**LES DOSSIERS TECHNIQUES**

# Démarche d'un projet PCI DSS

Août 2013

**CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS**

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

# Table des matières

# Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

| | | |
|---|---|---|
| Rodolphe | **SIMONETTI** | *Verizon* |

Les contributeurs :

| | | |
|---|---|---|
| Gregory | **ABISROR** | Protiviti |
| Laurent | **ALEXANDRE** | Conforama |
| Thierry | **AUTRET** | GIE CB |
| Michel | **BANGUERSKI** | Verizon |
| Sylvain | **CONCHON** | Conix |
| Vincent | **DI GIAMBATISTA** | ST€T |
| Mathieu | **GARIN** | Solucom |
| Jean-Marc | **GREMY** | Cabestan Consultants |
| Grégoire | **GUETIN** | Elitt |
| Gabriel | **LEPERLIER** | Verizon |
| Yann | **PIEDERRIERE** | Provadys |
| Hervé | **SCHAUER** | HSC |
| François | **ZAMORA** | Orange |

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

# Introduction

La démarche de mise en conformité PCI DSS est un projet à part entière avec ses différentes étapes, acteurs, enjeux, difficultés et opportunités.

Grâce à la collaboration d'un panel de personnes intervenant sur ce type de projet, que cela soit en tant que consultant, auditeur de conformité, partie prenante ou responsable du projet en entreprise, nous aborderons les notions structurantes, les étapes clés, et les démarches complémentaires facilitant la bonne réussite de ce type de projet.

Ainsi, l'étude approfondie de la notion de périmètre permettra d'identifier les processus métiers et les moyens techniques impliqués dans la mise en conformité, qu'ils soient internes ou réalisés avec des prestataires ou des fournisseurs externes. Des méthodes et actions permettant de réduire de manière structurante ce périmètre seront détaillées, ce qui pourra simplifier la mise en conformité, voire s'affranchir de certains efforts.

De même, les différentes étapes organisant le projet seront appréhendées avec les facteurs clés de réussite rencontrés ce qui pourra vous aider dans votre cheminement vers la conformité.

Enfin, nous évoquerons des démarches complémentaires, comme par exemple l'analyse de risque, les tests d'intrusion ou de vulnérabilités qui sont nécessaires pour mener à bien la mise en conformité.

Bonne lecture et bon courage dans votre projet !

# I. Projet d'entreprise : au-delà de l'IT

## *I.1. La conformité / un vrai projet d'entreprise*

### I.1.1. La conformité PCI DSS, un projet

La mise en conformité PCI DSS peut être considérée comme un programme plus qu'un projet en raison de son caractère transverse. En effet, elle aborde des aspects juridiques, contractuels, métiers, organisationnels et techniques. Ce caractère multiple doit être clairement partagé lors de la phase d'initialisation.

### I.1.2. L'impact financier et sa justification

Le ROI en tant que tel est difficile à évaluer sauf dans le cas où le développement commercial requiert une mise en conformité. Cependant, dans tous les cas cet investissement doit être considéré comme une assurance vis-à-vis de certains risques et donc les coûts liés à la conformité peuvent être mis en perspective des coûts que pourraient engendrer ces risques : perte d'exploitation, fraude, perte d'image, procès, coût de réémission de cartes, etc...

### I.1.3. La réduction du périmètre : les processus avant tout!

La réduction du périmètre, telle que nous l'avons traitée au chapitre II, est un élément clé et la première étape de tout projet PCI DSS. Il est généralement tentant de directement se pencher sur les données, les systèmes et l'architecture. Néanmoins, l'expérience montre que de nombreux points d'achoppement lors des projets PCI DSS proviennent de l'incapacité à traiter des points techniques et organisationnels qui sont liés au métier. Si ces points sont identifiés en cours de projet, le chemin critique est touché, et le projet pourra soit souffrir de décalages, soit nécessiter des efforts significatifs incluant des coûts et des charges de travail additionnels. Ceci pourrait aboutir à une décrédibilisation de la démarche et à une perte de confiance des parties prenantes dans celle-ci. Deuxièmement, la non prise en compte des processus métiers dans la phase initiale de dimensionnement du projet pourrait induire l'inclusion d'un périmètre de travail trop large, et donc de coûts significatifs pour le projet.

La bonne démarche consiste donc à réaliser une cartographie fonctionnelle des processus métiers utilisant des données cartes, et d'identifier, pour chaque sous-processus ou tâche, si les données cartes sont réellement nécessaires pour la conduite du processus. Cette démarche permet d'inclure dans le projet, au plus tôt, les responsables des différents processus, et de mettre les enjeux en perspective du standard.

Nous attirons néanmoins l'attention sur le fait que la seule prise en compte des processus métiers, de par la nature des travaux de cartographie sous-jacents (entretiens et revues de documentation principalement) ne permet pas d'avoir une vue exhaustive de l'utilisation et du stockage de données cartes. Ces travaux doivent donc être complétés par des travaux informatisés de recherche de données cartes sur l'ensemble des systèmes des départements susceptibles d'avoir ces données. Cette recherche inclut bien évidemment les postes de travail et donc les applications de type "*end-user computing*" et les fichiers bureautiques.

### I.1.4. Les enjeux du projet :

Les projets PCI DSS ne sont pas des projets purement techniques et de sécurité informatique. Comme nous venons de le voir, ces projets ont des composantes multiples, s'articulant autour de trois grands enjeux :

- Le métier
- L'organisation
- Les systèmes et la technique

Le métier aura un impact significatif sur la démarche à suivre et les solutions à adopter en cours de projet, et rendra donc chaque projet PCI DSS unique. Les contraintes seront forcément différentes entre un *tour operator*, un vendeur à distance par Internet ou une société de concession autoroutière. Par exemple, il est fréquent de noter que certains services fonctionnent en identifiant les individus par leur PAN, alors que finalement, cette donnée n'est pas nécessaire à l'exercice de leur fonction.

L'organisation est également un enjeu important de chaque projet de conformité PCI DSS. En effet, de nombreuses exigences du standard PCI DSS nécessitent, en complément d'équipements, de procédures et de technologies, la mise en œuvre de processus et d'organisations permettant de gérer efficacement la sécurité. Ces processus peuvent nécessiter des ajustements de l'organisation des équipes informatiques impliquées dans la gestion de la sécurité informatique et l'administration des systèmes, mais également de l'organisation au niveau des métiers.

Bien entendu, les systèmes d'informations, les applications mises en œuvre, les équipements réseaux sont le dernier enjeu majeur de la conformité. L'infrastructure et les applications existantes auront un impact sur le périmètre, mais également sur les solutions techniques autorisées par certaines exigences du standard ; Par exemple, l'utilisation de systèmes de type Mainframe implique des limitations techniques qui pourront être contournées par l'ajout de technologies ou la mise en œuvre de contrôles compensatoires. En fonction de la maturité de la société, l'adoption de certaines technologies sera nécessaire pour être conforme aux différentes exigences.

## *I.2. Les facteurs clés de succès du projet*

### I.2.1. Le "sponsoring"

De par la multiplicité des domaines à aborder lors d'un programme de mise en conformité, un sponsoring adapté est un facteur de succès. Ce rattachement projet doit avoir une légitimité reconnue de tous et pouvoir interagir de manière transverse au sein de l'entreprise. Ainsi il dépendra du type d'entreprise et des enjeux liés à la mise en conformité : obligation contractuelle, levier de développement métier, aspects financiers, et pourra suivant les cas être le DSI, les responsable monétique, financier, commercial ou le RSSI

### I.2.2. Une démarche "projet"

Nous parlons dans ce document de "projet PCI DSS". Ces projets, compte tenu de leurs différentes composantes (détaillées ci-avant), du nombre d'acteurs, de leur complexité et de leurs coûts, doivent être réalisés en mettant en œuvre une démarche de gestion de projet rigoureuse. Cette démarche doit permettre de définir l'organisation du projet, son budget, sa documentation, son suivi, ses risques, ses jalons, son planning et mettre en œuvre des organes de suivis. La bonne pratique peut consister à adopter des standards de gestions tels que ceux

définis par le *Project Management Institute* (PMI). A l'aide d'un outil de suivi rigoureux, il sera possible d'orienter le projet efficacement, d'alerter en temps et en heure et traiter ces alertes, d'impliquer les niveaux de management nécessaires pour prendre les décisions et apporter des solutions aux problèmes, et donc atteindre la conformité dans le respect du temps et des budgets initialement définis.

### I.2.3. Une communication maîtrisée avec l'acquéreur

Le demandeur de la conformité est l'acquéreur. Un processus de communication auprès du responsable de la conformité de l'acquéreur est donc nécessaire ; Il conviendra de mettre en œuvre un processus contrôlé, permettant de communiquer uniquement lorsque cela est nécessaire, et notamment à des fins de validation. L'utilisation d'une société qualifiée et disposant d'une expérience significative dans la conduite de projets de conformité PCI DSS permettra de s'appuyer sur les expériences passées du QSA et donc de défendre plus efficacement les solutions adoptées pour la conformité, et par exemple les mesures compensatoires décidées.

### I.2.4. Des échanges entre réseaux de pairs, ...

Le standard PCI DSS est parfois très précis sur certaines mesures à mettre en place, et sur d'autres thèmes nécessite une analyse plus approfondie. Cette analyse peut être facilitée par les différentes sociétés de conseils et QSA. De plus, des échanges entre confrères travaillant sur les mêmes thématiques permettent d'avoir une diversité de retours d'expériences sur les difficultés et les succès de mise en œuvre suivant le contexte.

### I.2.5. La gestion du changement

Comme abordé précédemment, un programme de mise en conformité est très lié aux métiers, et sa mise en œuvre aura des impacts plus ou moins importants suivant les processus. Ainsi l'accompagnement tout au long de la démarche afin de sensibiliser et d'expliquer les changements permettra une adhésion. Le comportement des acteurs durant la phase de mise en conformité permettra de faciliter cette mise en œuvre et sa conservation dans le temps.

### I.2.6. L'intégration avec d'autres démarches

Un des avantages de la démarche de conformité PCI DSS est sa transversalité. Nous avons évoqué ci-dessus les nombreux enjeux et impacts que pourra avoir le projet sur de nombreux services, métiers, organisations et processus de l'entreprise. Ceci fait de chaque projet PCI DSS un véritable projet d'entreprise. Compte tenu néanmoins du sujet, qui s'articule autour d'une meilleure maîtrise des risques, il convient de considérer, au plus tôt dans la démarche d'initialisation du projet, d'identifier les potentialités d'intégration de la démarche avec d'autres démarches de conformité, de gestion de la sécurité, de gestion des risques et de gestion du contrôle interne de l'entreprise (ex : loi de sécurité financière, contrôle interne, démarche CNIL, conformité ISO, ...) . L'intégration de la démarche avec d'autres initiatives transverses telles que celles-ci permettra :

- D'améliorer l'adhésion et l'implication financière de la part des décideurs ;
- De tirer parti des canaux de communications et méthodologies existantes ;
- D'intégrer le projet dans des outils ou démarches existantes (exemple : existence d'outils de GRC dans l'entreprise permettant de documenter le projet) ;
- D'améliorer le retour sur investissement du projet.

## *I.3. Les bonnes pratiques pour débuter*

### I.3.1. Inclure les métiers en amont du projet

La donnée carte étant nécessaire à la réalisation d'un certain nombre de processus métier, il est important d'expliquer le plus tôt possible la démarche de mise en conformité aux différents responsables métiers. Ainsi ils percevront mieux les enjeux et seront force de proposition pour modifier des processus en place afin de manipuler différemment les données cartes, voir afin de ne plus les manipuler du tout.

### I.3.2. Spécialisation et/ou Externalisation

Une fois la cartographie des processus nécessitant des données cartes réalisée, le périmètre initial de la mise en conformité est déterminé. En spécialisant les processus, il est possible dans un certain nombre de cas d'atteindre un périmètre minimal. La mise en conformité pouvant alors s'appliquer à ce dernier via la mise en place d'une structure spécialisée ou bien via une externalisation vers un tiers déjà conforme (exemple des Payment Service Providers ou PSP). Attention même si l'externalisation permet de faciliter la mise en conformité, la responsabilité est la même (Cf. Chapitre VI.3 du document « PCI DSS : Une présentation » publié par le CLUSIF en 2009)

### I.3.3. Analyse de risque préalable

PCI DSS est le résultat d'une analyse de risques réalisée par les membres fondateurs du PCI Council. Il n'est pas laissé de latitude quant aux mesures à appliquer, comment les appliquer et où les appliquer sauf dans le cadre des mesures compensatoires qui sont très encadrées. Cependant une analyse de risques préalable permettra de mieux comprendre les enjeux en amont de la mise en conformité et de disposer d'éléments à partager avec les différentes parties prenantes et avec les sponsors.

