Exigence de la norme PCI DSS v4.0	Appareils autonomes – connexion commutée	Appareils autonomes	Appareils semi-intégrés	Appareils de chiffrement point à point (P2PE)	Plateformes et passerelles de paiement	Solution hébergée pour le titulaire de carte	Solution hébergée pour le commerçant	Appareils intégrés du commerçant
1.1 Les processus et mécanismes d'installation et de maintenance des mesures de sécurité de sécurité du réseau sont définis et compris.								
1.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 1 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 1 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
1.2 Les mesures de sécurité de sécurité réseau (NSC) sont configurés et maintenus.								
1.2.1 Les standards de configuration pour les ensembles de règles NSC sont : • Définies. • Mise en oeuvre. • Maintenues.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.3 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.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.4 Un ou des diagrammes de flux de données précis sont maintenus et répondent aux critères suivants : • Affiche tous les flux de données de carte à travers tous les systèmes et les réseaux. • Mis à jour au besoin lors de modifications apportées à l'environnement.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.5 Tous les services, protocoles et ports autorisés sont identifiés, approuvés et ont un besoin métier défini.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.6 Les fonctionnalités de sécurité sont définies et mises en oeuvre pour tous les services, protocoles et ports utilisés et considérés comme non sécurisés, de sorte que le risque soit atténué.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.7 Les configurations des NSC sont revues au moins une fois tous les six mois pour confirmer qu'elles sont pertinentes et efficaces.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.2.8 Les fichiers de configuration des NSC sont comme suit : • Sécurisés contre les accès non autorisés. • Maintenus cohérents avec les configurations de réseau actives.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.3 L'accès au réseau vers et depuis l'environnement de données du titulaire de carte est restreint.								
1.3.1 Le trafic entrant vers le CDE est limité comme suit : • Seul le trafic qui est nécessaire. • Tout autre trafic est spécifiquement refusé.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
1.3.2 Le trafic sortant du CDE est limité comme suit : • Seul le trafic qui est nécessaire. • Tout autre trafic est spécifiquement refusé.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
1.3.3 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 : • Tout le trafic sans fil allant des réseaux sans fil vers le CDE est refusé par défaut. • Seul le trafic sans fil avec des besoins métier autorisés est autorisé à accéder au CDE.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
1.4 Les connexions réseau entre les réseaux de confiance et les réseaux non fiables sont contrôlées.								
1.4.1 Les NSC sont mis en oeuvre entre les réseaux approuvés et les réseaux non fiables.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.

1.4.2 Le trafic entrant des réseaux non fiables vers les réseaux de confiance est limité : • Aux communications avec des composants systèmes autorisés à fournir des services, des protocoles et des ports accessibles au public. • Aux réponses avec état aux communications initiées par les composants système dans un réseau de confiance. • Tout autre trafic est refusé.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.4.3 Des mesures d'anti usurpation sont mises en oeuvre afin de détecter et empêcher les adresses IP sources falsifiées d'entrer dans le réseau de confiance.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.4.4 Les composants système qui stockent les données des titulaires de cartes ne sont pas directement accessibles à partir de réseaux non fiables.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
1.4.5 La divulgation des adresses IP internes et des informations de routage est limitée aux seules parties autorisées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
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.								
1.5.1 Des mesures de sécurité de sécurité sont mis en oeuvre 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 : • Des paramètres de configuration spécifiques sont définis afin d'empêcher l'introduction de menaces dans le réseau de l'entité. • Les mesures de sécurité de sécurité sont activées et en cours d'exécution. • Les mesures de sécurité 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.	S.O.	S.O.	Commerçant	S.O.	Commerçant	Commerçant	Commerçant	S.O.
2.1 Les processus et mécanismes d'application de configurations sécurisées à tous les composants système sont définis et compris.								
2.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 2 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
2.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 2 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
2.2 Les composants système sont configurés et gérés en toute sécurité.								
2.2.1 Les standards de configuration sont élaborées, mises en oeuvre et maintenues pour : • Couvrir tous les composants système. • Corriger toutes les vulnérabilités de sécurité connues. • Se conformer aux standards relatifs à la sécurité renforcée des systèmes agréés par l'industrie ou aux recommandations pour une sécurité renforcée des fournisseurs. • Se tenir informé des nouvelles vulnérabilités identifiées, comme défini dans l'exigence 6.3.1. • 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
2.2.2 Les comptes par défaut du fournisseur sont gérés comme suit : • 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. • Si le ou les comptes par défaut du fournisseur ne sont pas utilisés, le compte est supprimé ou désactivé.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
2.2.3 Les fonctions principales nécessitant différents niveaux de sécurité sont gérées de la manière suivante : • Une seule fonction principale existe sur un composant système, OU • Les fonctions principales avec des niveaux de sécurité différents qui existent sur le même composant système sont isolées les unes des autres, OU • 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant

2.2.4 Seuls les services, protocoles, démons et fonctions nécessaires sont activés et toutes les fonctionnalités inutiles sont supprimées ou désactivées.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
2.2.5 Si des services, protocoles ou démons non sécurisés sont présents : • La justification métier est documentée. • Des fonctionnalités de sécurité supplémentaires sont documentées et mises en oeuvre afin de réduire le risque d'utilisation de services, de protocoles ou de démons non sécurisés.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
2.2.6 Les paramètres de sécurité du système sont configurés afin d'éviter toute utilisation abusive.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
2.2.7 Tous les accès d'administration non-console sont chiffrés à l'aide d'une cryptographie robuste.	S.O.	Commerçant	Commerçant	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
2.3 Les environnements sans fil sont configurés et gérés en toute sécurité.								
2.3.1 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 : • Clés cryptographiques sans fil par défaut. • Mots de passe par défaut des points d'accès sans fil. • Valeurs SNMP par défaut. • Toute autre valeur par défaut du fournisseur sans fil liée à la sécurité.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	S.O.	Commerçant	Commerçant
2.3.2 Pour les environnements sans fil connectés au CDE ou transmettant des données de carte, les clés cryptographiques sans fil sont modifiées comme suit : • Chaque fois que le personnel connaissant la clé quitte l'entreprise ou le rôle pour lequel la connaissance de la clé était nécessaire. • Chaque fois qu'une clé est soupçonnée ou avérée être compromise.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	S.O.	Commerçant	Commerçant
3.1 Les processus et mécanismes de protection des données de carte stockées sont définis et compris.								
3.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 3 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	Commerçant	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
3.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 3 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
3.2 Le stockage des données de carte est réduit au minimum.								
3.2.1 Le stockage des données de carte est réduit au minimum grâce à la mise en oeuvre de politiques, procédures et processus de conservation et d'élimination des données qui incluent au moins les éléments suivants : • Couverture de tous les emplacements des données de carte stockées. • Couverture de toutes les données d'authentification sensibles (SAD) stockées avant la fin de l'autorisation. 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. • 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. • 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. • 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. • 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.	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	S.O.	Commerçant
3.3 Les données d'authentification sensibles (SAD) ne sont pas stockées après autorisation.								
3.3.1 Les SAD ne sont pas conservées après autorisation, même si elles sont chiffrées. Toutes les données d'authentification sensibles reçues sont rendues irrécupérables à la fin du processus d'autorisation.	Commerçant	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
3.3.1.1 Le contenu complet d'une piste n'est pas conservé à la fin du processus d'autorisation.	Commerçant	Commerçant	Commerçant	S.O.	Commerçant	S.O.	S.O.	S.O.

