Information security

AVIS D'EXPERT

IT Maker provadys

# Le contrôle permanent PCI DSS : objectifs et opportunités

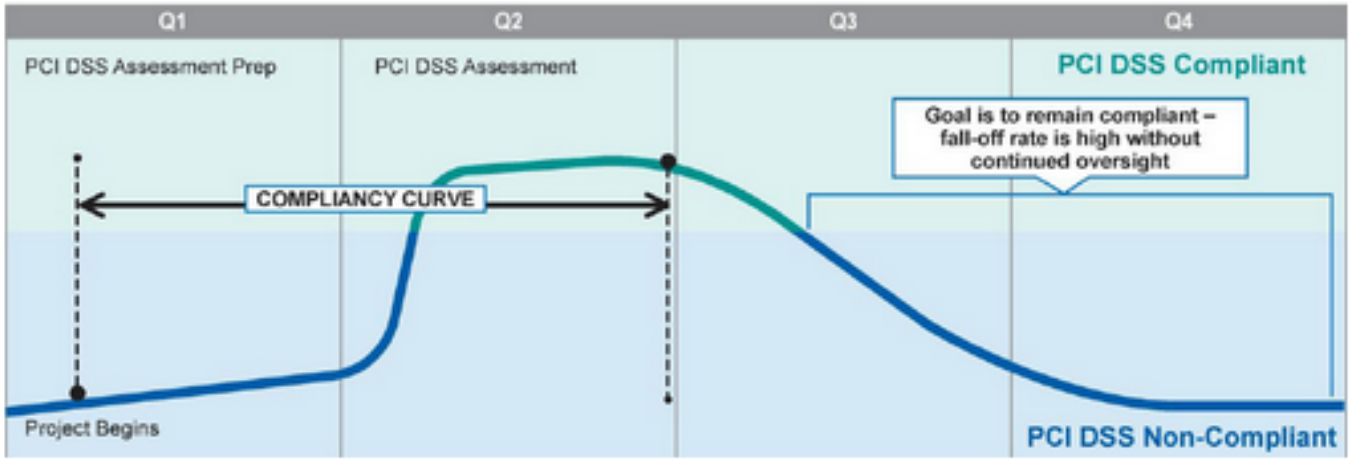
par Aurelien Barraud, Project Expert Information Security Nantes
et l'équipe Provadys Information Security

La dernière version 3.2 du standard PCI DSS publiée en Avril 2016 a introduit de nouvelles exigences dont la 12.11 et la 12.11.1, obligatoires depuis le 1er Février 2018 pour les fournisseurs de services, mais demeurant une bonne pratique pour toutes les autres entités :

*12.11 Exigence supplémentaire pour les prestataires de services uniquement : Effectuer des revues au moins une fois par trimestre pour confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles. Les examens doivent couvrir les processus suivants :*
*• Examens quotidiens des journaux*
*• Examens des règles de pares-feux*
*• Application des normes de configuration aux nouveaux systèmes*
*• Réponse aux alertes de sécurité*
*• Processus de gestion du changement*

*12.11.1 Exigence supplémentaire pour les prestataires de services uniquement : La gestion de la documentation du processus de revue trimestrielle comprend ce qui suit :*
*• Documentation des résultats des revues*
*• Revue de ces résultats et signature de ces résultats par le personnel responsable du programme de conformité au standard PCI DSS*

**Quels sont les objectifs de ces 2 nouvelles exigences ?**
Un des dangers qui guette la plupart des organisations engagées dans un projet de certification PCI DSS est de relâcher ses efforts après le passage de l'auditeur et l'obtention de l'attestation de conformité.