### I.3.4. Utilisation de l'Analyse d'écart ou Gap Analysis pour justifier coûts et risques sous-jacents

Une des étapes clés du projet reste l'évaluation des coûts ; L'expérience montre fréquemment une sous-évaluation de ces coûts, entraînant la mise à disposition de budgets insuffisant, et donc des contraintes budgétaires en cours de projet, nécessitant soit l'obtention de fonds additionnels, soit le report de la conformité. Afin de bien évaluer les coûts du projet, une bonne pratique consiste à réaliser une analyse d'écarts (ou "*gap analysis*"). Cette analyse peut être réalisée assez rapidement et sans nécessité la réalisation de tests complexes. La bonne pratique consiste, pour chacun des objectifs de contrôle, à évaluer la conformité, principalement en utilisant du déclaratif (ou auto-évaluation). A cette étape, le plus simple reste d'employer une échelle de notation simple, comme par exemple :

- 0 – non conforme
- 1 – conformité partielle, effort nécessaire
- 2 –conforme

Puis, pour chaque point de non-conformité ou de conformité partielle, une estimation des besoins de conformité, du coût des solutions potentielles et de la charge de travail associée pourra être estimé.

Cette première estimation nécessitera d'être affinée dans le temps mais permettra de dimensionner les éléments budgétaires relatifs au projet.

La notation de base du projet permettra également de mettre en œuvre un tableau de bord de suivi de l'avancement du projet.

### I.3.5. Le besoin d'un processus de monitoring permanent de la conformité et d'amélioration continue

La démarche de conformité PCI DSS nécessite la mise en œuvre d'une démarche de monitoring permanent de la conformité. En effet, il ne s'agit pas ici d'un processus unique, tel un examen, visant à obtenir une certification, mais bien d'un processus à mettre en œuvre permettant de garantir la conformité dans le temps ; Rien ne serait plus désastreux que de mettre en œuvre des efforts majeurs de conformité et donc d'engendrer des coûts significatifs pour l'organisation, sans mettre en œuvre des processus pérennes et sans suivre la conformité dans le temps. Une telle situation aboutirait généralement à une dérive de la conformité et à nouveau à des coûts significatifs de (re)-mise en conformité pour l'audit annuel suivant. Il convient donc, dès la phase de définition des processus nécessaires à la conformité de bien intégrer les deux éléments suivants :

- La définition d'un processus pérenne permettant de maintenir la situation de contrôle dans le temps
- La définition d'un processus de suivi de la conformité des processus mis en œuvre, s'appuyant sur des dispositifs de reporting et éventuellement un dispositif de surveillance contrôle continu ("*continuous control monitoring*").

## *I.4. Les avantages de la démarche :*

Finalement, quels sont les avantages d'un projet de conformité à PCI DSS?

### I.4.1. La certification

Bien évidemment, il s'agit de l'objectif principal de tout projet. Nous avons vu néanmoins que beaucoup d'autres objectifs de l'entreprise et de sécurité informatique pourront être atteints grâce à un projet de mise en conformité PCI DSS.

### I.4.2. Protection contre le risque d'image et la perte de clientèle

Les scandales récents le confirme, la perte d'image, et donc de clientèle est réelle en cas de compromission de données. Les coûts sous-jacents peuvent être extrêmement importants et très préjudiciables, notamment pour des entreprises dont le modèle s'appuie uniquement sur la vente à distance par exemple.

### I.4.3. La définition et la mise en œuvre de capacités

Ces dernières, après avoir atteint leur stade de maturité, peuvent être transférées à d'autres parties de l'organisation. En effet, certains objectifs de contrôle de PCI DSS nécessitent la mise en œuvre d'outils, d'organisations et de processus nouveaux pour les traiter. Bien qu'initialement limités au périmètre de PCI DSS, une bonne pratique consistera à déployer progressivement, après les avoir éprouvées, ces nouvelles capacités sur d'autres pans de l'organisation. Le déploiement pourra s'opérer en utilisant par exemple la classification des données, ciblant en priorité les données et systèmes sensibles.

### I.4.4. Intégration des différents partenaires dans la démarche

Un autre avantage de la démarche consiste en l'intégration des différents partenaires dans la démarche, incluant responsables, opérationnels métiers, équipes informatiques, prestataires, ...

L'accès à ces parties prenantes permet, non seulement de les impliquer dans la démarche, mais également de les sensibiliser et de les former aux impératifs de sécurité liés à l'exécution de leurs tâches et aux données auxquelles ils ont accès. Il s'agit donc d'une voie royale permettant de faire passer des messages et principes de sécurité, et par exemple des principes de la politique de sécurité devant être appliqués par chacun des acteurs en fonction de son rôle dans l'organisation. Cela permettra à la fois de donner du sens à la conformité, en indiquant qu'il ne s'agit pas uniquement d'une obligation externe, mais qu'il s'agit bien aussi d'être conforme aux politiques de sécurité qui étaient déjà existante préalablement à la mise en conformité PCI DSS. Afin de gérer efficacement, et par exemple organiser des sessions de formations auprès des responsables et équipes métiers, il conviendra d'intégrer la Direction des Ressources Humaines dans la démarche. Cela permettra à la fois de respecter les processus internes, mais également d'apporter du poids et des moyens à cette démarche de sensibilisation et de formation.

### I.4.5. Intégration de la sécurité dans les projets métiers

Le dernier avantage que nous souhaitions mettre en exergue est l'intégration de la sécurité dans les projets métiers en cours et futurs de l'entreprise. En effet, afin de se conformer aux exigences du standard ou de maintenir la conformité, il est impératif de prendre en compte les exigences de sécurité lors de l'initiation de tout projet. Cet objectif est souvent difficile à atteindre par les RSSI lors de l'exercice de leur fonction. Par l'intégration obligatoire de cette démarche pour la conformité PCI DSS, il est alors possible d'instaurer un comportement et un usage, démontrant la valeur de l'approche et des méthodologies d'analyse de risques développées en ce sens.

## *I.5. Tableau de relations de PCI DSS vs ITIL, LSQ, LCEN, CNIL, Directive EU, …*

Logique du contrôle permanent à mettre en avant sous-jacentes à ces exigences et bonnes pratiques

*Relation PCI DSS / ISO 27001* : les finalités sont distinctes, les synergies existent

ISO 27001 établit les exigences d'une gouvernance de la sécurité de l'information, le corps de la norme étant en fait le modèle d'amélioration continue PDCA. Elle ne préjuge pas des mesures de sécurité suivies dans cette gouvernance, à part celles qui relèvent de la gouvernance elle-même, laissant libre le choix de leur applicabilité dans une déclaration prévue à cet effet. Il est prévu pour cela que la déclaration d'applicabilité, tout en utilisant le format et explicitant sa complétude sur l'annexe A de la norme, peut être enrichie de mesures ou de référentiel de mesures spécifiques complémentaire.

Le standard PCI DSS impose une posture de conformité à un certain nombre d'exigences de sécurité et impose le périmètre de l'entreprise sur lesquelles elles portent, selon un cadre de gouvernance largement dilué dans celles-ci :

- L'approche par les risques : mentionnée au point de contrôle 12.1.2a, mais pas de mise en perspective dans le contexte donné, a fortiori dans le contexte PCI DSS (enjeux métier, natures du traitement du risque, porteur du risque, acceptation des risques résiduels, etc.)
- Le contrôle périodique et permanent plus exactement, les différents composants de la phase CHECK : la section 11 couvre un certain nombre de points relevant de IS 27001 4.2.3 ; néanmoins, il s'agit essentiellement d'exigences de sécurité techniques.

- La logique d'amélioration continue, plus exactement, la logique de revue périodique qui relève d'un modèle CHECK / ACT : mentionnée au titre de certaines de ces exigences (1.1.6, 10.6, 12.1.2b, 12.1.3…)
- La logique de gestion des enregistrements et de la documentation « dire ce que je fais, faire ce que je dis » : mentionnée explicitement dans certaines exigences (ex. : 1.1.5, 12.2…), mentionnée assez largement dans les « procédures de test »

Un tableau est envisageable, mais les défauts de la norme 27001 (d'une part des éléments de gouvernance énoncés strictement, puis dilués dans des exigences en annexe, d'autre part un périmètre laissé au choix de l'entreprise) et ceux de PCI DSS (des exigences incluant des éléments de gouvernance peu développés – voire peu opérants, une délimitation de périmètre qui repose sur l'information du porteur de carte bancaire, les fonctions qui l'utilisent, et un critère de séparation préalable) rendent difficile l'exercice de mise en correspondance *stricto-sensu*.

*Relation PCI DSS / ISO 20000/ITIL* : les finalités sont distinctes, les synergies existent largement du fait de l'inscription forte du périmètre décrit par PCI DSS dans un contexte de production informatique et réseau, notamment :

- Gestion des incidents : focalisée dans un contexte particulier pour PCI DSS (12.5.3, 12.9)
- Gestion des changements : focalisée dans un contexte particulier pour PCI DSS 6.4, 11.2
- Gestion des configurations : 1.1, et d'autres exigences diluées ; l'utilisation d'une CMDB ITIL, ISO 20 000) rend industrialisables plusieurs exigences PCI DSS
- Gestion des mises en production : Comme pour la Gestion des changements, focalisée dans un contexte particulier pour PCI DSS 6.4, 11.2.
- Le modèle PDCA de la norme ISO 20000 : les remarques sont identiques à celles effectuées sur la synergie au modèle PDCA de la norme 27001

Un tableau de correspondance est envisageable et utile, mais l'imprécision de la norme ISO 20000 (ou ITIL, d'ailleurs) risque de donner un tableau assez vide.

| **Repères** | **PCI** | **SOX** | **Bale III** |
|---|---|---|---|
| Objet | Confidentialité des informations sensibles carte Visa / Mastercard / Discover / AMEX / JCB | Sincérité et fiabilité des comptes | Robustesse opérationnelle bancaire |
| Cadre | Contractuel | Pénal, US | Réglementaire |
| Entreprises éligibles | Entreprise actrice de tout ou partie du paiement électronique par carte Visa/Mastercard | Entreprises cotées sur territoire US ou avec plus de 5% d'actionnariat d'origine US | Banques |
| Menace traitée | Fraude liée à l'utilisation de données cartes | Fraude à la comptabilité | Dysfonctionnement métier |

On peut le constater avec le tableau ci-dessus, les finalités des référentiels SOX, Bale III et PCI DSS sont indépendantes, et relèvent d'enjeux et d'activités bien séparés.

Des processus comptables efficaces peuvent enregistrer de façon parfaitement intègre des anomalies issues des fonctions de paiement électronique dont les moyens sont vulnérables aux menaces identifiées dans le référentiel PCI DSS. Les comptes d'une société peuvent ainsi être certifiés conforme SOX alors qu'elle a subi des attaques significatives sur sa fonction de commerce électronique.

Cependant, il se peut que dans certaines entreprises, le personnel en charge du pilotage et de la mise en œuvre des processus de sécurité visant le respect des règles issues de ces référentiels soit le même. A ce titre, les tactiques de communication interne pour la gestion du changement peuvent « concentrer » les discours. Ainsi, certains pilotes de projet pourront choisir d'exprimer « on applique certaines de nos bonnes pratiques de sécurité issues de PCI sur les ressources informatiques utilisées par nos processus comptables ».