3.3.1.2 Le code de vérification de la carte n'est pas conservé à la fin du processus d'autorisation.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
3.3.1.3 Le numéro d'identification personnel (PIN) et le bloc PIN ne sont pas conservés à la fin du processus d'autorisation.	Commerçant	Commerçant	Commerçant	S.O.	Commerçant	Commerçant	S.O.	Commerçant
3.3.2 Les SAD qui sont stockées électroniquement avant l'achèvement de l'autorisation sont chiffrées à l'aide d'une cryptographie robuste.	Moneris	Moneris	Moneris	S.O.	Commerçant	S.O.	S.O.	Commerçant
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 : Tout stockage de données d'authentification sensibles est : • Limité à ce qui est nécessaire pour un besoin métier d'émission légitime, et est sécurisé. • 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.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
3.4 L'accès à l'affichage du PAN complet et la possibilité de copier les données des titulaires de cartes sont limités.								
3.4.1 Le PAN est masqué lorsqu'il est affiché (le BIN et les quatre derniers chiffres sont le nombre maximum de chiffres à afficher), de sorte que seul le personnel ayant un besoin métier légitime peut voir plus que le BIN et les quatre derniers chiffres du PAN.	Commerçant	Commerçant	Commerçant	S.O.	Commerçant	S.O.	Commerçant	Commerçant
3.4.2 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	S.O.
3.5 Le numéro de compte primaire (PAN) est sécurisé partout où il est stocké.								
3.5.1 Le PAN est rendu illisible partout où il est stocké en utilisant l'une des approches suivantes : • Hachage à sens unique basé sur une cryptographie robuste de l'intégralité du PAN. • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN). – 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. • Token d'index. • Cryptographie robuste avec processus et procédures de gestion des clés associés.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
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.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
3.5.1.2 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 oeuvre uniquement de la manière suivante : • Sur des supports électroniques amovibles OU • 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
3.5.1.3 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 : • L'accès logique est géré séparément et indépendamment de l'authentification du système d'exploitation natif et des mécanismes de contrôle d'accès. • Les clés cryptographiques ne sont pas associées aux comptes utilisateur. • 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
3.6 Les clés cryptographiques utilisées pour protéger les données de carte stockées sont sécurisées.								

3.6.1 Des procédures sont définies et mises en oeuvre afin de protéger les clés cryptographiques utilisées pour protéger les données de carte stockées contre la divulgation et l'utilisation abusive, notamment : • L'accès aux clés est limité au plus petit nombre d'opérateurs nécessaire. • Les clés de chiffrement des clés sont au moins aussi robustes que les clés de chiffrement des données qu'elles protègent. • Les clés de chiffrement des clés sont stockées séparément des clés de chiffrement de données. • Les clés sont stockées en toute sécurité dans le moins d'emplacements et de formes possibles.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
3.6.1.1 Exigences supplémentaires pour les prestataires de services uniquement : Une description documentée de l'architecture cryptographique est maintenue, et qui comprend : • 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. • 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. • Une description de l'utilisation des clés pour chaque clé. • 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, comme indiqué dans l'exigence 12.3.4.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	Commerçant
3.6.1.2 Les clés secrètes et privées utilisées pour chiffrer/déchiffrer les données de carte stockées sont conservées sous l'une (ou plusieurs) des formes suivantes à tout moment : • 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. • Dans un dispositif cryptographique sécurisé (SCD), tel qu'un module de sécurité matérielle (HSM) ou un dispositif de point d'interaction approuvé PTS. • 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	S.O.	S.O.	Commerçant
3.6.1.3 L'accès aux composants de clé cryptographique en texte clair est limité au plus petit nombre d'opérateurs nécessaire.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.6.1.4 Les clés cryptographiques sont stockées dans le moins d'emplacements possibles.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
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 oeuvre.								
3.7.1 Des politiques et procédures de gestion des clés sont mises en oeuvre pour inclure la génération de clés cryptographiques robustes utilisées pour protéger les données de carte stockées.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.2 Des politiques et procédures de gestion des clés sont mises en oeuvre pour inclure la distribution de clés cryptographiques utilisées pour protéger les données de carte stockées.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.3 Des politiques et procédures de gestion des clés sont mises en oeuvre pour inclure le stockage de clés cryptographiques utilisées pour protéger les données de carte stockées.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.4 Les politiques et procédures de gestion des clés sont mises en oeuvre 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 : • Une cryptopériode définie pour chaque type de clé utilisé. • Un processus pour les changements de clé à la fin de la cryptopériode définie.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.5 Les procédures et politiques de gestion des clés sont mises en oeuvre pour inclure le retrait, le remplacement ou la destruction des clés utilisées pour protéger les données de carte stockées, comme jugé nécessaire lorsque : • La clé a atteint la fin de sa cryptopériode définie. • 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. • La clé est suspectée ou avérée être compromise. Les clés retirées ou remplacées ne sont pas utilisées pour les opérations de chiffrement.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.6 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 oeuvre, notamment la gestion de ces opérations à l'aide du fractionnement des connaissances et du double contrôle.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant

3.7.7 Des politiques et procédures de gestion des clés sont mises en oeuvre pour inclure la prévention de la substitution non autorisée de clés cryptographiques.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.8 Des politiques et procédures de gestion des clés sont mises en oeuvre 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.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
3.7.9 Exigences supplémentaires pour les prestataires de services uniquement : 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.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
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 documentés.								
4.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 4 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
4.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 4 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
4.2 Le PAN est protégé par une cryptographie robuste pendant la transmission.								
4.2.1 Des protocoles de chiffrement et de sécurité robustes sont mis en oeuvre comme suit afin de protéger le PAN pendant la transmission sur des réseaux publics ouverts : • Seuls les clés et certificats de confiance sont acceptés. • 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. 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. • 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 oeuvre non sécurisés. • La robustesse du chiffrement est adéquate pour la méthodologie de chiffrement utilisée.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Moneris	Commerçant
4.2.1.1 Un inventaire des clés et des certificats approuvés par l'entité utilisés pour protéger le PAN pendant la transmission, est maintenu.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	S.O.	Commerçant
4.2.1.2 Les réseaux sans fil transmettant le PAN ou connectés au CDE utilisent les meilleures pratiques de l'industrie pour mettre en oeuvre une cryptographie robuste pour l'authentification et la transmission.	S.O.	Commerçant	Moneris	Moneris	Commerçant	S.O.	Commerçant	Commerçant
4.2.2 Le PAN est sécurisé avec une cryptographie robuste chaque fois qu'il est envoyé via les technologies de messagerie des utilisateurs finaux.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
5.1 Les processus et mécanismes de protection de tous les systèmes et réseaux contre les logiciels malveillants sont définis et compris.								
5.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 5 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
5.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 5 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
5.2 Les logiciels malveillants (malware) sont empêchés ou détectés et traités.								
5.2.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.

