniques afin d'empêcher la copie et/ou la relocalisation du PAN lors de l'utilisation de technologies d'accès à distance, sauf autorisation explicite.	✓			✓
3.5.1.1	Les hachages utilisés pour rendre le PAN illisible (selon la première puce de l'exigence 3.5.1) sont des hachages cryptographiques de l'ensemble du PAN, avec les processus et procédures de gestion des clés associés.	✓			✓

[1]Ne s'applique qu'aux émetteurs et aux entreprises qui prennent en charge les services d'émission et stockent des données d'authentification sensibles.

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
3.5.1.2	Mise en œuvre du chiffrement au niveau du disque ou au niveau de la partition lorsqu'il est utilisé pour rendre le PAN illisible.	✓			✓
3.6.1.1	Une description documentée de l'architecture cryptographique comprend la prévention de l'utilisation de clés cryptographiques dans les environnements de production et de test.		✓		✓
4.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 4 sont documentés, attribués et compris.	✓		✓	
4.2.1	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.	✓			✓
4.2.1.1	Un inventaire des clés et des certificats de confiance de l'entité est maintenu.	✓			✓
5.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 5 sont documentés, attribués et compris.	✓		✓	
5.2.3.1	Une analyse ciblée des risques est effectuée pour déterminer la fréquence des évaluations périodiques des composants systèmes identifiés comme ne présentant aucun risque de programmes malveillants.	✓			✓
5.3.2.1	Une analyse ciblée des risques est effectuée pour déterminer la fréquence des analyses périodiques des programmes malveillants.	✓			✓
5.3.3	Des analyses anti-programmes malveillants sont effectuées lorsqu'un support électronique amovible est utilisé.	✓			✓
5.4.1	Mécanismes automatisés sont en place pour détecter et protéger le personnel contre les attaques d'hameçonnage.	✓			✓
6.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 6 sont documentés, attribués et compris.	✓		✓	

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
6.3.2	Le maintien d'un inventaire des logiciels sur mesure et personnalisés afin de faciliter la gestion des vulnérabilités et des correctifs.	✓			✓
6.4.2	Déploiement d'une solution technique automatisée pour les applications Web destinées au public qui détecte et empêche en permanence les attaques Web.	✓			✓
6.4.3	Gestion de tous les scripts de la page de paiement qui sont chargés et exécutés dans le navigateur du client.	✓			✓
7.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 7 sont documentés, attribués et compris.	✓		✓	
7.2.4	Examen de tous les comptes d'utilisateurs et des privilèges d'accès associés de manière appropriée.	✓			✓
7.2.5	Attribution et gestion de tous les comptes d'applications et système et les privilèges d'accès associés de manière appropriée.	✓			✓
7.2.5.1	Examiner l'accès par les applications et le système et les privilèges d'accès associés de manière appropriée.	✓			✓
8.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 8 sont documentés, attribués et compris.	✓		✓	
8.3.6	Niveau minimum de complexité des mots de passe lorsqu'ils sont utilisés comme facteur d'authentification.	✓			✓
8.3.10.1	Si les mots de passe/phrases secrètes sont le seul facteur d'authentification pour l'accès des utilisateurs clients, les mots de passe/phrases secrètes sont modifiés au moins tous les 90 jours, ou la posture de sécurité des comptes est analysée dynamiquement pour déterminer l'accès en temps réel aux ressources.		✓		✓
8.4.2	Authentification à plusieurs facteurs pour tous les accès au CDE.	✓			✓
8.5.1	Les systèmes d'authentification à plusieurs facteurs sont mis en œuvre de manière appropriée.	✓			✓

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
8.6.1	La connexion interactive pour les comptes utilisés par les systèmes ou les applications est gérée de manière appropriée.	✓			✓
8.6.2	Les mots de passe/phrases de passe utilisés pour la connexion interactive pour les comptes des applications et du système sont protégés contre toute utilisation abusive.	✓			✓
8.6.3	Les mots de passe/phrases secrètes pour tous les comptes d'applications et système sont protégés contre toute utilisation abusive.	✓			✓
9.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 9 sont documentés, attribués et compris.	✓		✓	
9.5.1.2.1	Une analyse ciblée des risques est effectuée afin de déterminer la fréquence des analyses périodiques des programmes malveillants.	✓			✓
10.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 10 sont documentés, attribués et compris.	✓		✓	
10.4.1.1	Les examens des journaux d'audit sont automatisées.	✓			✓
10.4.2.1	Une analyse ciblée des risques est effectuée pour déterminer la fréquence des examens des journaux pour tous les autres composants système.	✓			✓
10.7.2	Les défaillances des systèmes de contrôle de sécurité critiques sont détectées, signalées et traitées rapidement.	✓			✓
10.7.3	Les défaillances des systèmes de contrôle de sécurité critique sont traitées rapidement.	✓			✓
11.1.2	Les rôles et les responsabilités pour l'exécution des activités de l'exigence 11 sont documentés, attribués et compris.	✓		✓	
11.3.1.1	Les vulnérabilités applicables non classées haut risque ou critiques sont traitées.	✓			✓