# II. Analyse et Réduction du périmètre

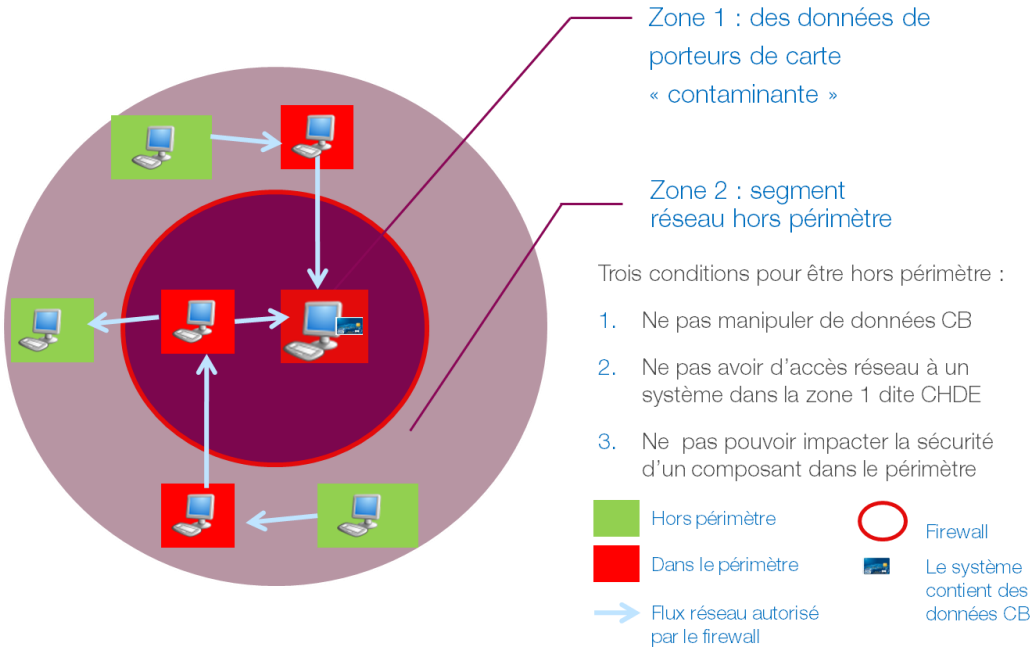
## *II.1. Définition du périmètre*

Les exigences du standard PCI DSS s'appliquent à tous les composants réseau, serveur ou application inclus dans, ou connectés à, l'environnement des données des titulaires de cartes.

L'environnement des données de titulaires de cartes est constitué d'individus, de processus et de technologies qui stockent, traitent ou transmettent les données de titulaires de cartes ou des données sensibles d'authentification.

On peut donc représenter cette définition du périmètre par l'approche par zone suivante, chaque zone devant être délimitée par un firewall (ou un cloisonnement de niveau 2 avec un durcissement approprié). Cette approche n'est pas « académique » dans le sens où elle n'est actuellement pas présentée comme tel par le PCI SSC, il semblerait cependant que le groupe de travail officiel du PCI SSC sur la définition du périmètre (« *SIG Scoping* ») tende à adopter une représentation similaire :

- **Zone 1** : c'est l'environnement de données de porteurs de carte, qui va contenir des données cartes. Tout système dans cette zone est impacté par PCI DSS, même s'il n'a aucun rapport avec le traitement de données CB. Pour cela, on dit parfois que cette zone 1 est « *contaminante* ».
- **Zone 2** : c'est un segment réseau qui ne contient pas de données de porteurs de carte, mais dont certains systèmes ont des accès pour se connecter via des firewalls à la zone 1 ou qui peuvent avoir un impact sur la sécurité de composants dans le périmètre (ex : annuaire LDAP, serveur d'antivirus…). Alors seuls ces systèmes sont impactés par PCI DSS (« contaminés »). Les autres systèmes de la zone 2 (sans accès réseau à la zone 1, ni impact sécurité possible) ne sont pas concernés.



Les technologies couvertes :

- Les composants réseau comprennent notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans fil, les équipements réseau et d'autres appareils de sécurité ;
- Les types de serveur comprennent, sans s'y limiter : les serveurs Web, d'application, de base de données, d'authentification, de messagerie, proxy, NTP (Network Time Protocol) et DNS (Domain Name Server) ;
- Les applications comprennent toutes les applications achetées et personnalisées, y compris les applications internes et externes (par exemple Internet) ;
- Les « composants du système » comprennent, en ce qui les concerne, tous les composants de virtualisation comme les machines, commutateurs/routeurs, outils, applications/bureaux virtuels ainsi que les hyperviseurs.

L'ensemble des personnes techniques ou métier, qui ont accès à un composant dans le périmètre PCI DSS rentre également dans le périmètre (même si leur usage normal ou leurs habilitations voudraient qu'ils n'aient pas accès aux données de porteurs de cartes).

## *II.2. Fournisseurs de service*

Les entités impactées par PCI DSS peuvent être amenées à faire appel à un prestataire tiers :

- pour le stockage, le traitement ou la transmission des données des titulaires de cartes en son nom,

et/ou

- pour la gestion de composants tels que les routeurs, les pare-feu, les bases de données, la sécurité physique et/ou les serveurs. Dans ce cas, la sécurité de l'environnement des données des titulaires de cartes peut s'en trouver affectée.

Dans ce cas, ce prestataire doit se mettre en conformité avec PCI DSS dans le cadre des activités dont il est question. Il existe deux options de validation de la conformité des prestataires de services tiers :

1. Ils peuvent subir une évaluation PCI DSS de leur propre chef et fournir à leurs clients la preuve de leur conformité.
2. S'ils choisissent de ne pas subir une évaluation PCI DSS de leur propre chef, leurs services devront être examinés en même temps que les évaluations PCI DSS de chacun de leurs clients.

## *II.3. Identification des composants contenant des données porteur de carte*

Au regard de la définition donnée pour le périmètre PCI DSS, l'élément central est bien sûr la présence de données carte (CHD). Dans la pratique, l'expérience a montré que les entreprises avaient une vision incomplète ou trop théorique des lieux de stockage de ces données. De nombreux lieux de stockage sont méconnus ou oubliés, comme par exemple certains fichiers de logs, des archives, des sauvegardes, des partages de fichiers réseau (parfois sur les postes de utilisateurs), les serveurs de messagerie, des plateformes d'échanges de fichiers, voire certaines bases de données. De même, certains flux de données, contenant des données PCI DSS en clair ou non, transitent par des segments réseau qui ne sont pas toujours identifiés comme faisant partie du périmètre.

La version 2.0 de PCI DSS introduit plus clairement une obligation de cartographie des CHD précise et confirmée par un certain nombre de vérification techniques à l'aide d'outils de recherche. Cette vérification n'a évidemment de sens que si elle est périodique. La fréquence d'une fois par an est indiquée.

La démarche suivante est préconisée pour confirmer l'exactitude et l'adéquation du champ d'application de PCI DSS :

- Étape 1 : recherche technique de données CHD dans l'ensemble des composants du système d'information. L'entreprise évaluée identifie et documente l'existence de toutes les données de titulaires de cartes dans son environnement, afin de vérifier que de telles données n'existent pas en dehors de l'environnement actuellement défini (CDE).
- Étape 2 : confrontation des lieux de stockage réels avec la vision théorique du CDE. Une fois tous les emplacements de données de titulaires de cartes identifiés et documentés, l'entreprise utilise les résultats pour vérifier que le champ d'application PCI DSS est approprié (par exemple, les résultats peuvent être un diagramme ou un inventaire des emplacements des données de titulaires de cartes).
- Étape 3 : correction des éventuels écarts avec la théorie. L'entreprise tient compte des données de titulaires de cartes qui se trouvent dans le champ d'application de l'évaluation PCI DSS et font partie du CDE, sauf si lesdites données sont supprimées ou transférées/regroupées dans le CDE actuellement défini.
- Étape 4 : traçabilité de cette vérification en vue de l'audit. L'entreprise conserve la documentation montrant comment le champ d'application PCI DSS a été confirmé et les résultats, pour l'examen de l'évaluateur et/ou pour référence au cours de l'activité annuelle de confirmation du champ d'application PCI DSS.

Cette recherche de PAN est généralement une démarche nouvelle pour les entreprises qui ne sont pas du tout habituées à procéder à de telles « enquêtes » sur leurs propres systèmes, d'autant plus que les recherches doivent obligatoirement être réalisées sur les environnements de production ET de non production (homologation, développement, recette…). Il convient de prendre des précautions pour éviter d'impacter la qualité de service, car ces outils de recherche sont particulièrement gourmands en ressources, et doivent être exécutés avec des privilèges élevés pour pouvoir accéder à l'ensemble des fichiers.

Le principe de fonctionnement de ces outils est toujours le même :

1. L'outil collecte les données dans lesquelles il doit chercher des données CHD : fichiers systèmes, bases de données, capture réseau, fichiers de sauvegarde…
2. L'outil utilise des expressions régulières pour identifier des donnés cartes. En effet, les données cartes ont un format bien déterminé : taille, caractères numériques, « plage BIN ». Voici quelques exemples de ces expressions régulières :

```
Visa: ^4[0-9]{12}(?:[0-9]{3})?$ All Visa card numbers start with a 4. New cards
have 16 digits. Old cards have 13.

MasterCard: ^5[1-5][0-9]{14}$ All MasterCard numbers start with the numbers 51
through 55. All have 16 digits.

American Express: ^3[47][0-9]{13}$ American Express card numbers start with 34 or
37 and have 15 digits.

Diners Club: ^3(?:0[0-5]|[68][0-9])[0-9]{11}$ Diners Club card numbers begin with
300 through 305, 36 or 38. All have 14 digits. There are Diners Club cards that
begin with 5 and have 16 digits. These are a joint venture between Diners Club and
MasterCard, and should be processed like a MasterCard.

Discover: ^6(?:011|5[0-9]{2})[0-9]{12}$ Discover card numbers begin with 6011 or
65. All have 16 digits.

JCB: ^(?:2131|1800|35\d{3})\d{11}$ JCB cards beginning with 2131 or 1800 have 15
digits. JCB cards beginning with 35 have 16 digits.
```

**Figure 1 : Regular expression searches for credit card numbers**

3. Comme ces expressions régulières génèrent beaucoup de fausses alertes (« falses positives »), une autre propriété des PAN est utilisée et vérifiée par les outils : il s'agit de la « clef de Luhn ».

**Rappel sur la clé de Luhn** :

C'est un checksum qui permet de vérifier si un numéro de carte bancaire peut être valide. Mais en aucun cas il ne permet de dire que le numéro existe. Cette formule permet de contrôler l'exactitude de la saisie du numéro de carte.

**Calcul de la clé de Luhn** :

| 4 | 4 | 0 | 8 | 9 | 8 | 5 | 5 | 0 | 0 | 0 | 0 | 0 | 5 | 8 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | |
| 8 | | 0 | | 18 | | 10 | | 0 | | 0 | | 0 | | 16 | |
| | | | | -9 | | -9 | | | | | | | | -9 | |
| 8 | 4 | 0 | 8 | 9 | 8 | 1 | 5 | 0 | 0 | 0 | 0 | 0 | 5 | 7 | 5 |

- ❖ 1ère étape : doubler les chiffres du PAN de rang pair en commençant par la droite.
- ❖ 2ème étape : soustraire 9 à tous les résultats dont la valeur est >= 10
- ❖ 3ème étape : on additionne les nouvelles valeurs qui ont un rang impair avec les chiffres de rang pair, le dernier digit exclu.
- ❖ 4ème étape : on divise cette somme par 10 et on soustrait le reste obtenue à 10.
- ❖ Si on obtient une différence égale au dernier digit du numéro de carte alors la clé de Luhn est vérifiée.

**Remarque** :

Après l'étape 2, si on fait l'addition de tous les chiffres qui ont un rang pair avec ceux qui ont un rang impair, si le résultat obtenu est un multiple de 10 alors la formule de Luhn est vérifiée. Ce qui veut dire que la clé de Luhn peut être n'importe quel chiffre de la carte bancaire mais uniquement de rang impair.

**Figure 2 : Clé de Luhn**

Voici à titre d'information une liste d'outils non-exhaustive employés par les QSA pour réaliser ce type de recherche :

**Outils OpenSource**

- Spider
- Ccsrch
- SENG
- Nessus
- Snort
- Outils open source forensic tools

**Outils commerciaux**

- Symantec
- RSA DLP
- Vericept
- Code Green Networks
- Reconnex
- Workshare
- Websense
- EnCase Forensic
- Card Recon

## *II.4. Détermination du périmètre*

Conformément à la procédure d'audit QSA, le périmètre doit être réévalué et confirmé tous les ans par l'auditeur lors de l'audit annuel. Dans le cadre de cet audit, il est de la responsabilité du QSA de valider le périmètre.