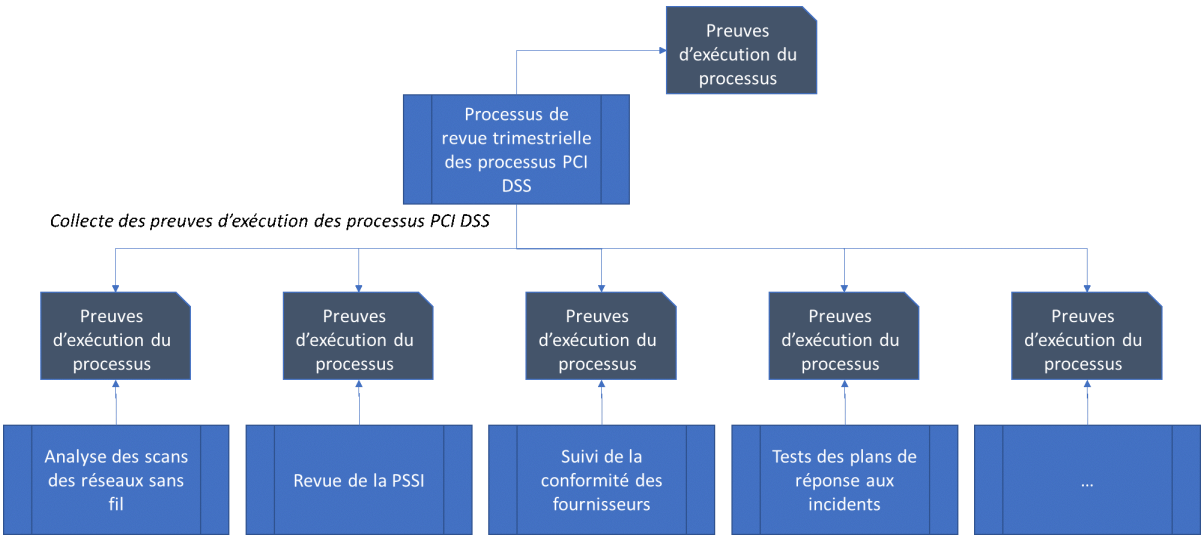


Ce risque majeur pourrait non seulement mettre en péril le maintien de la conformité et le renouvellement annuel de la certification, mais surtout exposer l'organisation à la survenue d'un évènement affectant les données de cartes bancaires (CB). Pour s'en prémunir, ces nouvelles mesures sont là pour s'assurer de manière régulière et durable que les processus de sécurité PCI DSS concourant à protéger ces données sensibles fonctionnent correctement.

A cette fin, les fournisseurs de services doivent désormais effectuer une revue trimestrielle afin de s'assurer que le personnel impliqué dans le périmètre PCI DSS suit bien les politiques et les procédures opérationnelles PCI DSS en vigueur.
Ces mesures conduisent à veiller à ce que les activités périodiques réclamées par PCI DSS (exemple : application des patchs critiques de sécurité sous un délai d'un mois, revue quotidienne des logs sur les composants critiques…) soient effectuées tout au long de l'année. Ces activités périodiques ont pour objectif la détection rapide de défaillances dans les processus et de corriger au plus tôt ce qui pourrait se traduire en non-conformité PCI DSS ou pire, en une compromission des données CB !

## Ce que ces mesures ne sont pas

Ces mesures ne visent aucunement à mettre en œuvre les procédures de test correspondant à l'ensemble des exigences PCI DSS visées dans le périmètre de la revue, comme le fait l'auditeur annuellement. Mais, elles visent à s'assurer que les exigences PCI DSS et les processus qui les portent produisent bien une ou plusieurs preuves démontrant qu'ils sont correctement exécutés. A charge de chaque responsable de processus PCI DSS de mettre à disposition les preuves en ligne avec les procédures de test correspondant aux exigences que ces processus surveillés doivent respecter.
Par exemple, concernant le processus de patching sécurité (exigence 6.2), le processus de revue trimestrielle pourra demander la liste des patchs de sécurité installés sur les composants du périmètre précisant la criticité de ces derniers et la date de déploiement pour vérifier que les patchs de sécurité sont installés dans les délais définis dans les procédures.



## Une opportunité pour faciliter sa mise en conformité

**Si le premier processus PCI DSS que vous mettriez en place était ce « méta processus » de revue trimestrielle…**

• Quels seraient alors les processus PCI DSS nécessaires à surveiller pour répondre aux exigences PCI DSS ?

• Quelles preuves devraient alors être générées et mises à disposition par ces différents processus pour se conformer à ces exigences ?

En imaginant un pilotage de votre projet de mise en conformité suivant ce processus de revue trimestrielle, ne disposez-vous pas d'une nouvelle approche représentant une opportunité pour construire de manière plus efficace et accélérée votre conformité ?