5.2.2 La ou les solutions anti-programmes malveillants déployées : • Détecte tous les types connus de logiciels malveillants. • Supprime, bloque ou contient tous les types connus de logiciels malveillants.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.2.3 Tous les composants système qui ne présentent pas de risque de logiciels malveillants sont évalués périodiquement pour inclure les éléments suivants : • Une liste documentée de tous les composants système ne présentant pas de risque de logiciels malveillants. • Identification et évaluation des menaces de logiciels malveillants en évolution pour ces composants système. • Confirmation indiquant si ces composants système continuent de ne pas nécessiter de protection anti-programmes malveillants.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
5.2.3.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
5.3 Les mécanismes et processus anti-programmes malveillants sont actifs, maintenus et surveillés.								
5.3.1 La ou les solutions anti-programmes malveillants sont tenues à jour via des mises à jour automatiques.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.3.2 La ou les solutions anti-programmes malveillants : • Effectue des analyses périodiques et des analyses actives ou en temps réel, OU • Effectue une analyse comportementale continue des systèmes ou des processus.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.3.2.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
5.3.3 Pour les supports électroniques amovibles, la solution anti-programmes malveillants : • Effectue des analyses automatiques lorsque le support est inséré, connecté ou monté logiquement, OU • Effectue une analyse comportementale continue des systèmes ou des processus lorsque le support est inséré, connecté ou monté logiquement.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.3.4 Les journaux d'audit pour la solution anti-programmes malveillants sont activés et conservés conformément à l'exigence 10.5.1.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.3.5 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
5.4 Les mécanismes anti-hameçonnage protègent les utilisateurs contre les attaques par hameçonnage.								
5.4.1 Des processus et des mécanismes automatisés sont en place pour détecter et protéger le personnel contre les attaques d'hameçonnage.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
6.1 Les processus et mécanismes de développement et de maintenance de systèmes et de logiciels sécurisés sont définis et compris.								
6.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 6 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
6.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 6 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
6.2 Des logiciels sur mesure et personnalisés sont développés de manière sécurisée.								

6.2.1 Les logiciels sur mesure et personnalisés sont développés de manière sécurisée comme suit : • Sur la base des normes et standards de l'industrie et/ou des meilleures pratiques pour un développement sécurisé. • Conformément au standard PCI DSS (par exemple, authentification et journalisation sécurisées). • Intégration de la prise en compte des problèmes de sécurité de l'information à chaque étape	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
6.2.2 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 : • Sur la sécurité des logiciels en rapport avec leur fonction et leurs langages de développement. • Inclure la conception de logiciels sécurisés et les techniques de codage sécurisé. • Inclure, si des outils de test de sécurité sont utilisés, la manière d'utiliser les outils pour détecter les vulnérabilités dans les logiciels.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
6.2.3 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 : • Les examens de code garantissent que le code est développé conformément aux directives de codage sécurisé. • Les examens de code recherchent les vulnérabilités logicielles existantes et émergentes. • Des corrections appropriées sont mises en oeuvre avant la publication.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	S.O.
6.2.3.1 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 : • 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. • Examinées et approuvées par la direction avant la publication.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
6.2.4 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 : • Attaques par injection, y compris SQL, LDAP, XPath ou d'autres failles de type commande, paramètre, objet, erreur ou injection. • 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. • 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. • 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). • 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 oeuvre de ces mécanismes.	Moneris	Moneris	Moneris	Moneris	Commerçant	Commerçant	Commerçant	Commerçant
6.3 Les vulnérabilités de sécurité sont identifiées et corrigées.								
6.3.1 Les vulnérabilités de sécurité sont identifiées et gérées de la manière suivante : • 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). • 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. • Les classements des risques identifient, au minimum, toutes les vulnérabilités considérées comme à haut risque ou critiques pour l'environnement. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
6.3.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.

6.3.3 Tous les composants système sont protégés contre les vulnérabilités connues en installant les correctifs/mises à jour de sécurité applicables comme suit : • Les correctifs/mises à jour critiques ou de haute sécurité (identifiés selon le processus de classement des risques énoncé à l'exigence 6.3.1) sont installés dans le mois suivant leur publication. • Tous les autres correctifs/mises à jour de sécurité applicables sont installés dans un délai approprié déterminé par l'entité (par exemple, dans les trois mois suivant leur publication).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
6.4 Les applications Web destinées au public sont protégées contre les attaques.								
6.4.1 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 : • 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 : – Au moins une fois tous les 12 mois et après des modifications importantes. – Par une entité spécialisée dans la sécurité des applications. – Y compris, au minimum, toutes les attaques logicielles courantes énoncées dans l'exigence 6.2.4. – Toutes les vulnérabilités sont classées conformément à l'exigence 6..3.1. – Toutes les vulnérabilités sont corrigées. – L'application est réévaluée après les corrections OU • L'installation d'une ou plusieurs solutions techniques automatisées qui détectent et empêchent en permanence les attaques basées sur le Web, comme suit : – Installé devant les applications Web destinées au public afin de détecter et empêcher les attaques Web. - En exécution active et à jour, le cas échéant. – Génération de journaux d'audit. – Configuré pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
6.4.2 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 : • Est installée devant les applications Web destinées au public et configurée afin de détecter et empêcher les attaques Web. • En exécution active et à jour, le cas échéant. • Génération de journaux d'audit. • Configurée pour bloquer les attaques Web ou générer une alerte qui est immédiatement examinée.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
6.4.3 Tous les scripts de la page de paiement qui sont chargés et exécutés dans le navigateur du consommateur sont gérés comme suit : • Une méthode est mise en oeuvre pour confirmer que chaque script est autorisé. • Une méthode est mise en oeuvre pour assurer l'intégrité de chaque script. • Un inventaire de tous les scripts est maintenu avec une justification écrite expliquant pourquoi chacun est nécessaire.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
6.5 Les modifications apportées à tous les composants système sont gérées de manière sécurisée.								
6.5.1 Les modifications apportées à tous les composants système dans l'environnement de production sont effectuées conformément aux procédures établies qui comportent : • Raison et description du changement. • Documentation de l'impact sur la sécurité. • Approbation des changements documentée par les parties autorisées. • Tests pour vérifier que le changement n'a pas d'incidence négative sur la sécurité du système. • 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. • Procédures pour la résolution des échecs et le retour à un état sécurisé.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
6.5.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant

6.5.3 Les environnements de pré-production sont séparés des environnements de production et la séparation est appliquée avec des mesures de sécurité d'accès.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
6.5.4 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
6.5.5 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
6.5.6 Les données de test et les comptes de test sont supprimés des composants système avant que le système ne passe en production.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
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.								
7.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 7 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 7 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.2 L'accès aux composants système et aux données du système est défini et attribué de manière adéquate.								
7.2.1 Un modèle de contrôle d'accès est défini et inclut l'octroi d'accès comme suit : • Accès approprié en fonction de l'activité de l'entité et des besoins d'accès. • Accès aux composants système et aux ressources de données en fonction de la classification et des fonctions des utilisateurs. • Les moindres privilèges requis (par exemple, utilisateur, administrateur) pour exécuter une fonction.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.2.2 L'accès est attribué aux utilisateurs, y compris les utilisateurs privilégiés, selon : • La classification du poste et de la fonction. • Les moindres privilèges nécessaires pour exercer les responsabilités de la tâche.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
7.2.3 Les privilèges requis sont approuvés par un personnel autorisé.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
7.2.4 Tous les comptes et les privilèges d'accès associés, y compris les comptes tiers/fournisseurs, sont examinés comme suit : • Au moins une fois tous les six mois. • Pour garantir que les comptes d'utilisateurs et l'accès restent appropriés selon la fonction du poste. • Tout accès inapproprié est traité. • La direction reconnaît que l'accès demeure approprié.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
7.2.5 Tous les comptes d'applications et système et les privilèges d'accès associés sont attribués et gérés comme suit : • Basé sur les moindres privilèges nécessaires à l'opérabilité du système ou de l'application. • L'accès est limité aux systèmes, applications ou processus qui nécessitent spécifiquement leur utilisation.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
7.2.5.1 Tous les accès par comptes d'applications et système et les privilèges d'accès associés sont examinés comme suit : • 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). • L'accès à l'application ou au système reste approprié pour la fonction exécutée. • Tout accès inapproprié est traité. • La direction reconnaît que l'accès demeure approprié.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