Le cas particulier des cartes mises en opposition ou dans une liste noire est abordé dans la FAQ du PCI SSC dans l'article n°5382 : s'il est confirmé par l'émetteur que les cartes en question ne sont plus valides, alors ces cartes sont considérées désensibilisées et PCI DSS ne s'applique plus dessus, jusqu'à leur éventuelle réactivation.

| **Does PCI DSS apply to "hot cards," fraudulent or invalid card numbers, or cancelled cards?** | Article # 5382 |
|---|---|
| If the issuer confirms the cards are inactive or disabled, the PANs (Primary Account Numbers) no longer pose fraud risk to the payment system. The PCI DSS would not apply in these cases. If however, the PAN is later reactivated, PCI DSS will again apply. | **Reviewed:** 12/29/2008 |

**Figure 3 : Article #5382 de la FAQ du PCI SSC**

## *II.5. Réduction du périmètre par désensibilisation des données de porteur de carte*

Cette approche cherche à désensibiliser les données afin de réduire le périmètre d'application de PCI DSS. Il convient en premier lieu de rappeler que des données de porteur de carte chiffrées sont encore considérées comme des données sensibles et que tout système qui stockerait, manipulerait ou ferait transiter de telles données chiffrées serait toujours pleinement impacté par PCI DSS.

NB :

Il existe une exception à cette règle : si l'on peut prouver que l'entité juridique qui reçoit les données DÉJÀ chiffrées avec de bons algorithmes et ne dispose pas des clefs permettant de réaliser le déchiffrement (source : FAQ du PCI SSC, Article #10359), alors les données sont considérées comme désensibilisées. Voici deux exemples pour illustrer cette exception :

- Si une entité externalise des bandes de sauvegardes chiffrées sur un site externe appartenant à un tiers, et que ce tiers ne dispose pas des clefs de déchiffrement, alors ce tiers est hors périmètre.
- Si ces mêmes sauvegardes sont stockées sur le NAS de l'entreprise, alors le NAS est dans le périmètre, car il appartient à la même entité juridique qui détient les clefs de déchiffrement.

Pour désensibiliser les données PCI DSS, il convient d'utiliser l'une de ces 3 différentes méthodes :

- On peut appliquer au PAN une fonction de hachage basé sur une méthode de cryptographie robuste. La fonction utilisée doit être mathématiquement irréversible. L'utilisation de l'algorithme SHA-224 est le minimum recommandé. L'utilisation d'un grain de sel unique est recommandée.
  Le résultat d'un PAN auquel on applique SHA-256 a la forme suivante :
  - Hash (1234 5678 9012 3456)= e3c4f2b46378660d18369ed506a72987ec1ff56e
- Pour désensibiliser les applications on peut tronquer le PAN. Tronquer le PAN revient à masquer certains numéros de la carte bancaire. PCI DSS recommande de conserver en

clair les 6 premiers chiffres du PAN et les 4 derniers (au maximum).
- 1234 56XX XXXX 4321

- Une autre option de désensibilisation est le remplacement du PAN par un identifiant. On appelle cette méthode de remplacement, la tokenisation. Le vrai PAN sera remplacé par un token, qui peut avoir ou non le format d'un PAN (voir chapitre suivant).

Dans ces 3 cas, le caractère « irréversible » de ces opérations de désensibilisation sur les PAN fait que les applications qui manipulent uniquement ces données désensibilisées peuvent être exclues du périmètre d'application de PCI DSS.

Point important : il ne faut pas conserver à la fois le PAN tronqué et le PAN Hashé, sans quoi, des attaques cryptographiques simples permettent de reconstituer le PAN complet. Pour cette raison, si une entité est contrainte de stoker à la fois les PAN tronqué et le PAN Hashé, alors ces données conjointes ne seront pas considérée comme étant désensibilisées, et les systèmes concernés seront dans le périmètre PCI DSS.

| **Type de donnée** | **Données considérée désensibilisée** |
|---|---|
| PAN | Non |
| PAN Chiffré | Non |
| PAN Tronqué | Oui |
| PAN Hashé | Oui |
| PAN Tronqué + PAN Hashé | Non |
| Token | Oui |

**Les données PCI DSS correctement hachées ou tronquées seules ne sont plus considérées comme des données PCI DSS à protéger.**

Ces précédentes opérations de désensibilisation ne sont pas transparentes pour l'utilisateur légitime. Le hash et la troncature sont des méthodes relativement simples à mettre en œuvre, mais qui ont l'inconvénient de ne pas répondre à tous les besoins métiers. En effet, dans certains cas on a besoin du numéro complet de la carte bancaire, pour effectuer certaines opérations. Le numéro de carte bancaire est utilisé pour le paiement mais il sert aussi à identifier les personnes de par son caractère unique.

Or, à partir du hash ou du tronqué du PAN, il est impossible d'effectuer certaines opérations (irréversibilité de ces méthodes de désensibilisation). Par exemple :

- Dans le cas d'une fraude au paiement, il est impossible de retrouver un porteur avec pour seul numéro le hash du PAN ou le PAN tronqué.
- Dans le cas d'une opération de remboursement, le marchand a besoin du numéro complet de la carte pour effectuer l'opération.

C'est pourquoi une analyse fine de ces besoins métier est nécessaire afin de déterminer la stratégie de désensibilisation à utiliser.

Dans de nombreux cas, il est nécessaire de pouvoir revenir in fine aux données porteur en clair pour des usages bien particuliers, tel que la réquisition judiciaire ou le contentieux ou parfois simplement l'opération de paiement en elle-même. Ces usages rendent les méthodes

de désensibilisation basées sur des hash ou des troncatures insuffisantes pour couvrir tous ces usages métiers. C'est pourquoi la tokenisation, qui permet de retrouver les données en clair, présente un avantage certain.

### II.5.1. Principe de tokenisation

La tokenisation est le processus qui consiste à remplacer le numéro de carte bancaire (PAN) par un identifiant unique pour chaque PAN qu'on appellera un token. Une table de correspondance PAN/Token est gardée dans un système sécurisé. Les PAN (et autres données sensibles) seront stockés chiffrés dans cette table.

**Les avantages de la tokenisation**

- La tokenisation permet de réduire le périmètre d'application du standard PCI DSS : les composants du système qui traitaient des numéros de cartes vont désormais manipuler des tokens. Le token n'ayant aucun lien avec le vrai PAN (on ne peut pas retrouver le vrai PAN à partir du token), les applications seront désensibilisées.
  - Les composants ne seront plus soumis à PCI DSS.
  - En cas de vol du token, celui-ci sera inexploitable puisqu'il est irréversible.
- Le token peut avoir le format d'un PAN, c'est-à-dire qu'il peut avoir la même longueur qu'un PAN et le même format (des chiffres).

**Les inconvénients de la tokenisation**

- Pour pouvoir « *tokeniser* », il faut rajouter à l'architecture de paiement un composant qui permet de faire cette opération, il faut donc mettre en œuvre le système, gérer les communications avec le reste des composants, et faire en sorte que la nouvelle architecture fonctionne et respecte les exigences PCI DSS.
- Selon la méthode utilisée pour désensibiliser les applications, la migration peut être plus ou moins complexe concernant la gestion d'un nouveau type de donnée (voir plus loin).

**Format d'un token**

Les algorithmes permettant de créer les tokens doivent remplir deux objectifs :

- Maintenir une relation d'unicité entre le PAN et le token, c'est-à-dire que pour un PAN donné on aura un unique token correspondant et inversement.
- Conserver le PAN tronqué c'est-à-dire ne conserver qu'au plus les 6 premiers chiffres et les 4 derniers. L'intérêt d'avoir un PAN tronqué c'est qu'il peut être utilisé par certaines personnes qui en ont besoin pour une utilisation particulière. Le PAN tronqué permet par exemple de prouver l'utilisation d'une carte à un moment donné, en cas de déni d'utilisation de la part de la personne.

Le token généré contiendra le PAN tronqué (avec au plus les 6 premiers et les 4 derniers chiffres du PAN original) et le reste des chiffres du token sera représenté par un compteur, donc le token sera unique pour chaque PAN donné.

Exemple :

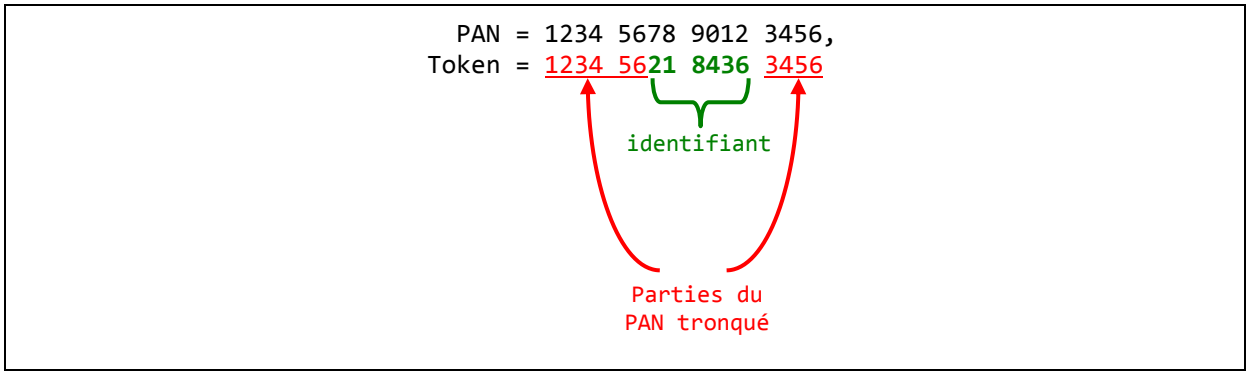



**Figure 4 : exemple de token**

- Les avantages :
  - La migration des applications est moins complexe car le format obtenu suite à la génération du token est identique à celui d'un PAN (16 chiffres par exemple).
  - Pas de changement au niveau des schémas des tables des bases de données.
- Les inconvénients :
  - Le calcul du PAN est un calcul « statefull », c'est-à-dire qu'on a besoin d'aller chercher dans une table le PAN reçu pour savoir si un token lui correspondant existe déjà ou pas.
    Cela induit une latence de la recherche car il faut chercher parmi tous les PAN déjà existants dans la table.
  - La clé de Luhn peut ne plus être vérifiée

**Les recommandations de Visa concernant la tokenisation**

Le 14 Juillet 2010, Visa a publié un document sur les meilleures pratiques pour l'utilisation de la technologie de tokenisation Visa Best Practices, Tokenization Version 1.0.

Voici les principales préconisations :

1. Le système de tokenisation

Le système qui permet de faire de la tokenisation :

- doit être correctement segmenté du reste du réseau et doit être déployé dans un environnement conforme à PCI DSS.
- L'accès à ce système ne doit être autorisé qu'aux entités ayant été authentifiées.
- Il convient de faire une surveillance du système lors de la demande d'un PAN pour un token donné pour détecter les activités anormales.
- Le système doit pouvoir également faire la différence entre le token et le PAN pour éviter les erreurs.

2. La génération du token

On ne doit pas pouvoir retrouver (calculer) le PAN à partir d'un token donné. Pour cela, les différentes méthodes suivantes peuvent être utilisées pour générer le token :

- Une fonction irréversible : un compteur, une fonction de hachage (avec un sel d'une longueur de 64bits au minimum) ou un une fonction qui génère les nombres de manière aléatoire.

- Un algorithme connu pour sa robustesse

**Important :**

Ne jamais garder ou transmettre un PAN haché avec un PAN tronqué sans utiliser un grain de sel robuste et secret (risque d'attaque par force brute).

On peut générer différents types de token :

- Le token à usage unique
- Le token à multi-usage

3. Association token/PAN

Le PAN ne doit être envoyé qu'aux utilisateurs et systèmes dûment habilités. Toute application qui est habilitée à récupérer les PAN en clair se retrouve dans le périmètre d'application de PCI DSS.

4. Le « Card Data Vault »

Le PAN doit être chiffré lors de son stockage et le « *Card Data Vault* » doit être géré et protégé selon les exigences PCI DSS.

5. Chiffrement et gestion des clés

Les clés de chiffrement et les signatures doivent respecter une taille minimale selon l'algorithme de chiffrement ou la fonction de hash utilisées.

| Algorithme | Longueur en bit |
|---|---|
| TDES | 112 |
| AES | 128 |
| RSA | 2048 |
| ECC | 224 |
| SHA | 224 |

6. Reprise d'antériorité sur les données

Les données sensibles cartes bancaires présentes avant l'implémentation de la tokenisation, doivent être protégées, soit en les supprimant, soit en les intégrant dans le système de tokenisation.