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
11.3.1.2	Les analyses de vulnérabilité internes sont effectuées via une analyse authentifiée.	✓			✓
11.4.7	Les prestataires de services tiers hébergés/cloud assistent leurs clients dans les tests d'intrusion externes.		✓		✓
11.5.1.1	Les canaux de communication masqués des programmes malveillants sont traités via des techniques de détection et/ou de prévention des intrusions.		✓		✓
11.6.1	Un mécanisme de détection des modifications et de falsification est déployé sur les pages de paiement.	✓			✓
12.3.1	Une analyse ciblée des risques est effectuée pour chaque exigence du standard PCI DSS, ce qui offre une flexibilité quant à la fréquence de son exécution.	✓			✓
12.3.2	Une analyse ciblée des risques est effectuée pour chaque exigence du standard PCI DSS qui est satisfaite avec l'approche personnalisée.	✓		✓	
12.3.3	Les suites de chiffrement cryptographique et les protocoles utilisés sont documentés et examinés.	✓			✓
12.3.4	Les technologies matérielles et logicielles sont examinées.	✓			✓
12.5.2	Le périmètre PCI DSS est consigné et confirmé au moins une fois tous les 12 mois.	✓		✓	
12.5.2.1	Le périmètre PCI DSS est documenté et confirmé au moins une fois tous les six mois et lors d'importantes modifications.		✓		✓
12.5.3	L'impact des changements organisationnels importants sur le périmètre PCI DSS est documenté et examiné et les résultats sont communiqués à la direction.		✓		✓
12.6.2	Le programme de sensibilisation à la sécurité est revu au moins une fois tous les 12 mois et mis à jour au besoin.	✓			✓

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
12.6.3.1	La formation de sensibilisation à la sécurité aborde la sensibilisation aux menaces qui pourraient avoir un impact sur la sécurité du CDE, y compris l'hameçonnage et les attaques connexes et l'ingénierie sociale.	✓			✓
12.6.3.2	La formation de sensibilisation à la sécurité comporte la sensibilisation à une utilisation acceptable des technologies de l'utilisateur final.	✓			✓
12.9.2	Les TPSP prennent en charge les demandes des clients de fournir le statut de la conformité au standard PCI DSS et des informations sur les exigences du standard PCI DSS qui relèvent de la responsabilité du TPSP.		✓	✓	
12.10.4.1	Une analyse ciblée des risques est effectuée afin de déterminer la fréquence de la formation périodique du personnel de réponse en cas d'incident.	✓			✓
12.10.5	Le plan de réponse aux incidents de sécurité comprend des alertes du mécanisme de détection de modifications et de falsification des pages de paiement.	✓			✓
12.10.7	Des procédures de réponse en cas d'incident sont en place et lancées dès la détection d'un PAN.	✓			✓
A1.1.1	Le prestataire confirme que l'accès vers et depuis l'environnement du client est logiquement séparé pour empêcher tout accès non autorisé.		✓		✓
A1.1.4	Le prestataire confirme l'efficacité des contrôles de séparation logique utilisés pour séparer les environnements des clients au moins une fois tous les six mois via des tests d'intrusion.		✓		✓
A1.2.3	Le prestataire met en œuvre des processus ou des mécanismes pour signaler et traiter les incidents de sécurité et les vulnérabilités soupçonnés ou confirmés.		✓		✓

Nouvelle Exigence		Applicable à		Date Effective	
		Toutes les Entités	Prestataire de Services Uniquement	Immédiatement Pour Toutes les Évaluations de la v4.0	31 mars 2025
A3.3.1	Les défaillances des éléments suivants sont détectées, alertées et signalées en temps opportun : Les mécanismes automatisés d'examen des Journaux Les outils automatisés d'examen du code.	✓			✓
Totaux :		53	11	13	51
Total Général : 64					