7.2.6 Tout accès utilisateur pour envoyer aux référentiels des requêtes de données de titulaires de cartes stockées est limité comme suit : • Via des applications ou d'autres méthodes programmatiques, avec accès et actions autorisées en fonction des rôles d'utilisateur et des moindres privilèges. • Seuls les administrateurs responsables peuvent accéder directement ou envoyer des requêtes aux référentiels de CHD stockés.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.3 L'accès aux composants et aux données système est géré via un ou plusieurs systèmes de contrôle d'accès.								
7.3.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.3.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
7.3.3 Le ou les systèmes de contrôle d'accès sont définis par défaut pour « refuser tout le monde ».	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
8.1 Les processus et mécanismes d'identification des utilisateurs et d'authentification des accès aux composants système sont définis et compris.								
8.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 8 sont : • Documentées • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	S.O.
8.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 8 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
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.								
8.2.1 Tous les utilisateurs reçoivent un identifiant unique avant d'être autorisé à accéder aux composants système ou aux données des titulaires de cartes.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.2.2 Les comptes 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 : • L'utilisation du compte est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles. • L'utilisation est limitée au temps nécessaire à la circonstance exceptionnelle. • La justification métier de l'utilisation est documentée. • L'utilisation est explicitement approuvée par la direction. • L'identité de l'utilisateur est confirmée avant que l'accès au compte ne soit accordé. • Chaque action effectuée est attribuable à un utilisateur.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.2.3 Exigences supplémentaires pour les prestataires de services uniquement : Les prestataires de services accédant à distance à l'environnement des clients utilisent des facteurs d'authentification différents pour chaque consommateur.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
8.2.4 L'ajout, la suppression et la modification des identifiants utilisateur, des facteurs d'authentification et d'autres objets identifiants sont gérés comme suit : • Autorisés avec l'approbation appropriée. • Mis en oeuvre avec uniquement les privilèges spécifiés sur l'approbation documentée.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.2.5 L'accès des utilisateurs dont le contrat a été résilié est immédiatement révoqué.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.2.6 Les comptes utilisateur inactifs depuis 90 jours sont supprimés ou désactivés.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.2.7 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 : • Activés uniquement pendant la période d'intervention et désactivés en dehors de la période. • L'utilisation est surveillée pour détecter toute activité inhabituelle.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.2.8 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant

8.3 L'authentification forte des utilisateurs et des administrateurs est implémentée et gérée.								
8.3.1 Tous les accès utilisateur et administrateurs aux composants système sont authentifiés via au moins l'un des facteurs d'authentification suivants : • Quelque chose que vous connaissez, comme un mot de passe ou une phrase secrète. • Quelque chose que vous possédez, comme un jeton d'authentification ou une carte à puce. • Quelque chose que vous êtes, comme un élément biométrique.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.3.2 Une cryptographie robuste est utilisée pour rendre tous les facteurs d'authentification illisibles pendant la transmission et le stockage sur tous les composants système.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant
8.3.3 L'identité de l'utilisateur est vérifiée avant de modifier tout facteur d'authentification.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.3.4 Les tentatives d'authentification infructueuses sont limitées par : • Le verrouillage de l'identifiant utilisateur après 10 tentatives échouées maximum. • Le réglage de la durée de verrouillage à 30 minutes minimum ou jusqu'à la confirmation de l'identité de l'utilisateur.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant
8.3.5 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 : • Définis sur une valeur unique pour chaque première utilisation et lors de la réinitialisation. • Doivent être modifiés immédiatement après la première utilisation.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant
8.3.6 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 : • Une longueur minimale de 12 caractères (ou 8 caractères si le système ne prend pas en charge les 12 caractères). • Contenir à la fois des caractères numériques et alphabétiques.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.3.7 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/phrase secrètes utilisés.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant
8.3.8 Les politiques et procédures d'authentification sont documentées et communiquées à tous les utilisateurs, notamment : • Des conseils sur le choix de facteurs d'authentification robustes. • Des conseils sur la façon dont les utilisateurs doivent protéger leurs facteurs d'authentification. • Des instructions pour ne pas réutiliser les mots de passe/phrases secrètes précédemment utilisés. • 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	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.3.9 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 : • Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours, OU • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Moneris	Commerçant
8.3.10 Exigences supplémentaires pour les prestataires de services uniquement : 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 oeuvre d'authentification à facteur unique), des conseils sont fournis aux utilisateurs clients, notamment : • Des conseils aux clients pour modifier périodiquement leurs mots de passe/phrases secrète d'utilisateur. • Des conseils sur quand et dans quelles circonstances les mots de passe/phrases secrètes sont modifiés.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	Commerçant
8.3.10.1 Exigences supplémentaires pour les prestataires de services uniquement : 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 oeuvre d'authentification à un seul facteur), alors soit : • Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours, OU • La posture de sécurité des comptes est analysée de manière dynamique et l'accès en temps réel aux ressources est automatiquement déterminé en conséquence.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	Commerçant

8.3.11 Lorsque des facteurs d'authentification tels que des tokens physiques ou logiques, des cartes à point ou des certificats sont utilisés : • Les facteurs sont attribués à un utilisateur individuel et ne sont pas partagés entre plusieurs utilisateurs. • Les mesures physiques et/ou logiques garantissent que seul l'utilisateur prévu peut utiliser ce facteur pour obtenir l'accès	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.4 L'authentification multifacteur (MFA) est mise en oeuvre pour sécuriser l'accès au CDE.								
8.4.1 Le MFA est mis en oeuvre pour tous les accès non-console dans le CDE pour le personnel avec des accès d'administration.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
8.4.2 L'authentification MFA est mise en oeuvre pour tous les accès au CDE.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.4.3 L'authentification MFA est mise en oeuvre pour tous les accès réseau distants provenant de l'extérieur du réseau de l'entité qui pourraient accéder ou avoir une incidence sur le CDE comme suit : • Tous les accès à distance par tout le personnel, utilisateurs et administrateurs, provenant de l'extérieur du réseau de l'entité. • Tous les accès à distance par des tiers et des fournisseurs.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.5 Les systèmes d'authentification multifacteurs (MFA) sont configurés de sorte à ne pas pouvoir être contournés.								
8.5.1 Les systèmes MFA sont mis en oeuvre comme suit : • Le système MFA n'est pas sensible aux attaques par rejeu. • 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. • Au moins deux types différents de facteurs d'authentification sont utilisés. • La réussite de tous les facteurs d'authentification est obligatoire avant que l'accès ne soit accordé.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.6 Les comptes applicatifs, les comptes systèmes et les facteurs d'authentification associés est gérés rigoureusement.								
8.6.1 Si les comptes utilisés par les systèmes ou les applications peuvent être utilisés pour la connexion interactive, ils sont gérés comme suit : • L'utilisation interactive est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles. • L'utilisation interactive est limitée au temps nécessaire à la circonstance exceptionnelle. • La justification métier de l'utilisation interactive est documentée. • L'utilisation interactive est explicitement approuvée par la direction. • L'identité de l'utilisateur individuel est confirmée avant que l'accès au compte ne soit accordé. • Chaque action entreprise est attribuable à un utilisateur individuel.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.6.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
8.6.3 Les mots de passe/phrases secrètes pour tous les comptes applicatifs et système sont protégés contre les abus comme suit : • 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. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
9.1 Les processus et mécanismes de restriction de l'accès physique aux données des titulaires de cartes sont définis et compris.								
9.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 9 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	Commerçant	Commerçant
9.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 9 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