### II.5.2. Détermination du périmètre dans le cas des groupes

Pour les entreprises qui ont une structure de groupe, avec différents filiales ou franchises (entités légales) amenées à manipuler des données de porteur de carte, les règles de détermination du périmètre sont les suivantes :

- Pour pouvoir envisager une approche par certification entité par entité, il est nécessaire de s'assurer du cloisonnement sécurité de ces entités tant sur le plan technique que fonctionnel. Si le cloisonnement n'est pas conforme à PCI DSS, il est nécessaire d'envisager de certifier l'ensemble.
- Pour déterminer le « niveau » de ces entités, basées sur le nombre de transactions annuelles et par réseau Cartes, il y a plusieurs cas de figure :
  - Pour les filiales, il convient de comptabiliser le total de toutes les transactions annuelles de l'ensemble des filiales ;
  - Pour les franchisés :
    - S'il y a une centralisation des données cartes au niveau du groupe, alors il convient de comptabiliser le total de toutes les transactions annuelles de l'ensemble des franchisés,
    - S'il n'y a pas une telle centralisation des données cartes[2] (par exemple lors d'une transmission directe des données à la banque depuis chaque franchise), alors on comptabilise le nombre de transactions franchise par franchise.

### II.5.3. Champs d'audit de certification

Il convient de différencier le champ d'audit de certification du périmètre de l'audit :

- Le périmètre d'application de PCI DSS, que nous avons décrit jusqu'à présent dans ce document,
- Le champ de l'audit de certification, qui peut être un sous ensemble de ce premier.

Voici les éléments qui permettent de réduire le périmètre de l'audit de certification, et donc les coûts associés :

- La notion d'échantillonnage permet de ne pas auditer la totalité des composants qui présente des similitudes dans leur configuration. Le choix de la taille de l'échantillon est du ressort de l'auditeur. Si l'auditeur se rend compte de que les configurations ne sont pas identiques, alors la taille de l'échantillon est amenée à augmenter au cours de l'audit.
- L'utilisation d'applications certifiées PA-DSS permet de réduire le périmètre de l'audit d'un client. En effet, tous les aspects de conformité de l'application (chiffrement de PAN, développement sécurisé, logs…) sont considérés déjà validés. Seule la procédure d'installation de l'application et l'environnement sous-jacent sur lequel sera implémentée l'application sur un environnement et la formation des utilisateurs sont évalués dans le cadre de l'audit.

# III. Externalisation : certification, contrainte

Pour faciliter sa mise en conformité PCI DSS, une entreprise peut choisir d'externaliser certaines activités afin de réduire son périmètre d'évaluation. L'externalisation des traitements de cartes bancaires (pour info CB est une « marque » du système de paiement carte français) vers un tiers (PSP) ou du développement d'applications de paiement sécurisé présente des avantages certains mais n'exempt pas l'entreprise de tout contrôle.

## *III.1. Les PSP*

Les PSP (*Payment Service Providers*) sont aujourd'hui assez largement implantés dans beaucoup d'entreprises, et notamment les « nouvelles » entreprises très présentes sur la vente en ligne sur Internet. Ces acteurs permettent en effet de simplifier et de centraliser les échanges avec les différents acquéreurs, tout en offrant des niveaux de service très élevés.

Ces PSP sont aujourd'hui des acteurs très actifs sur le marché PCI DSS. Ils peuvent en effet jouer un rôle majeur dans une stratégie de mise en conformité, dans la mesure où leurs offres permettent d'externaliser une bonne partie des traitements cartes bancaires des entreprises, et sont très souvent proposées en standard sur des environnements entièrement certifiés PCI DSS. Les PSP sont aujourd'hui en mesure de proposer l'externalisation de tous les composants de la chaine de liaison paiement par Internet ou par téléphone :

- Collecte des données par page web, serveur vocal interactif ou TPE ;
- Demandes d'autorisation et de paiement (paiement immédiat, à l'expédition, à l'abonnement, remboursement…) ;
- Contrôles anti-fraude avancés (listes grises, clé de Luhn, adresse IP de l'utilisateur, nombre d'utilisations par jour…).

Et l'externalisation peut aller encore plus loin… Motivés par PCI DSS, les PSP sont aujourd'hui en mesure de proposer des tables de correspondance « tokenizer ». Lors de la collecte de données, un token personnalisable est renvoyé à l'entreprise et peut donc circuler dans le SI sans aucune contrainte vis-à-vis de la norme PCI DSS.

L'externalisation permet ainsi de réduire conséquemment le périmètre applicatif, mais attention… l'externalisation n'est pas une échappatoire à PCI DSS…

1. Il est en effet indispensable de s'assurer que le prestataire est conforme PCI DSS sur les services offerts. Dans une très grande majorité, les PSP assurent une conformité PCI DSS de leur côté, mais notons qu'il est également possible d'inclure le périmètre externalisé dans l'audit PCI DSS, même si l'intérêt d'une telle configuration est clairement limité. Ajoutons qu'un accord écrit spécifique est nécessaire dans lequel il est stipulé que le PSP est responsable des données porteur qu'il traite (exigence 12.8.2).
2. Il existera très souvent un périmètre PCI DSS en interne chez le marchand. Certaines populations auront parfois le besoin d'accéder au numéro de carte depuis leur poste de travail. Nous pouvons par exemple citer les services de lutte anti-fraude ou les téléconseillers. Ces populations auront toujours la possibilité d'interroger le PSP pour récupérer le numéro à partir de l'identifiant unique, mais leurs terminaux devront alors rester dans le périmètre PCI DSS. Il est donc illusoire de penser qu'aucun composant du SI ne manipulera de données cartes.

VISA a introduit au premier trimestre 2012 la notion de « *merchant agent* » plus large que la notion de PSP.

## *III.2. Comment choisir son PSP*

### III.2.1. Contexte et objectifs de la démarche

En Europe, le passage à la conformité PCI DSS n'est pas une contrainte légale pour les commerçants. Pourtant, au travers des pressions répétées et appuyées de leurs banques d'acquisition, ceux-ci commencent à reconnaître la mise en conformité PCI DSS comme un passage obligé.

Sont concernés tout particulièrement les sites de e-commerce, où la phase de paiement est primordiale dans la confiance accordée par le client au vendeur, et où le commerçant doit disposer d'une solution d'encaissement fiable et efficace. Le choix de faire appel à un PSP pour assurer cette phase "délicate" permet alors au commerçant de faire d'une pierre deux coups : s'affranchir de tous traitements afférant aux données cartes bancaires clients tout en résolvant la mise en conformité PCI DSS.

### III.2.2. Appel d'offre

La consultation porte sur la phase "acceptation", qui peut être décomposée en trois étapes :

- collecte des données,
- conservation des données,
- gestion du paiement.

Le commanditaire peut aussi choisir une formule avec lotissement :

- les deux premières étapes uniquement : le soumissionnaire ne réalise que la collecte et la sauvegarde des données, puis s'interface avec le PSP pour l'étape de gestion du paiement,
- l'ensemble des trois étapes de la phase acceptation, le soumissionnaire est alors le PSP.

### III.2.3. Critères de choix

Comme pour toute consultation, les critères de choix restent classiques :

- qualité de la réponse,
- pertinence du soumissionnaire : pérennité et référence,
- qualité de la solution technique : adéquation, services, disponibilité, évolutivité,
- coûts : compétitivité et lisibilité,
- autres critères : solutions proposées pour d'autres canaux de vente (MOTO, magasins), réactivité de mise en place et de changement, localisation géographique des moyens de traitement, autres.

### III.2.4. Fonctionnalités attendues

La partie ci-après est structurée par thèmes, où pour chacun d'eux, une énumération la plus exhaustive possible des différents points à considérer est proposée. A chacun de développer ou non ces différents points selon ses propres besoins.

1. collecte des données :
   - PSP e-commerce
     i. collecte par page web,
     ii. page web dédiée au site (cas d'enseignes multi-sites),
     iii. graphisme adaptable,
     iv. multi langues,
     v. utilisation d'un protocole sécurisé,
     vi. information du client concernant la page sécurisée,
     vii. redirection complète du client avec personnalisation de l'adresse,
     viii. console d'administration de la page de paiement,
     ix. exhaustivité des cartes bancaires, privatives, ou autre moyen de paiement
     x. multiplicité des moyens de règlement pour un même achat,
   - PSP « carte présente »
     i. Support des technologies (TPE, automates…)
     ii. multi langues,
     iii. utilisation d'un protocole sécurisé,
     iv. console d'administration de la solution de paiement,
     v. exhaustivité des cartes bancaires, privatives, ou autre moyen de paiement
   - PSP de type Call Center
     i. Langues
     ii. …

2. demandes d'autorisation :
   - capacité à traiter avec l'ensemble des acquéreurs du marché,
   - information du client sur le résultat de la demande d'autorisation,

3. conservation des données :
   - durée de vie de la carte ou autre durée,
   - cloisonnement et/ou partitionnement logique entre base de données (cas multi-sites),

4. gestion des données cartes bancaires par les clients :
   - enregistrement, modification, suppression, gestion de plusieurs cartes,
   - accès par utilisation identifiant/authentifiant du site client,
   - charte graphique personnalisable,

- possibilité d'association token/données cartes bancaires,
- gestion de la date d'expiration de la carte bancaire,
- fourniture possible PAN tronqué, token, date d'expiration,

5. mise à jour et évolutivité :
   - engagement de délais,

6. lutte anti-fraude :
   - présence d'un module anti-fraude, quels contrôles ?,

7. 3D Secure (e-commerce) :
   - mise en œuvre possible,
   - avec choix des sites (cas multi-sites),
   - mise en œuvre différée possible,

8. méthodes de paiements :
   - immédiat,
   - par lots,
   - sur demande,
   - suivant échéancier,
   - micro paiement,
   - paiement 1 clic,

9. demande d'opérations bancaires :
   - renouvellement autorisation,
   - demande paiement,
   - annulation paiement,
   - remboursement,
   - autres propositions …

10. reporting :
    - fréquence et moyens,
    - mode et méthode de consultation,
    - granularité (par enseigne, par franchisé etc.)
    - possibilité vue globale (cas multi-sites),

11. solution de retrait achat en magasin par identification via carte bancaire.

12. niveaux de services :
    - engagements en fonction des périodes,
    - mesures techniques mises en œuvre,
    - temps de conversion,
    - capacité de connexions et de sauvegardes,
    - capacité de traitements en pics,
    - surveillance et escalade,
    - support technique,
    - langues

## *III.3. Les applications de paiement PA-DSS*

Les entreprises peuvent également envisager l'achat d'applications de paiement dans le cadre du traitement de l'autorisation ou du règlement. Ces applications doivent répondre au standard PA-DSS, ce qui assure que son développement et sa maintenance ont été audités et sont considérés comme sécurisés, et faciliterons la conformité PCI DSS.

Toute application de paiement PA-DSS est accompagnée d'un guide de mise en œuvre de la norme PA-DSS. L'entreprise choisissant d'utiliser une application PA-DSS reste néanmoins soumise aux exigences PCI DSS et doit respecter les recommandations d'exploitation préconisées par le fournisseur d'applications de paiement dans son guide d'implémentation de l'application, fourni obligatoirement avec l'application.

Par exemple, la gestion des droits d'accès de l'application doit être convenablement configurée. De même, les derniers correctifs de sécurité doivent être installés et les procédures de contrôle de modification convenablement documentées.

Attention toutefois : la certification PA-DSS ne concerne que des applications « prêtes à l'emploi », non personnalisées. Elle ne concerne pas non plus des applications développées sur mesure pour un seul client. Dans ce cas, le développement de ces applications reste dans le périmètre de l'audit PCI DSS du client. Il faut donc le prévoir dans les relations contractuelles entre le client et son fournisseur.