En mettant en place un dispositif de contrôle/suivi de la conformité sur l'environnement, PCI DSS pousse les organisations à penser en termes de processus et non plus uniquement en termes d'exigences. Cette approche est toujours plus fiable quand on cherche à sécuriser le Système d'Information, et d'autant plus pertinente dans un contexte où les processus de sécurité inhérents à PCI DSS peuvent se retrouver dans d'autres référentiels de sécurité (exemple : ISO 27001:2013, ISAE 3402) ou réglementaires (exemple : Règlement Européen sur la protection des données, etc.).

## Quelle organisation mettre en place ?

Provadys conseille fortement de rattacher ce processus de revue trimestrielle à un groupe de personnes ou à un service de l'entreprise indépendant des opérationnels portant les processus de sécurité PCI DSS à surveiller. Il peut par ailleurs être judicieux que cette cellule bénéficie de l'alimentation des éléments produits par le contrôle interne / contrôle permanent de l'entreprise lorsque ce dernier existe, ou soit directement rattachée à ce dernier.

Par ailleurs, les personnes ayant la responsabilité de cette revue trimestrielle auront de facto une vision globale des risques pesant sur la conformité PCI DSS de l'ensemble des processus du périmètre soumis à la certification et seront les plus à même de remonter un statut de la conformité au Management exécutif de l'entreprise, comme le réclame la nouvelle exigence 12.4.1 :

*12.4.1 Exigence supplémentaire pour les prestataires de services uniquement : L'équipe de direction a défini la responsabilité relative à la protection des données de titulaires de carte et un programme de conformité à la norme PCI DSS, comme suit :*

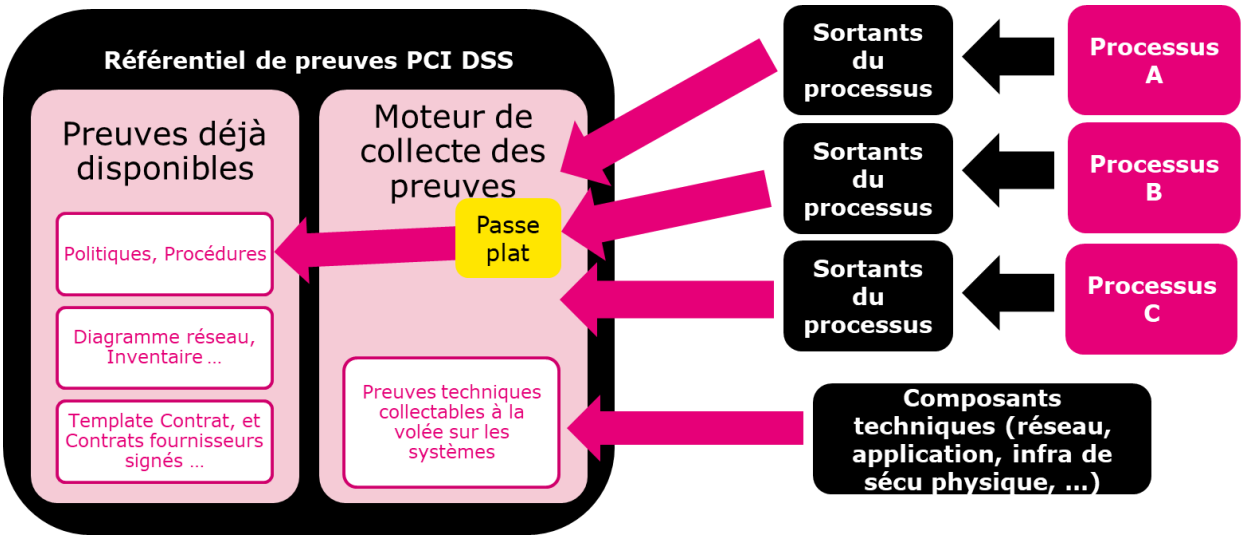
*• Responsabilité globale pour respecter la conformité à la norme PCI DSS*

*• Définition d'une charte pour un programme de conformité à la norme PCI DSS* ***et des canaux de communication avec la direction***