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.								
9.2.1 Des mesures de sécurité d'accès aux installations appropriés sont en place pour limiter l'accès physique aux systèmes du CDE.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.2.1.1 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 : • Les points d'entrée et de sortie des zones sensibles du CDE sont surveillés. • Les dispositifs ou mécanismes de surveillance sont protégés contre l'altération ou la désactivation. • Les données recueillies sont examinées et corrélées avec d'autres entrées. • Les données recueillies sont conservées pendant au moins trois mois, sauf restriction légale contraire.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
9.2.2 Des mesures de sécurité physiques et/ou logiques sont mis en oeuvre pour limiter l'utilisation des prises réseaux accessibles au public au sein de l'installation.	S.O.	Commerçant	Commerçant	S.O.	Commerçant	S.O.	S.O.	Commerçant
9.2.3 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.2.4 L'accès aux consoles dans les zones sensibles est limité par un système de verrouillage lorsqu'elles ne sont pas utilisées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.3 L'accès physique du personnel et des visiteurs est autorisé et géré.								
9.3.1 Des procédures sont mises en oeuvre pour autoriser et gérer l'accès physique du personnel au CDE, notamment : • Identification du personnel. • L'exigence de gérer les modifications d'accès physique d'une personne. • Révoquer ou mettre fin à l'identification du personnel. • Limiter l'accès au processus ou au système d'identification au personnel autorisé.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.3.1.1 L'accès physique aux zones sensibles au sein du CDE pour le personnel est contrôlé comme suit : • L'accès est autorisé et basé sur la fonction individuelle du poste. • L'accès est révoqué immédiatement après la résiliation du contrat de travail. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.3.2 Des procédures sont mises en oeuvre afin d'autoriser et gérer l'accès des visiteurs au CDE, notamment : • Les visiteurs sont autorisés avant d'entrer. • Les visiteurs sont escortés en tout temps. • Les visiteurs sont clairement identifiés et reçoivent un badge ou autre moyen les identifiants, ayant un délai d'expiration. • Les badges de visiteur ou autre moyen d'identification distinguent visiblement les visiteurs du personnel.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.3.3 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.3.4 Un journal des visiteurs est utilisé pour conserver un enregistrement physique de l'activité des visiteurs au sein de l'installation et dans les zones sensibles, y compris : • Le nom du visiteur et l'organisation représentée. • La date et l'heure de la visite. • Le nom du personnel autorisant l'accès physique. • Conserver le journal pendant au moins trois mois, sauf restriction légale contraire.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.4 Les supports contenant les données des titulaires de carte sont stockés, consultés, distribués et détruits de manière sécurisée.								
9.4.1 Tous les supports contenants les données des titulaires de cartes sont physiquement sécurisés.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.1.1 Les sauvegardes hors ligne des supports contenants les données des titulaires de cartes sont stockées dans un emplacement sécurisé.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.1.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant

9.4.2 Tous les supports contenant des données de titulaires de cartes sont classés en fonction de la sensibilité des données.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.3 Les supports avec les données des titulaires de cartes envoyées à l'extérieur de l'installation sont sécurisés comme suit : • Les supports envoyés à l'extérieur de l'installation sont documentés. • Les supports sont envoyés par courrier sécurisé ou par un autre mode de livraison pouvant être suivi avec précision. • La documentation de suivi des supports hors site inclue des détails sur l'emplacement des supports.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.4 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).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.5 Un inventaire de tous les supports électroniques contenant les données des titulaires de cartes est conservé.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
9.4.5.1 Les inventaires des supports électroniques avec les données des titulaires de cartes sont réalisés au moins une fois tous les 12 mois.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
9.4.6 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 : • Les matériaux sont déchiquetés, incinérés ou réduits en pâte afin que les données des titulaires de cartes ne puissent pas être reconstituées. • Les documents sont stockés dans des conteneurs de stockage sécurisés avant destruction.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
9.4.7 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 : • Les supports électroniques sont détruits. • Les données des titulaires de cartes sont rendues irrécupérables de sorte qu'elles ne peuvent pas être reconstituées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
9.5 Les dispositifs de point d'interaction (POI) sont protégés contre l'altération et la substitution non autorisée.								
9.5.1 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 : • Maintenir une liste des périphériques POI. • Inspecter périodiquement les appareils POI pour rechercher des altérations ou des substitutions non autorisées. • Former le personnel à être conscient des comportements suspects et à signaler toute altération ou substitution non autorisée d'appareils.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	S.O.	Commerçant
9.5.1.1 Une liste à jour des appareils POI est maintenue, y compris : • La marque et le modèle de l'appareil. • L'emplacement de l'appareil. • Numéro de série de l'appareil ou autres méthodes d'identification uniques.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	S.O.	Commerçant
9.5.1.2 Les surfaces des appareils POI sont inspectées périodiquement afin de détecter les altérations et les substitutions non autorisées.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	S.O.	Commerçant
9.5.1.2.1 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.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	S.O.	S.O.
9.5.1.3 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 : • 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. • Des procédures pour garantir que les appareils ne sont pas installés, remplacés ou retournés sans vérification. • Être conscient des comportements suspects entourant les appareils. • Signaler les comportements suspects et les indications d'altération ou de substitution de l'appareil au personnel approprié.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	S.O.	Commerçant
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 documentés.								

10.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 10 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
10.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 10 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
10.2 Les journaux d'audit sont mis en oeuvre pour prendre en charge la détection des anomalies et des activités suspectes, ainsi que l'analyse criminelle des événements.								
10.2.1 Les journaux d'audit sont activés et actifs pour tous les composants système et les données des titulaires de cartes.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
10.2.1.1 Les journaux d'audit capturent tous les accès des utilisateurs individuels aux données des titulaires de cartes.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
10.2.1.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.2.1.3 Les journaux d'audit capturent tous les accès aux journaux d'audit.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
10.2.1.4 Les journaux d'audit capturent toutes les tentatives d'accès logique non valides.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.2.1.5 Les journaux d'audit capturent toutes les modifications apportées à l'identification et aux identifiants d'authentification, y compris, sans toutefois s'y limiter : • La création de nouveaux comptes. • L'élévation des privilèges. • Toutes les modifications, ajouts ou suppressions de comptes avec accès administrateur.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.2.1.6 Les journaux d'audit capturent les éléments suivants : • Toutes les initialisations des nouveaux journaux d'audit, et • Tous les démarrages, arrêts ou pauses des journaux d'audit existants.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
10.2.1.7 Les journaux d'audit capturent toutes les créations et suppressions d'objets au niveau du système.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
10.2.2 Les journaux d'audit enregistrent les détails suivants pour chaque événement auditable : • Identification de l'utilisateur. • Type d'événement. • Date et heure. • Indication de réussite et d'échec. • Origine de l'événement. • Identité ou nom des données, composant système, ressource ou service touchés (par exemple, nom et protocole).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.3 Les journaux d'audit sont protégés contre la destruction et les modifications non autorisées.								
10.3.1 L'accès en lecture aux fichiers journaux d'audit est limité aux personnes ayant un besoin lié à leur poste.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.3.2 Les fichiers journaux d'audit sont protégés pour empêcher les modifications par des personnes.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.3.3 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.3.4 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.4 Les journaux d'audit sont examinés pour identifier les anomalies ou les activités suspectes.								