## *III.4. Transfert de responsabilité dans le cadre de l'externalisation*

L'externalisation est un moyen pour réduire le périmètre d'application de PCI et peut souvent s'avérer une solution moins coûteuse qu'une mise en conformité complète en interne. Mais pour réussir un projet d'externalisation, il est important de ne pas considérer les projets d'externalisation comme de « simples » projets PCI DSS. En effet, un projet d'externalisation est particulièrement impactant sur les chaines applicatives et les processus, et doit être motivé par des besoins ou considérations avant tout métiers et/ou financières. Or un projet

d'externalisation peut devenir stratégique pour l'entreprise. Parmi les critères stratégiques pour le choix ou non d'un PSP :

- Le développement de nouveaux moyens de paiements (ex : cartes cadeaux), de nouveaux marchés internationaux (facilités de connexions aux acquéreurs étrangers) ou de nouvelles fonctionnalités (ex : paiement one-click sans renseignement des données CB).
- Le champ du transfert de responsabilité
- Avantage concurrentiel pour adresser de nouveaux marchés
- Impact sur le coût de la transaction (à la hausse ou à la baisse)

Pour l'entreprise concernée, au regard des conséquences d'image, de pertes financières et de pénalités contractuelles, induites par l'atteinte à la confidentialité de l'information du porteur de carte bancaire, il est nécessaire de distinguer en premier lieu les parties prenantes suivantes dans son organisation :

- en anglais, l'*accountable*, en français le redevable : il subit l'impact de la conséquence du risque et rend les comptes devant les parties intéressées (son management, les actionnaires, les clients) de l'éventuelle incapacité de l'entreprise à atteindre certains de ses objectifs (opérationnels, financiers, de leader de confiance). On le désigne pour cela « porteur » du risque.
- le *responsible*, en français le responsable des actions utiles à la maîtrise du risque. Ainsi dans une approche de gestion de risque il met en place les mesures de sécurité mettant en œuvre un plan de traitement du risque. Dans une approche de conformité contractuelle, les mesures de sécurité sont imposées par le référentiel auquel il est décidé de se conformer.

En pratique, il arrive souvent une distorsion des visions : le responsable peut disposer du budget utile à la mise en conformité PCI sans pour autant recevoir d'objectifs le rendant solidaire du redevable, qui demeure comptable des conséquences devant les parties intéressées.

Lorsqu'une externalisation d'activité opérationnelle est envisagée, il est donc possible :

- d'externaliser l'« *accountability* » : c'est un transfert du risque
  - c'est le cas de l'externalisation de la fonction de paiement et de l'ensemble des moyens concernés à un prestataire PCI DSS, qui prend la responsabilité contractuelle de la conformité PCI DSS avec la banque acquéreur
- de garder interne l'*accountability* et d'externaliser la « *responsability* » : ce n'est pas un transfert du risque, c'est seulement un transfert de ressource opérationnelle sans transfert de responsabilité contractuelle avec la banque acquéreur :
  - Externalisation de tout ou partie des processus de MCO
  - Externalisation de la gestion des clefs de chiffrement
  - Externalisation de la fonction de contrôle (section 11)
  - … tout est potentiellement envisageable !

Note : un engagement de résultat dans une prestation d'externalisation n'implique pas nécessairement le transfert du risque, tout dépend de la nature de l'engagement.

Au titre du maintien de la relation contractuelle, les éléments de la section 12.8 s'appliquent dans tous les cas. Dans le cas d'externalisation de la « *responsability* », l'éligibilité PCI DSS

du périmètre impose des points de contrôle appropriés, permettant d'apporter la preuve de la maîtrise du périmètre et de la conformité elle-même.

Dans tous les cas, un contrat devra être établi entre l'entreprise et le PSP, qui déterminera l'étendue des responsabilités respectives. Toutefois, les parties devront respecter les dispositions relatives à l'informatique et aux libertés, qui s'imposent à elles.

En France, la loi du 6 janvier 1978 « informatique et libertés » encadre strictement la responsabilité et les obligations des parties en termes de traitement de données à caractère personnel. Cette législation se retrouve à l'échelon européen du fait de l'uniformisation apportée par la directive du 24 octobre 1995.

Il importe de distinguer deux cas :

### 1. L'entreprise traite des données à caractère personnel

Dans cette hypothèse, l'entreprise collecte par exemple elle-même des données de cartes bancaires, avant de les transmettre au PSP.

Les données de cartes bancaires sont des données à caractère personnel puisqu'elles permettent d'identifier, directement ou indirectement, une personne physique (art. 2 de la loi du 6 janvier 1978).

Ici, l'entreprise détermine les finalités et les moyens du traitement qu'elle met en œuvre pour traiter les données de cartes bancaires. Par conséquent, elle acquiert la qualité de responsable du traitement (art. 3 de la loi du 6 janvier 1978).

Dès lors, en application de l'article 34 de la loi du 6 janvier 1978, l'entreprise est tenue de prendre « toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Dans cette configuration, le PSP apparaît comme un sous-traitant, c'est-à-dire une personne traitant des données à caractère personnel pour le compte du responsable du traitement, et agissant sur instruction de ce dernier. En application de l'article 35 de la loi du 6 janvier 1978, le PSP doit en conséquence présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité prévues à l'article 34. En particulier, le contrat liant l'entreprise au PSP doit comporter l'indication des obligations incombant au PSP en matière de protection de la sécurité et de la confidentialité des données, et doit prévoir que le PSP ne peut agir que sur instruction du responsable du traitement. L'entreprise devra donc veiller à ce que ses instructions soient systématiquement conformes aux exigences du standard PCI DSS.

Dans tous les cas, l'entreprise, responsable du traitement, n'est pas déchargée de son obligation de veiller au respect des mesures de sécurité (art. 35 de la loi du 6 janvier 1978), aucun transfert de responsabilité envers le PSP n'étant possible.

Aux termes de l'article 226-17 du Code pénal, « le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 (…) est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende », la peine d'amende étant portée au quintuple pour les personnes morales (art. 131-38 du Code pénal).

## 2. L'entreprise ne traite pas de données à caractère personnel

Si l'entreprise se contente de renvoyer tout traitement de données de cartes bancaires au PSP, alors chargé de déterminer lui-même les finalités et les moyens du traitement, elle n'est pas considérée comme responsable du traitement des données de cartes bancaires et n'est donc pas concernée, pour ce type de données, par les dispositions de la loi du 6 janvier 1978.

Qu'en est-il des données transmises via des passerelles : dans le cas de données porteurs envoyées par une passerelle et non traitées ?

Dans cette hypothèse, le contrat liant l'entreprise au PSP précisera généralement que le PSP sera responsable de tout dommage causé par le traitement de données de cartes bancaires, notamment en cas de non-respect du standard PCI DSS.

# IV. Projet de mise en conformité

## *IV.1. Gouvernance des projets PCI DSS*

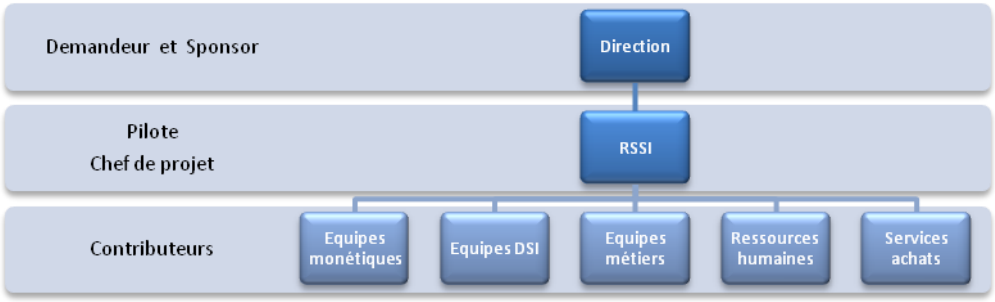
Le standard PCI DSS a la particularité de couvrir de façon transverse de nombreux sujets, et donc de domaines de responsabilité au sein des entreprises. Il en résulte que l'organisation humaine des projets de mise en conformité peut prendre des aspects très différents d'une entreprise à l'autre. De façon générale, les profils suivants sont généralement mis à contribution :

- La direction financière, ou autre entité métier en relation avec la banque ou les réseaux de carte, reçoivent en premier les demandes de mise en conformité. Il en résulte qu'ils ont généralement un rôle de demandeur dans le projet, voire de sponsor.
- Le responsable Risques, une fois le risque de compromission des données cartes bancaires identifié dans la cartographie des risques, peut également devenir demandeur de la mise en conformité PCI DSS.
- Le Responsable Sécurité des Systèmes d'Information est nécessairement un contributeur du projet, tant les exigences portent largement sur des sujets de sécurité informatique.
- Les Responsables métier et/ou monétique : les modifications qu'entraine PCI DSS dépassent le simple cadre de la sécurité informatique ; les modifications dans les applications métiers/monétiques manipulant de la carte, voire dans certains processus métier requièrent une implication forte des acteurs fonctionnels en charge de ces composants.
- Les équipes informatiques et métiers, les ressources humaines, les services achats sont mis à contribution dans le cadre de la mise en œuvre des différents chantiers.

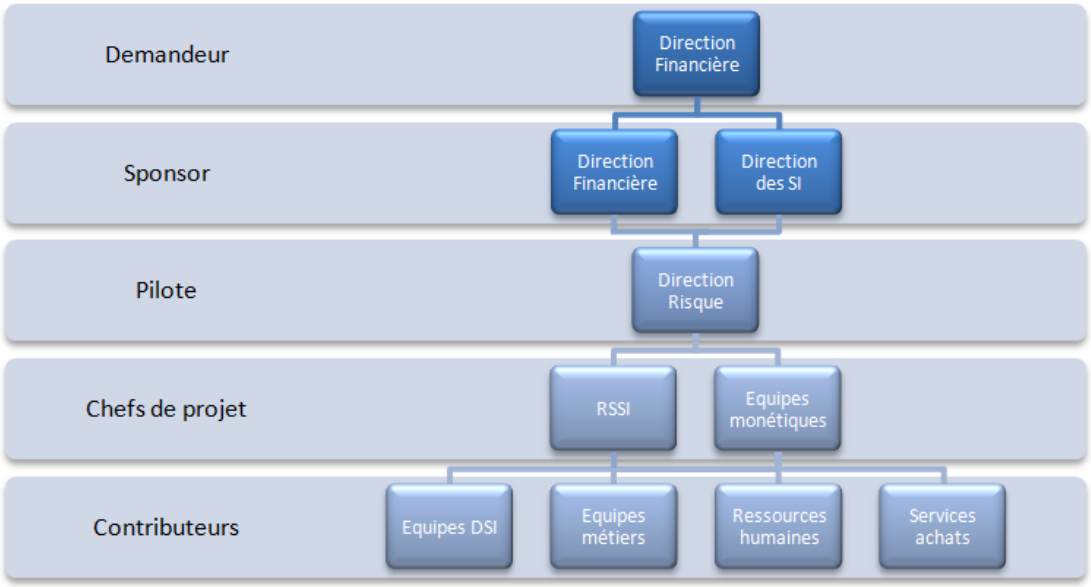
Selon la taille de l'entreprise, les contextes et enjeux particuliers, et les sensibilités de chaque personne, les organisations du projet PCI DSS peuvent être très différentes. Voici deux exemples de typologies d'organisation projet :

Les exemples de poste correspondent à des fonctions qui peuvent être cumulées entre elles ou avec d'autres fonctions, selon la taille de l'entreprise.