## Repenser la mise à disposition des preuves

La vérification régulière de la conformité par les organisations elles-mêmes peut représenter un surcoût non négligeable dans la vie d'un périmètre certifié PCI DSS. Afin d'optimiser ces coûts, Provadys conseille d'**automatiser et centraliser la collecte des preuves.**

Concrètement, il s'agira à ce stade, en tant que responsable de processus PCI DSS, de ne pas attendre la sollicitation du dispositif en charge de la revue trimestrielle pour produire les éléments de preuves de conformité, mais d'anticiper la production de ces preuves au plus tôt. Il s'agira donc en amont de mettre en place un dispositif permettant de générer et de mettre à disposition de manière rapide ces mêmes preuves.
Par ailleurs, l'auditeur PCI DSS verra généralement d'un très bon œil une organisation ayant l'idée de mettre en place ce type d'automatisation. En effet, au-delà de surveiller de manière plus fiable toute dérive dans les processus de sécurité PCI DSS, c'est l'exercice d'audit PCI DSS qui sera facilité non seulement pour l'auditeur, mais également pour l'audité via la réduction du temps nécessaire à répondre aux nombreuses sollicitations de l'auditeur PCI DSS.




## Une organisation pouvant être simplifiée dans les petites structures / entreprises

Concernant la revue elle-même, il peut être particulièrement intéressant pour les petites structures ne disposant pas des ressources humaines disponibles, d'externaliser ce service de revue trimestrielle auprès d'une société de prestation externe spécialisée sur PCI DSS ou en sécurité des systèmes d'information.

## Quelles preuves pour démontrer que le processus de revue trimestriel est conforme ?

Les preuves attendues par l'auditeur QSA sont les suivantes :

- Politique de réalisation de revue trimestrielle confirmant que les politiques et procédures de sécurité PCI DSS sont respectées
- Procédure décrivant la manière dont sont réalisées les revues trimestrielles confirmant que les politiques et procédures de sécurité PCI DSS sont respectées
- Entretiens pour identifier comment et à quelle fréquence sont réalisées les revues trimestrielles confirmant que les procédures de sécurité sont respectées
- Enregistrements démontrant que les revues de respect des politiques et procédures de sécurité PCI DSS sont bien réalisées tous les 3 mois au minimum
- Résultats des revues trimestrielles signées par le personnel responsable du programme de conformité PCI DSS

## Quels sont les processus à vérifier dans cette revue trimestrielle ?

Les processus PCI DSS explicitement cités par le standard comme devant **intégrer le périmètre** de la revue trimestrielle :

• Revue des règles des pares-feux
• Application de normes de configuration aux nouveaux systèmes
• Gestion des changements (vérifier qu'une analyse d'impacts, validation, ... a bien eu lieu pour les changements du mois)
• Revue des logs
• Formation des personnes en charge de réponse aux incidents
• Tests des plans de réponse aux incidents

## Les processus PCI DSS additionnels qui peuvent selon Provadys être intégrés dans le périmètre de la revue trimestrielle :

• Recherche de PAN
• Revue de l'analyse de risques liés aux contrôle compensatoire et à l'utilisation de SSL/TLS
• Suppression des données CB qui ont dépassé les volumes de rétention
• Veille sécurité périodique
• Mise à jour des serveurs
• Renouvellement des mots de passe (si réalisé manuellement)
• Désactivation des comptes inactifs (si réalisée manuellement)
• Revue des données issues de la vidéo surveillance en DC
• Revue de l'inventaire des médias, revue de la sécurité des coffres-forts
• Analyse des scans des réseaux sans fil
• Analyse des scans de vulnérabilités internes et externes
• Tests d'intrusion internes et externes, tests de segmentation
• Revue de la PSSI
• Revue de l'analyse de risques
• Sensibilisation du personnel, Approbation des politiques de sécurité
• Suivi de la conformité des fournisseurs
• Formation des développeurs

## Mieux se préparer aux évolutions du standard

Les mesures relatives à la revue trimestrielle des processus s'inscrivent plus généralement dans l'approche poussée par PCI SSC consistant à intégrer le suivi de la conformité en tant que **pratique habituelle** (« Business As Usual ») des organisations. Elles sont directement inspirées de l'exigence A3.3.3 de l'annexe A3 (composée de 20 exigences) dédiée aux « entités désignées », c'est-à-dire faisant l'objet d'une surveillance accrue de la part des marques de cartes bancaires et/ou des acquéreurs du fait d'un volume important de données cartes bancaires, ou ayant subi des fuites importantes ou répétées de données cartes bancaires.