10.4.1 Les journaux d'audit suivants sont examinés au moins une fois par jour : • Tous les événements de sécurité. • Les journaux de tous les composants système qui stockent, traitent ou transmettent des CHD et/ou des SAD. • Les journaux de tous les composants système critiques. • 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).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.4.1.1 Des mécanismes automatisés sont utilisés pour effectuer des examens des journaux d'audit.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.4.2 Les journaux de tous les autres composants système (ceux non spécifiés dans l'exigence 10.4.1) sont examinés périodiquement.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.4.2.1 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	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.4.3 Les exceptions et anomalies identifiées au cours du processus d'examen sont traitées.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.5 L'historique des journaux d'audit est conservé et disponible pour analyse.								
10.5.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.6 Les mécanismes de synchronisation temporelle prennent en charge des paramètres de temps cohérents sur tous les systèmes.								
10.6.1 Les horloges système et l'heure sont synchronisées à l'aide de la technologie de synchronisation date/heure.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.6.2 Les systèmes sont configurés pour l'heure correcte et cohérente comme suit : • Un ou plusieurs serveurs de temps désignés utilisés. • Seul le ou seuls les serveurs de temps centraux désignés reçoit l'heure de sources externes. • L'heure reçue de sources externes est basée sur le temps atomique international ou le temps universel coordonné (UTC). • 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. • 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. • Les systèmes internes ne reçoivent des informations de date/heure que du ou des serveurs de temps centraux désignés.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.6.3 Les paramètres et les données de synchronisation date/heure sont protégés comme suit : • L'accès aux données date/heure est limité au personnel ayant un besoin professionnel. • Toute modification des paramètres horaires sur les systèmes critiques est enregistrée, surveillée et examinée.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
10.7 Les défaillances des systèmes de contrôle de sécurité critiques sont détectées, signalées et traitées rapidement.								
10.7.1 Exigences supplémentaires pour les prestataires de services uniquement : Les défaillances des systèmes de contrôle de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances des systèmes de contrôle de sécurité critiques suivants : • Les mesures de sécurité réseau • IDS/IPS • FIM • Les solutions anti-programmes malveillants • Les mesures d'accès physiques • Les mesures d'accès logiques • Les mécanismes de journalisation des audits • Les mesures de segmentation (le cas échéant)	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.

10.7.2 Les défaillances des systèmes de contrôle de sécurité critiques sont détectées, signalées et traitées rapidement, y compris, sans toutefois s'y limiter, les défaillances des systèmes de contrôle de sécurité critiques suivants : • Les mesures de sécurité réseau • IDS/IPS • Les mécanismes de détection des modifications • Les solutions anti-programmes malveillants • Les mesures d'accès physiques • Les mesures d'accès logiques • Les mécanismes de journalisation des audits • Les mesures de segmentation (le cas échéant) • Les mécanismes d'examen des Journaux d'audit • Des outils automatisés de test de la sécurité (le cas échéant)	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
10.7.3 Les défaillances de tout système de contrôle de sécurité critique sont traitées rapidement, y compris, sans toutefois s'y limiter : • Restauration des fonctions de sécurité. • Identifier et documenter la durée (date et heure du début à la fin) de la défaillance de sécurité. • Identifier et documenter la ou les causes de la défaillance et documenter les mesures correctives nécessaires. • Identifier et résoudre tous les problèmes de sécurité survenus lors de la défaillance. • Déterminer si d'autres mesures est nécessaires à la suite de la défaillance de sécurité. • Mettre en oeuvre des mesures afin d'éviter que la cause de la défaillance ne se reproduise. • Reprendre la surveillance des mesures de sécurité.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
11.1 Les processus et mécanismes pour tester régulièrement la sécurité des systèmes et des réseaux sont définis et compris.								
11.1.1 Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 11 sont : • Documentées. • Tenues à jour. • Utilisées. • Connues de toutes les parties concernées.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
11.1.2 Les rôles et les responsabilités liées aux activités de l'exigence 11 sont documentés, attribués et compris.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
11.2 Les points d'accès sans fil sont identifiés et surveillés, et les points d'accès sans fil non autorisés sont traités.								
11.2.1 Les points d'accès sans fil autorisés et non autorisés sont gérés de la manière suivante : • La présence de points d'accès sans fil (Wi-Fi) est testée, • Tous les points d'accès sans fil autorisés et non autorisés sont détectés et identifiés, • Les tests, la détection et l'identification sont effectués au moins une fois tous les trois mois. • Si une surveillance automatisée est utilisée, le personnel doit être averti via la génération d'alertes.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
11.2.2 Un inventaire des points d'accès sans fil autorisés est conservé, y compris une justification métier documentée.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
11.3 Les vulnérabilités externes et internes sont régulièrement identifiées, priorisées et traitées.								
11.3.1 Les scans de vulnérabilités internes sont effectuées comme suit : • Au moins une fois tous les trois mois. • Les vulnérabilités à haut risque et critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues. • Des rescans sont effectués pour confirmer que toutes les vulnérabilités à haut risque et critiques, comme indiqué ci-dessus, ont été résolues. • L'outil de scan est tenu à jour avec les dernières informations sur les vulnérabilités. • Les scans sont effectués par du personnel qualifié et l'indépendance organisationnelle du testeur existe.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
11.3.1.1 Toutes les autres vulnérabilités applicables (celles qui ne sont pas classées comme à haut risque ou critiques (selon les classements de risque de vulnérabilité de l'entité définis à l'exigence 6.3.1) sont gérées comme suit : • 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. • Des scans de vérification sont effectués si besoin.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