1. Organisation projet simple, généralement mise en place dans les petites structures :



2. Organisation projet pouvant être mise en place dans les plus grandes structures, où une collaboration forte RSSI/Responsable Monétique est nécessaire :

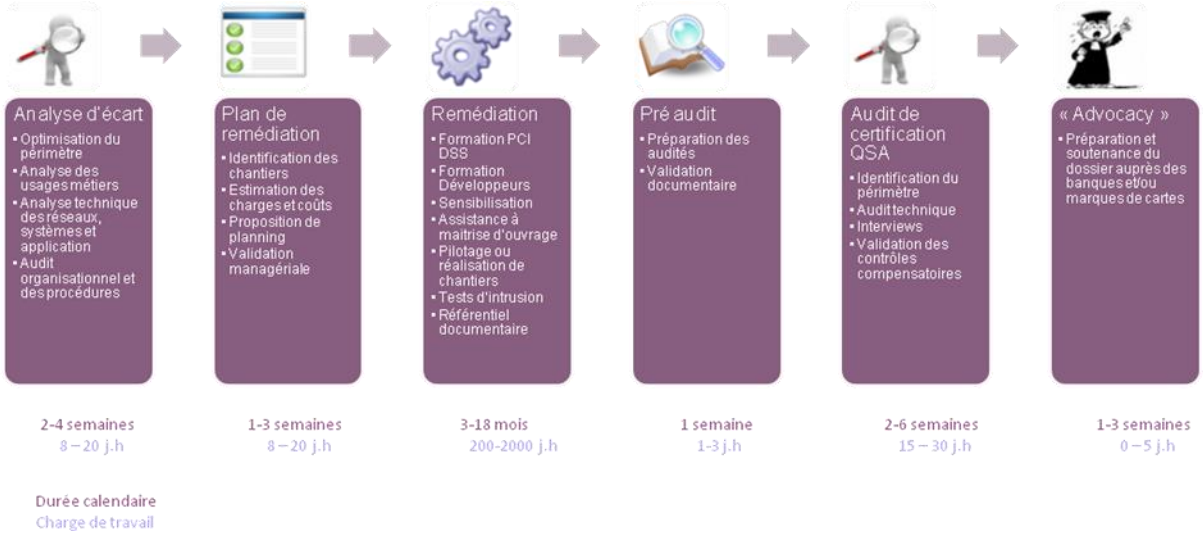



Entre ces deux exemples, une multitude d'organisations projet existe. Néanmoins, on peut identifier deux facteurs de succès communs dans l'organisation des projets de mise en conformité PCI DSS:

- l'identification d'un sponsor situé au-dessus de la Direction Information, tant les implications de PCI DSS dépassent le simple cadre de l'informatique (projet d'entreprise).
- Prévoir une collaboration entre sécurité (RSSI) et métier (Responsable Monétique), tant les projets PCI DSS sont structurants pour ces deux aspects.

## *IV.2. Étapes macroscopiques d'un projet de mise en conformité*

Voici les étapes macroscopiques d'un projet de mise en conformité, ainsi que quelques ordres de grandeurs sur les durées de chaque phase :



## *IV.3. Analyse d'écarts et plan de remédiation*

Les responsabilités de cette partie du projet au sein de l'entreprise se trouvent généralement au sein de l'équipe SSI (DSI / RSSI) et plus rarement au sein de l'équipe d'audit interne plus généralement impliquée plus tard lors de phases de maintien de la conformité.

Il existe 2 approches pour l'analyse d'écart :

- Approche déclarative
  - Moins efficace que l'approche par vérifications.
  - Plus rapide et donc moins couteuse.
  - Souvent utilisée quand on sait d'expérience qu'un gros travail de réduction du périmètre est encore à réaliser.
- Approche vérifications effectives à l'instar d'un audit réel :
  - Très efficace pour obtenir un plan de remédiation précis.
  - Quasiment aussi longue et couteuse qu'un audit réel.

L'une des premières étapes d'un projet de mise en conformité est l'analyse d'écarts entre l'existant et la cible demandée par PCI DSS. Cette étape est structurante pour la suite du projet, dans la mesure où elle détermine toute la stratégie et les actions qui seront mises en œuvre par la suite.

Cette analyse d'écarts s'articule autour des étapes suivantes :

- Identification d'un périmètre actuel et cible :
  - Identification des usages métiers autour de la donnée CB ;
  - Identification fonctionnelle et technique des composants supportant ces usages métier ;
  - Analyse du cloisonnement réseau ;
- Analyse d'écarts sur le périmètre actuel et/ou cible :
  - Interviews, analyse documentaire, (voire analyses techniques) sur les exigences PCI DSS (sur les composants réseau, système, applicatifs, sites physiques, aspects RH, etc).

À l'issue de cette étape, l'entité dispose d'une liste de tâches à réaliser :

* Approche par priorité / étapes (document du PCI SSC publié en mars 2009)

La première étape d'un projet PCI est bien entendu la définition du périmètre et sa remise en question qui passe par une réflexion entre autre de la légitimé de stocker, transmettre et traiter des données porteurs ayant un impact sur ce dernier. Une fois le périmètre identifié une approche par les risques est recommandée pour mettre en œuvre les exigences PCI DSS, c'est l'objet de l'approche par priorité développée par le PCI SSC.

L'approche par priorité développée par le PCI SSC est issue d'une analyse de risque qui permet, à travers une démarche structurée, d'identifier les zones à risques élevés afin de les traiter en priorité, de se reposer sur une démarche commune agréée par le PCI SSC et les émetteurs de cartes bancaires, et à démontrer sa progression dans le processus de mise en

conformité. Cette démarche est également recommandée dans le cadre d'un plan de mise en conformité et permet de sensibiliser et réduire les risques de compromissions de données porteurs au sein de l'entité concernée tout au long de la démarche.

L'approche par priorité est constituée de six jalons présentés ci-dessous priorisés en fonction des facteurs de risques les plus élevés et les menaces croissantes auxquelles est confrontée la sécurité des données porteurs :

1er jalon : Supprimer les données d'authentification et limiter la conservation des données

2ème jalon : Protéger le périmètre, interne les réseaux sans fil

3ème jalon : Sécuriser les applications de paiements par carte

4ème jalon : Surveiller et contrôler l'accès aux systèmes

5ème jalon : Protéger les données porteurs stockées

6ème jalon : Finaliser la mise en œuvre des exigences et s'assurer que toutes les mesures de sécurité sont en place

Le PCI SSC rappelle également qu'il s'agit là d'une approche par les risques dans le cadre d'un projet de mise en conformité PCI DSS et que la conformité ne sera validée qu'à partir du moment où l'ensemble des exigences PCI sont en place. La pratique a néanmoins démontré que les réseaux sont très sensibles à cette démarche qui permet aux commerçants de niveau 1 de faire état de leur conformité et de l'état d'avancement du projet aux réseaux, même en cas de conformité partielle.

# V. Démarches complémentaires

Le standard PCI DSS prévoit certaines activités qui ont pour vocation d'identifier les éventuelles failles dans le SI de la société. Ces activités doivent être effectuées de façon périodique et après tout changement majeur dans l'environnement PCI DSS de la société.

Les activités en question sont :

- Test d'intrusion : tous les douze mois
- Recherche de vulnérabilités externes : tous les trois mois
- Recherche de vulnérabilités internes : tous les trois mois
- Identification de points d'accès sans fil illicites : tous trois mois

## *V.1. Test d'intrusion annuel*

Le test d'intrusion doit avoir pour cible l'environnement PCI DSS : aussi bien les réseaux internes que les adresses externes de l'environnement.

Le test doit viser aussi bien les composants réseau afin de pénétrer dans les zones internes de l'environnement que les applications afin d'en prendre le contrôle. Au moins tous les types de failles listées dans les exigences 6.5.1 à 6.5.9 de PCI DSS doivent être vérifiés.

Les tests doivent être effectués par des individus qualifiés (ayant l'expertise de tests d'intrusion) et faisant partie d'une organisation indépendante de celle des équipes responsables de l'environnement PCI DSS.

Il n'y a pas de format particulier pour le rapport mais les résultats des tests doivent être consignés afin de permettre le suivi des actions correctives sur les failles identifiées et la validation lors d'un audit PCI DSS.

Des attaques de type « Social Engineering » peuvent faire partie du test mais ce n'est pas obligatoire.

## *V.2. Recherche de vulnérabilités externes*

Ce test doit être effectué par un prestataire agréé (ASV) sur l'ensemble des adresses publiques de l'organisation avec un outil automatisé

Le résultat d'un tel test est un rapport conforme aux exigences définies par PCI SSC pour les ASV.

Un rapport produit par un ASV contiendra les failles/problèmes identifiés assortis d'un degré de sévérité évalué conformément à CVSS et en se basant sur la liste des failles connues : NVD/CVE.

Un test qui révèle des failles dont le score CVSS est supérieur ou égal à 4.0 est considéré comme échoué. Le test est également considéré comme échoué s'il révèle des non conformités au standard PCI DSS. En cas d'échec, des corrections doivent être apportées et le test doit être réalisé à nouveau tant qu'il n'est pas réussi.

## V.3. Recherche de vulnérabilités internes

Similaire à la recherche de vulnérabilités externes, ce test a pour cible toutes les plages d'adresses internes appartenant à l'environnement PCI DSS a minima (mais peut être étendu à l'ensemble des réseaux internes de la société) et peut être effectué par une ressource interne à la société mais indépendante des équipes responsables de l'environnement PCI DSS. Ce test doit évaluer la criticité des failles révélées. Pour les failles classées comme élevées, une correction doit être apportée rapidement et validée par un nouveau test.

## V.4. Identification de points d'accès sans fil illicites

Les points d'accès sans fil illicites peuvent se présenter sous des formes différentes (équipements, cartes d'extension internes, contrôleurs intégrés, périphériques USB) et mettre en œuvre des technologies variées (wifi, Bluetooth, Infrarouge).

Leur identification peut être effectuée par divers moyens, notamment :

- Recherche de signal par des équipement et/ou logiciels adaptés ;
- Inspection des locaux à la recherche d'équipements illicites apparents ;
- Identification des équipements connectés aux réseaux locaux.

Cette recherche peut être effectuée par une ressource interne et doit donner lieu a un rapport qui permettra de donner suite aux anomalies relevées. La recherche doit être effectuée dans l'ensemble des locaux de la société qui hébergent tout ou partie de l'environnement PCI DSS.

## V.5. Autres activités de maintien de sécurité récurrentes

En plus des recherches de failles effectives sur l'infrastructure on peut noter les activités récurrentes suivantes nécessaires pour la conformité PCI DSS :

- Revue de la politique de sécurité : tous les douze mois ;
- Analyse de risque : tous les douze mois ;
- Test du plan de réponse aux incidents : tous les douze mois ;
- Campagne de sensibilisation des employés : tous les douze mois ;
- Formation du personnel responsable de la sécurité : tous les douze mois ;
- Suivi de la conformité à PCI DSS des sous-traitants : tous les douze mois ;
- Revue des règles des pare-feu : tous les six mois ;
- Revue de code des applications internes : avant chaque mise en production ;
- Identification de patchs de sécurité disponibles : permanent avec au plus un mois pour le déploiement ;
- Inspection des événements de sécurité remontés par les composants de l'environnement PCI DSS : quotidien (peut être partiellement automatisé).

## V.6. Références

https://www.pcisecuritystandards.org/documents/asv_program_guide_v1.0.pdf

https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf

https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf

## *V.7. Analyse de risques*

L'exigence N°12 du standard (*Requirement 12 : Maintain a policy that addresses information security for all personnel*.) attend de l'organisme qu'il réalise lui-même une étude des risques pesant sur son environnement. Cette appréciation des risques n'est pas à faire sur l'ensemble du périmètre retenu pour la certification dans la réduction du périmètre.

En effet, ce qui peut paraître troublant voire source de discussions lors de la première lecture du standard, c'est bien ce sentiment que l'appréciation des risques ainsi que le choix des mesures de traitement ont été fait pour l'organisme par le PCI-SSC. La politique de sécurité serait-elle écrite et imposée par le standard PCI DSS ?

***C'est vrai et c'est faux :***

**C'est vrai**. Effectivement l'ensemble des 12 exigences et 290 mesures associées expriment bien cette idée que les risques identifiés et retenus sont réduits par ces mêmes mesures ou cette politique de sécurité. Dans la posture de traitement des risques, la dynamique même du processus de certification peut s'assimiler à un transfert du risque, devrait-on même dire un partage de celui-ci, avec la société en charge d'instruire le *Report On Compliance (ROC)*, le QSA.

Cette posture dans la décision de traitement est par ailleurs un point de discorde entre les différents acteurs :

- Pour certains, les mesures imposées par le standard ne sont pas suffisantes ou trop contraignantes ; compte tenu de leurs propres enjeux et engagements vis-à-vis du réseau ou de l'acquéreur. Par ailleurs, si les mesures de sécurité correspondent à des risques faudrait-il savoir quels sont-ils ? Ils ne sont pas explicitement décrits dans le standard.
- Pour d'autres, ces mêmes mesures représentent les règles de sécurité à mettre en œuvre pour couvrir leurs besoins de sécurité, ceux-là mêmes permettant de garantir des besoins de sécurité quelques fois pas toujours exprimés voire identifiés.

Pour réconcilier l'ensemble et permettre une couverture plus réaliste et optimale des risques représentant des enjeux pour l'organisme, l'exigence 12 ouvre la porte à cette gestion du risque. Il s'agit bien d'impulser une culture de la sécurité au sein de l'organisme en adressant tant les intéressés par la démarche, le métier, le risk management dans sa globalité, et la direction des systèmes d'information, que les utilisateurs de l'organisme par le développement d'une politique de sécurité.