*• A3.1 Implémenter un programme de conformité à la norme PCI DSS (4 exigences)*
*• A3.2 Documenter et valider le champ d'application de la norme PCI DSS (10 exigences)*
*• A3.3 Confirmer que la norme PCI DSS est incorporée dans les activités courantes (BAU) (4 exigences)*
*• A3.4 Contrôler et gérer l'accès logique à l'environnement des données de titulaires de carte (1 exigence).*
*• A3.5 Identifier et résoudre les événements suspects (1 exigence)*

Le standard précise en page 14 **que toutes les organisations doivent envisager l'implémentation de ces meilleures pratiques dans leur environnement, même lorsqu'elles ne sont pas tenues de les auditer lors de leur certification.**

**Il est fort probable de voir apparaitre dans une évolution future du standard PCI DSS :**

• **Un renforcement du champ d'application des mesures additionnelles déjà présentes dans le standard PCI DSS v3.2** (par exemple une extension de l'application de l'exigence 12.11 / 12.11.1 aux entités marchandes, et plus seulement aux fournisseurs de services)
• **Un ajout de mesures complémentaires héritées de cette annexe A3**, qui passeraient ainsi du statut de « bonnes pratiques » au statut d' « exigences obligatoires » pour les entités soumises à PCI DSS, même si elles ne sont pas spécifiquement « désignées », car ces mesures sont pour la plupart des mesures de bon sens. A titre d'exemple, voici les exigences A3.3.2 et A3.4.1 ne faisant pas encore partie du corps du standard :

*A3.3.2 Examiner les technologies matérielles et logicielles au moins une fois par an pour confirmer qu'elles continuent de respecter les conditions du standard PCI DSS au sein de l'organisation. (Par exemple, un examen des technologies qui ne sont plus prises en charge par le fournisseur et/ou qui ne répondent plus aux besoins de sécurité de l'organisation.)*
*Ce processus suppose un plan pour gérer les technologies qui ne remplissent plus les conditions de la norme PCI DSS dans l'organisation. Ce plan peut inclure, mais sans s'y limiter, le remplacement des technologies, le cas échéant.*

*A3.4.1 Examiner les comptes d'utilisateur et les privilèges d'accès aux composants de système concernés au moins une fois par semestre pour confirmer qu'ils sont encore adaptés à la fonction et autorisés comme il se doit.*

**Provadys conseille d'intégrer ces bonnes pratiques au plus tôt dans votre organisation PCI DSS afin de renforcer la sécurité des données cartes bancaires, d'asseoir votre capacité à maintenir la conformité PCI DSS dans le temps, et de minimiser les impacts des probables évolutions du standard PCI DSS.**

## Provadys vous accompagne sur PCI DSS

Provadys est une société de conseil spécialiste des technologies de l'information.
Nous accompagnons les organisations en matière de Transformation du Système d'Information, Big Data, Infrastructure & Cloud et Cybersécurité. Nous mettons nos savoir-faire à leur service pour traiter les défis liés aux mutations des modèles et technologies informatiques.
Provadys est certifié en tant que « QSA Company », ce qui lui permet de se positionner en tant qu'entité habilitée à réaliser les audits de certification PCI DSS. Les consultants experts de Provadys vous apportent également tout leur retour d'expérience pour vous accompagner dans votre projet de mise en conformité, que ce soit sur PCI DSS ou sur d'autres référentiels de sécurité (ISO 27001, ARJEL, LPM, GDPR, ISAE …).
Provadys rayonne partout en France, possède des bureaux à Paris, Sophia-Antipolis et Nantes et compte plus de 500 clients.

## Contacts

**Paris** : +33 (0)1 46 99 93 80
**Sophia-Antopolis :** +33 (0)4 28 27 03 16
**Nantes :** +33 (0)2 55 59 01 10