11.3.1.2 Les scans de vulnérabilité internes sont effectués via un scan authentifié comme suit : • Les systèmes qui ne peuvent pas accepter les « credentials » pour le scan authentifié sont documentés. • Des privilèges suffisants sont utilisés pour les systèmes qui acceptent les « credentials » pour le scan. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
11.3.1.3 Les scans de vulnérabilités internes sont effectués après toute modification importante comme suit : • Les vulnérabilités à haut risque et critiques (selon les classements de risque des vulnérabilités de l'entité définis à l'exigence 6.3.1) sont résolues. • Des scans de vérification sont effectués au besoin. • 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).	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
11.3.2 Les scans de vulnérabilités externes sont effectués comme suit : • Au moins une fois tous les trois mois. • Par un fournisseur de scan de vulnérabilités agréé PCI SSC (ASV). • Les vulnérabilités sont résolues et les exigences du guide du programme de l'ASV pour un scan réussi sont respectées. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
11.3.2.1 Les scans de vulnérabilités externes sont effectués après toute modification importante comme suit : • Les vulnérabilités trouvées avec un CVSS égal à 4.0 ou plus sont résolues. • Des scans de vérification sont effectués si besoin. • 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).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
11.4 Des tests d'intrusion externes et internes sont effectués régulièrement, et les vulnérabilités exploitables et les faiblesses de sécurité sont corrigées.								
11.4.1 Une méthodologie de test d'intrusion est définie, documentée et mise en oeuvre par l'entité, et comprend : • Des approches de test d'intrusion acceptées par l'industrie. • Une couverture de l'ensemble du périmètre du CDE et des systèmes critiques. • Des tests à la fois à l'intérieur et à l'extérieur du réseau. • Des tests pour valider les mesures de segmentation et de réduction du périmètre. • Des tests d'intrusion de la couche application pour identifier, au minimum, les vulnérabilités répertoriées dans l'exigence 6.2.4. • 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. • L'examen et la prise en compte des menaces et des vulnérabilités rencontrées au cours des 12 derniers mois. • 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 conservation des résultats des tests d'intrusion et des activités de correction pendant au moins 12 mois.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
11.4.2 Un test d'intrusion interne est effectué : • Selon la méthodologie définie par l'entité, • Au moins une fois tous les 12 mois. • Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application • Par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
11.4.3 Un test d'intrusion externe est effectué : • Selon la méthodologie définie par l'entité • Au moins une fois tous les 12 mois. • Après toute mise à niveau ou modification importante d'une infrastructure ou d'une application • Par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.

11.4.4 Les vulnérabilités exploitables et les faiblesses de sécurité détectées lors des tests d'intrusion sont corrigées comme suit : • Conformément à l'évaluation par l'entité du risque posé par le problème de sécurité tel que défini dans l'exigence 6.3.1. • Les tests d'intrusion sont répétés pour vérifier les corrections.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
11.4.5 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 : • Au moins une fois tous les 12 mois et après toute modification des mesures ou méthodes de segmentation • Couvrir toutes les mesures ou méthodes de segmentation utilisée. • Conformément à la méthodologie des tests d'intrusion définie par l'entité. • Confirmer que les mesures ou méthodes de segmentation sont opérationnels et efficaces, et isolent le CDE de tous les systèmes hors du périmètre. • 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). • Effectués par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
11.4.6 Exigences supplémentaires pour les prestataires de services uniquement : 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 : • Au moins une fois tous les six mois et après toute modification des mesures de sécurité ou méthodes de segmentation • Couvrir tous les mesures ou méthodes de segmentation utilisée. • Conformément à la méthodologie des tests d'intrusion définie par l'entité. • Confirmer que les mesures ou méthodes de segmentation sont opérationnelles et efficaces, et isolent le CDE de tous les systèmes hors du périmètre. • 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). • Effectués par une ressource interne qualifiée ou un tiers externe qualifié • L'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
11.4.7 Exigence supplémentaire pour les prestataires de services mutualisés uniquement : Les prestataires de services mutualisés assistent leurs clients dans les tests d'intrusion externes conformément aux exigences 11.4.3 et 11.4.4.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
11.5 Les intrusions réseau et les modifications imprévues de fichiers sont détectées et traitées.								
11.5.1 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 : • Tout le trafic est surveillé à la périphérie du CDE. • Tout le trafic est surveillé aux points critiques du CDE. • Le personnel est alerté des suspicions de compromissions. • Tous les moteurs de détection et de prévention des intrusions, les lignes de base et les signatures sont tenus à jour.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
11.5.1.1 Exigences supplémentaires pour les prestataires de services uniquement : Les techniques de détection et/ou de prévention des intrusions détectent, alertent/préviennent et traitent les canaux secrets de communication des logiciels malveillants.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
11.5.2 Un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) est déployé de la façon suivante : • Pour alerter le personnel de modifications non autorisées (y compris les modifications, les ajouts et les suppressions) de fichiers critiques • Pour effectuer des comparaisons de fichiers critiques au moins une fois par semaine.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
11.6 Les modifications non autorisées sur les pages de paiement sont détectées et traitées.								

11.6.1 Un mécanisme de détection des changements et des altérations est déployé de la manière suivante : • Alerter le personnel des modifications non autorisées (y compris les indicateurs de compromission, de changements, d'ajouts et de suppressions) des en-têtes HTTP et du contenu des pages de paiement comme reçus par le navigateur du consommateur. • Le mécanisme est configuré pour évaluer l'en-tête HTTP et la page de paiement reçus. • Les fonctions des mécanismes sont exécutées comme suit : – Au moins une fois tous les sept jours OU – 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).	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
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.								
12.1.1 Une politique globale de sécurité de l'information est : • Établie. • Publiée. • Maintenue. • Diffusée à tout le personnel concerné, ainsi qu'aux fournisseurs et partenaires commerciaux concernés.	Commerçant	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
12.1.2 La politique de sécurité de l'information est : • Examinée au moins une fois tous les 12 mois. • Mise à jour, si besoin, pour refléter les modifications apportées aux objectifs professionnels ou les risques pour l'environnement.	Commerçant	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
12.1.3 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.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	S.O.	Commerçant
12.1.4 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
12.2 Des politiques d'utilisation acceptable des technologies de l'utilisateur final sont définies et mises en oeuvre.								
12.2.1 Des politiques d'utilisation acceptable pour les technologies d'utilisateur final sont documentées et mises en oeuvre, notamment : • Une approbation expresse par les parties autorisées. • Des utilisations acceptables de la technologie. • Une liste de produits approuvés par l'entreprise pour une utilisation par les employés, y compris le matériel et les logiciels.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	Commerçant
12.3 Les risques pour l'environnement des données des titulaires de cartes sont formellement identifiés, évalués et gérés.								
12.3.1 Chaque exigence du standard PCI DSS qui offre une flexibilité quant à la fréquence d'exécution (par exemple, les exigences à exécuter périodiquement) est soutenue par une analyse de risque ciblée qui est documentée et comprend : • L'identification des actifs à protéger. • L'identification de la ou des menaces contre lesquelles l'exigence protège. • L'identification des facteurs qui contribuent à la probabilité et/ou à l'impact d'une menace. • L'analyse résultante qui détermine et inclut la justification de la fréquence à laquelle l'exigence doit être exécutée afin de minimiser la probabilité que la menace se matérialise. • 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. • La réalisation d'analyses de risques mises à jour au besoin, tel que déterminé par l'examen annuel.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