**C'est faux**. Aucune entreprise ne dispose de la même politique de sécurité. Car les enjeux et les besoins, les scénarios de menace, les vulnérabilités et les risques ainsi que les objectifs de sécurité sont tous différents. Par analogie, si beaucoup d'entreprises s'imposent le choix de suivre les articles, les mesures et les préconisations associées issus de la norme internationale ISO 27002, peut-on dire que la norme impose la politique de sécurité ? Non.

De plus, si l'organisme doit passer par la mise en œuvre de contrôles compensatoires (dont les conditions sont précisées dans l'annexe B) ce dernier par une phase d'analyse des risques. Le

standard établit clairement, que si les mesures qu'il impose sont nécessaires et suffisantes pour atteindre les objectifs de sécurité poursuivis, il laisse la possibilité d'y déroger à condition d'apporter les justifications et la « preuve » d'une prise en compte des enjeux. Cette preuve pouvant être apportée par l'estimation des risques (probabilité, impact) lors de la description de chacune des mesures telles qu'attendues par l'annexe C (fiche de contrôles compensatoires). La sélection d'une mesure compensatoire n'est possible que si la réduction de probabilité d'occurrence du risque et/ou de la réduction de ses effets d'impact sont au moins équivalentes à ce que la mesure d'origine permettait.

Le suivi pour le respect du standard engage dans cette exigence n°12 que l'entreprise évalue son besoin de sécurité, qu'elle prenne la mesure des enjeux. Si elle dispose d'éléments de sécurité couvrant les 11 autres exigences, on attend d'elle qu'elle mette en œuvre une démarche pour élaborer sa politique de sécurité, sa communication et sa maintenance dans le seul et unique objectif de traiter les risques couverts par les 290 mesures du standard, et surtout de gérer les risques résiduels.

Le lecteur se fera donc son opinion à l'aune de la maturité de sa démarche SSI, tant dans l'ambition d'atteindre ses propres objectifs de sécurité que dans celle de satisfaire aux exigences du standard.

Revenons un instant, sur la démarche d'une PSSI. Si beaucoup souhaitent suivre le cadre de l'ISO 27002, savent-ils réellement quels en sont les objectifs et les grandes lignes pour arriver à développer et implémenter leur PSSI ? Nous laisserons au chapitre traitant des relations entre la démarche vers une certification PCI DSS et celle de la mise en œuvre d'un SMSI le soin d'évoquer les mesures de traitement choisies dans l'annexe A de l'ISO 27001.

La lecture attentive de la norme ISO 27002 apprendra à son lecteur qu'avant de se lancer dans l'écriture de sa politique de sécurité de l'information, noter ici la nuance avec la logique de Système d'Information, qu'il convient déjà de réaliser une appréciation des risques pour prendre des décisions de traitement. Le chapitre 4 de la norme permet donc de fixer la démarche vers une politique de sécurité de l'information. Cette logique concourt à ne choisir des mesures dans les 11 chapitres suivants que si ces dernières correspondent à des objectifs de sécurité, ceux identifiés avec décision de traitement.

La logique est donc bien de comprendre les besoins de sécurité, dans notre démarche ceux nécessaires à conserver le contrôle des données porteurs de carte, d'identifier les circonstances dans lesquelles une atteinte à la confidentialité de ces données est possible pour choisir des mesures de sécurité permettant de couvrir ces risques.

Le standard PCI DSS prétend donc, dans l'ensemble de ses 12 exigences et ses 290 mesures associées, apporter des réponses à cette question du choix du traitement des risques. Plus précisément, l'exigence 12 fixe et impose, quant à elle, deux éléments complémentaires :

- Il doit exister une Politique de Sécurité de l'Information (ici l'information est le bien essentiel représenté par les données porteurs de carte, et rien d'autre) ;
- Il doit exister une démarche d'appréciation des risques dans l'entreprise, avec un focus fort sur le risque résiduel.

Laissons de côté la logique de politique de sécurité de l'information, et revenons sur ce qui nous intéresse ici, le risque résiduel. Quel est-il ? Celui issu de l'appréciation des risques faite

par le PCI-SSC, réduit par les mesures de PCI DSS ? Ou celui que l'entreprise à elle-même évalué et traité ?

La vérité est encore entre les deux. La logique sous-tendue par les démarches de l'exigence 12 autour de cette notion de gestion des risques est bien double. Quels sont les risques résiduels ?

Dans une première approche le standard PCI DSS exige que les circonstances dans lesquelles une atteinte aux biens (ici toujours les données porteur de carte) sont possibles doivent être gardées sous contrôle, en d'autres termes :

- les **vulnérabilités**, devrait-on dire faiblesses, de l'organisme et de ses éléments techniques sont toujours identifiées. Une démarche de réduction de celles-ci est bien engagée. On attend plus qu'un engagement de moyens mais bien une atteinte du résultat,
- la **source de la menace** et les circonstances de sa manifestation ont été scénarisées. L'organisme a une vue précise de l'agent menaçant ses biens. S'agit-il de personnel de l'organisme ? De personnes externes ?...
- **l'exposition** à la menace est connue. Cette notion d'exposition recouvre tant les aspects vraisemblance de l'occurrence du scénario de menace, devrait-on dire du risque, que l'idée qu'il existe bien un chemin de relation entre la faiblesse et la source de la menace.
- L'évaluation des mesures de sécurité en place –qu'elles soient directes ou compensatrices- afin de garantir que **l'acceptation du risque résiduel** est bien telle qu'attendue par l'organisme.

Dans une démarche complémentaire, l'exigence 12 demande que l'organisme ait initié sa démarche d'étude des risques afin d'identifier, d'analyser, d'évaluer et estimer les conséquences de risques, ainsi que leur circonstance, sur le périmètre retenu par la certification PCI DSS. A cet égard, cette exigence se veut plus large que la seule étude des risques. Elle engage l'organisme dans une vraie politique de gestion de la sécurité de l'information :

- Quel est son patrimoine applicatif ? Dans le périmètre PCI DSS.
- Quels sont ses besoins de sécurité ?
- Quelles sont les scénarios de menace, leur vraisemblance, les vulnérabilités, les mesures de sécurité en place, la gravité des impacts ? Dans le but de déterminer les objectifs de sécurité.
- Comment et pourquoi la direction prend-elle la décision de tel traitement des risques ? Quelle emphase met-elle au développement d'une politique de sécurité de ses informations ?
- Quels liens faire entre cette exigence de conformité métier, voire commerciale, avec des exigences de conformité plus règlementaires ?
- Quelle communication de la politique est en œuvre ? Quelles mesures de sensibilisation et de formation des personnels sensibles sont en œuvre ?
- Comment la politique de sécurité est maintenue ?

Dans la même logique que nous l'avons exposé précédemment, on attend de l'organisme dans cette démarche de politique de sécurité qu'elle ne noircisse pas du papier pour écrire ses documents, mais bien qu'elle se lance dans un cercle vertueux de gestion de sa sécurité... avec

comme point d'orgue la gestion des risques résiduels. Notamment ceux qui peuvent attenter au maintien de la certification PCI DSS.

Pour conclure sur cette présentation de la démarche de l'analyse des risques attendue par le standard PCI DSS, il reste peut-être à aborder la logique d'acceptation des risques, résiduels en particulier. Qui fixe la limite entre le risque non supportable et celui qui peut être considéré comme supportable par l'organisme ? Au bénéfice de qui la décision d'acceptation doit-elle intervenir : L'organisme ? Son QSA ? Le(s) réseau(x) cartes ? Les acquéreurs ? ou finalement le principal intéressé : le porteur de la carte ? Ce critère d'acceptation du risque après la mise en œuvre des mesures de réduction indirectes (cas des contrôles compensatoires) fait appel à une précision importante sur les conditions qui amènent à accepter le risque résiduel après la mise en œuvre des dites mesures. Elles doivent être définies et acceptées lors de l'établissement du périmètre, même réduit, lors de la démarche vers la certification.

C'est souvent sur cette notion d'acception du risque résiduel que les points de vue achoppent entre les pours et les contres PCI DSS. L'ambition de l'exigence 12 est, sans doute, de réconcilier les uns et les autres en permettant à l'organisme de valoriser sa démarche SSI existante en démontrant sa gestion du risque.

En définitive, pour l'organisme dans la démarche PCI DSS, le risque le plus grave, celui qui serait intolérable pour la direction de l'entreprise, ne serait-il pas celui de ne pas obtenir voire de perdre sa certification PCI DSS ?

## *V.8. Les démarches en support*

La formation

Dans le document PCI DSS la formation n'est explicitement évoquée que dans deux chapitres. Le chapitre 6.5 pour le développement d'applications sûres et le chapitre 12.6 pour la sensibilisation des personnels impliqués de près ou de loin dans le programme PCI DSS.

Néanmoins, il apparait que la prise de conscience (*awareness*) est omniprésente dans tout le document. Chaque acteur impliqué dans le programme PCI DSS doit être conscient que les données qu'il manipule sont sensibles et requièrent une attention toute particulière aux règles de sécurité. Cette omniprésence est par ailleurs explicite par l'existence et la maintenance d'une PSSI qui, dès lors qu'elle s'appuie sur l'ISO 27001, inclut des exigences sur la formation et la sensibilisation des personnels.

Dans le chapitre 6.5 (développement et maintenance des systèmes et applications – applications basées sur des lignes directrices de codage sécurisé) il est explicitement mentionné que les développeurs doivent avoir suivi une formation reposant sur les meilleures pratiques et guides en la matière. Le contrôle doit se faire sur des interviews des développeurs afin de vérifier qu'ils maîtrisent ces techniques.

Le Chapitre 12 consacré à la maintenance d'une politique de sécurité de l'information pour l'ensemble du personnel (interne ou externe), évoque la sensibilisation à la sensibilité des données manipulées et la formation récurrente sur base annuelle aux bonnes pratiques de sécurité.

Le chapitre 12.6.1 insiste sur l'implication dans ce programme des prestataires. Il oblige que la vérification d'assistance aux formations et sensibilisation soit attestée formellement par chaque personne.

Enfin, concernant la formation, le chapitre 12.9 sur le plan de réponse aux incidents mentionne explicitement que les personnels doivent être préparés à réagir rapidement et cela par des entrainements réguliers.

En synthèse, la bonne application des règles d'une politique de sécurité basée sur l'ISO 27001 doit conduire le management à sensibiliser et former régulièrement l'ensemble du personnel à la sécurité de l'information. Concernant les personnels travaillant plus particulièrement sur des données cartes bancaires, soit dans la conception des applications, soit dans l'exploitation au quotidien des applications et des données, soit enfin dans la manipulation à la source ou aux extrémités (litiges, contentieux, statistiques, gestion de la fraude, etc.), il est essentiel de les sensibiliser plus que les autres, en particulier en attirant leur attention sur les risques pour l'entreprise et pour eux du non respect de ces règles.

# Conclusion

La mise en conformité PCI DSS doit être considérée comme un projet global transverse car elle impacte de nombreux acteurs bien au-delà du champ de l'informatique.

Sa mise en œuvre doit/peut être abordée comme une opportunité génératrice de valeur. En effet, l'évolution des processus et des technologies existantes dans l'entreprise, ou la création et mise en œuvre de nouvelles, sont autant d'occasions d'améliorer, d'optimiser et de développer les services fournis aux utilisateurs et clients.

Néanmoins, il convient de ne pas oublier que l'objectif principal de la conformité PCI DSS est la réduction du niveau de risque de fraude à partir des données cartes. Pour atteindre cet objectif, le PCI SSC a déterminé un certain nombre de mesures liées à la confidentialité et à la traçabilité de ces données cartes.

En parallèle il sera ainsi nécessaire d'atteindre les autres objectifs de la sécurité de l'information que sont la disponibilité et l'intégrité en fonction des besoins identifiés dans l'entreprise.

L'obtention de la conformité valide un état à un instant donné. Afin de conserver dans le temps ce niveau de conformité mais aussi d'optimiser les coûts de fonctionnement dans la durée et de maximiser la création de valeurs de ce projet pour l'entreprise, il sera essentiel de l'intégrer dans une démarche d'amélioration continue via la mise en œuvre d'un Système de Management de la Sécurité de l'Information.


L'ESPRIT DE L'ÉCHANGE

# CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

*Téléchargez les productions du CLUSIF sur*

www.clusif.fr