12.3.2 Une analyse de risque ciblée est effectuée pour chaque exigence du standard PCI DSS que l'entité satisfait à l'approche personnalisée, pour inclure : • 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). • Une approbation des preuves documentées par la haute direction. • Une réalisation de l'analyse de risque ciblée au moins une fois tous les 12 mois.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.3.3 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 : • Un inventaire tenu à jour de toutes les suites et protocoles de chiffrement cryptographiques utilisés, y compris le but et le lieu d'utilisation. • Une surveillance active des tendances de l'industrie concernant la viabilité continue de toutes les suites et protocoles de chiffrement cryptographiques utilisés. • Une stratégie documentée pour répondre aux changements anticipés des vulnérabilités cryptographiques.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	S.O.
12.3.4 Les technologies matérielles et logicielles utilisées sont examinées au moins une fois tous les 12 mois, en incluant au moins les éléments suivants : • Une analyse démontrant que les technologies continuent de recevoir rapidement des correctifs de sécurité des fournisseurs. • Une analyse démontrant que les technologies continuent de prendre en charge (et n'empêchent pas) la conformité au standard PCI DSS de l'entité. • 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. • 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 ».	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.4 La conformité au standard PCI DSS est gérée.								
12.4.1 Exigences supplémentaires pour les prestataires de services uniquement : 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 : • Responsabilité globale pour le maintien de la conformité PCI DSS. • Définition d'une charte pour un programme de conformité PCI DSS et sa communication à la direction générale.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.4.2 Exigences supplémentaires pour les prestataires de services uniquement : 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 : • Examens quotidiens des journaux. • Examens des configurations pour les mesures de sécurité réseau. • Application des standards de configuration aux nouveaux systèmes. • Réponse aux alertes de sécurité. • Processus de gestion des changements.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.4.2.1 Exigences supplémentaires pour les prestataires de services uniquement : Les revues effectuées conformément à l'exigence 12.4.2 sont documentées pour inclure : • Les résultats des revues. • La documentation des mesures correctives prises pour toutes les tâches qui se sont avérées non exécutées à l'exigence 12.4.2. • Revue et approbation des résultats par le personnel affecté à la responsabilité du programme de conformité PCI DSS.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.5 La périmètre du standard PCI DSS est documentée et validée.								
12.5.1 Un inventaire des composants système qui sont dans le périmètre PCI DSS, incluant une description de la fonction ou de l'utilisation, est maintenu et tenu à jour.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

12.5.2 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 : • L'identification tous les flux de données pour les différentes étapes de paiement (par exemple, l'autorisation, la capture des règlements, les rétrofacturations et les remboursements) et les canaux d'acceptation (par exemple, la carte présente, la carte non présente et le commerce électronique). • La mise à jour tous les diagrammes de flux de données conformément à l'exigence 1.2.4. • 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. • L'identification de tous les composants système dans le CDE, connectés au CDE, ou qui pourraient avoir une incidence sur la sécurité du CDE. • 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. • L'identification de toutes les connexions d'entités tierces ayant accès au CDE. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.5.2.1 Exigences supplémentaires pour les prestataires de services uniquement : 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.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.5.3 Exigences supplémentaires pour les prestataires de services uniquement : 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.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.6 La sensibilisation à la sécurité est une activité continue.								
12.6.1 Un programme formel de sensibilisation à la sécurité est mis en oeuvre 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.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.6.2 Le programme de sensibilisation à la sécurité est : • Revu au moins une fois tous les 12 mois. • Mis à jour si nécessaire pour prendre en compte toute nouvelle menace et vulnérabilité susceptible d'avoir une incidence sur la sécurité du CDE de l'entité, ou les informations fournies au personnel concernant son rôle dans la protection des données des porteurs de cartes.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.6.3 Le personnel reçoit une formation de sensibilisation à la sécurité comme suit : • À l'embauche et au moins une fois tous les 12 mois. • Plusieurs méthodes de communication sont utilisées. • Le personnel confirme au moins une fois tous les 12 mois avoir lu et compris la politique et les procédures de sécurité des informations.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.6.3.1 La formation de sensibilisation à la sécurité comprend la sensibilisation aux menaces et aux vulnérabilités qui pourraient avoir un impact sur la sécurité du CDE, y compris, sans toutefois s'y limiter : • L'hameçonnage et attaques associées. • L'ingénierie sociale.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	Commerçant	Commerçant
12.6.3.2 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.7 Le personnel est contrôlé afin de réduire les risques d'attaques internes								
12.7.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.8 Le risque pour les fonds documentaires associés aux relations avec les prestataires de services tiers (TPSP) est géré.								

12.8.1 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.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.8.2 Les accords écrits avec les TPSP sont maintenus comme suit : • Des accords écrits sont maintenus avec tous les TPSP avec lesquels les données de carte sont partagées ou qui pourraient avoir une incidence la sécurité du CDE. • Les accords écrits comprennent des reconnaissances des TPSP qu'ils 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 ils pourraient avoir un impact sur la sécurité du CDE de l'entité.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.8.3 Un processus établi est mis en oeuvre pour engager les TPSP, y compris des mesures de sécurité préalables appropriés avant l'engagement	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.8.4 Un programme est mis en oeuvre pour surveiller l'état de conformité au standard PCI DSS des TPSP au moins une fois tous les 12 mois.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.8.5 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.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.9 Les prestataires de services tiers (TPSP) prennent en charge la conformité du standard PCI DSS de leurs clients.								
12.9.1 Exigences supplémentaires pour les prestataires de services uniquement : Les TPSP confirment par écrit aux clients qu'ils 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 ils pourraient avoir un impact sur la sécurité du CDE du consommateur.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.9.2 Exigences supplémentaires pour les prestataires de services uniquement : 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 : • Des informations sur l'état de conformité au standard PCI DSS pour tout service que le TPSP effectue pour le compte des clients (exigence 12.8.4). • 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).	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
12.10 Les incidents de sécurité soupçonnés et confirmés qui pourraient avoir un impact sur le CDE sont traités immédiatement								
12.10.1 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 : • 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. • Les procédures de réponse aux incidents avec des activités de confinement et d'atténuation spécifiques pour différents types d'incidents. • Les procédures de reprise et de continuité de l'activité. • Les processus de sauvegarde des données. • L'analyse des exigences légales en matière de signalement des compromissions. • La couverture et les réponses de tous les composants critiques du système. • La référence ou l'inclusion des procédures de réponse aux incidents des marques de carte paiement.	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant	Commerçant
12.10.2 Au moins une fois tous les 12 mois, le plan de réponse aux incidents de sécurité est : • Revu et le contenu est mis à jour si besoin. • Testé, en incluant tous les éléments énumérés à l'exigence 12.10.1.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.10.3 Du personnel spécifique est désigné pour être disponible 24h/24 et 7j/7 pour répondre aux incidents de sécurité soupçonnés ou avérés.	S.O.	S.O.	S.O.	S.O.	Commerçant	Commerçant	S.O.	Commerçant
12.10.4 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.10.4.1 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.

12.10.5 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 : • Systèmes de détection et de prévention des intrusions. • Mécanismes de sécurité réseau. • Mécanismes de détection des modifications pour les fichiers critiques. • Mécanisme de détection des modifications et des altérations pour les pages de paiement. 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. • Détection des points d'accès sans fil non autorisés.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.10.6 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
12.10.7 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 : • 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. • Identifier si des données d'authentification sensibles sont stockées avec les PAN. • Déterminer d'où proviennent les données de carte et comment elles se sont retrouvées là où elles n'étaient pas prévues. • 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.	S.O.	S.O.	S.O.	S.O.	Commerçant	S.O.	S.O.	S.O.
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.								
A2.1.1 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.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
A2.1.2 Exigence supplémentaire pour les prestataires de services uniquement : 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 : • 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. • Résultats de l'évaluation des risques et mesures de réduction des risques en place. • Description des processus pour surveiller les nouvelles vulnérabilités associées à SSL et les versions obsolètes de TLS. • Description des processus de gestion des changements qui sont mis en oeuvre pour garantir que le protocole SSL et les versions obsolètes de TLS ne sont pas mis en oeuvre dans de nouveaux environnements. • Aperçu du plan de projet de migration pour remplacer SSL et les versions obsolètes de TLS à une date ultérieure.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
A2.1.3 Exigence supplémentaire pour les prestataires de services uniquement : Tous les prestataires de services proposent une offre de services sécurisée.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.