LES DOSSIERS TECHNIQUES

PCI DSS : une présentation

Novembre 2009

Groupe de travail « PCI DSS »

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr

Web : http://www.clusif.asso.fr

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective" et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ayants droit ou ayants cause est illicite" (alinéa 1er de l'article 40)

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal

REMERCIEMENTS

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

AUTRET Thierry	*GIE Cartes-Bancaires*
BRISSE François	*Capgemini*
DI GIAMBATTISTA Vincent	*Egencia Europe*
GREMY Jean-Marc	*Cabestant Consultants*
GREVREND Gérald	*Altran*
LATRECHE Abdelbaset	*Verizon Business*
LUPONIS David	*Mazars*
MARET Vincent	*E&Y*
MEYNARD Samuel	*Integralis*
NABET Benjamin	*Accor*
PIEDERRIERE Yann	*BT Services*
SCHAUER Hervé	*Hervé Schauer Consultants*
SIMONETTI Rodolphe	*Verizon Business*

Nous remercions aussi les adhérents du CLUSIF ayant participé à la relecture.

SOMMAIRE

I - Introduction

En France, début 2009, les acteurs bancaires ont clairement annoncé leur soutien au standard PCI DSS, tel cet extrait du site Web du Groupement des Cartes Bancaires « CB » :

> *« …La communauté bancaire française et le Groupement Cartes Bancaires CB partagent les objectifs du standard PCI DSS, eux-mêmes déclinés à partir des standards ISO 27001 de sécurité des systèmes d'information, en visant un haut niveau de protection des données sensibles des cartes. La communauté considère que les objectifs de sécurité définis par le référentiel PCI DSS correspondent à l'état de l'art de ce que recommandent aujourd'hui les experts pour sécuriser les bases de données, les échanges d'informations, pour protéger les contrôles d'accès, »… « Depuis plusieurs années, tous les acteurs concernés ont lancé des programmes de sécurisation de ces données sensibles ; à ce jour, de nombreux commerçants et prestataires de services ont déjà terminé ou sont sur le point de finaliser leur mise en conformité PCI DSS. »*

Visa, MasterCard, American Express, Discover et JCB ont fondé en 2006 le Payment Card Industry Security Standards Council (PCI SSC) avec pour objectif de définir un référentiel de sécurisation des données carte bancaires s'appuyant sur des bonnes pratiques : PCI DSS. Ce référentiel s'applique à toute entité qui traite et/ou stocke de la donnée carte.

Si les échéances données par les organismes cartes concernant la conformité sont échues, l'application des pénalités est envisagée au cas par cas dans les relations contractuelles entre les différents acteurs. A titre indicatif les pénalités publiées par VISA Inc. sont de l'ordre de 25 000$ mensuels en cas de non-conformité et de 500 000$ d'amende en cas de compromission avérée.

En effet, depuis la fin des années 1990, plusieurs fraudes massives ont touché les systèmes d'informations qui traitent des données carte, en voici quelques exemples :

- CardSystems Solutions Inc (Fournisseur de service de paiements)
  Une faille de sécurité a entraîné la compromission de 40 millions de cartes en 2005, cette société a fait faillite depuis.

  http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm

- TJX : Groupe de distribution (commerce) présent aux Etats-Unis et en Europe.
  Une faille concernant un réseau sans fil aurait conduit à la compromission de 45,6 millions de numéros de cartes en 2006.

  http://www.securityfocus.com/news/11455

- Royal Bank of Scotland WorldPay Inc. : activité fournisseur de services de paiement aux Etats-Unis de la banque anglaise RBS.
  Une fraude concernant potentiellement 1,5 million de numéros de cartes a été identifiée en 2008.

  http://www.rbslynk.com/RBS_WorldPay_Press_Release_Dec_23.pdf

- Heartland Payment Systems Inc. (Fournisseur de service de paiements).
  De multiples systèmes d'écoutes ont été trouvés sur les systèmes de la société Heartland en 2008, compromettant ainsi environ 130 millions de cartes.

  http://www.2008breach.com

II - Notions de données porteur

Les données porteur correspondent aux données liées au porteur de la carte de paiement qui sont fournies au commerçant ou récupérées par le commerçant lors d'une transaction de paiement.

Celles-ci sont constituées des informations suivantes :

- Données des porteurs de carte devant faire l'objet d'une protection :
  1. Numéro de compte primaire (PAN, Primary Account Number) ;
  2. Nom du titulaire de la carte de crédit ;
  3. Code de service ;
  4. Date d'expiration.
- Données d'authentification sensibles dont le stockage est interdit après l'autorisation de la transaction :
  5. Données de bandes magnétiques complètes ou leur équivalent stocké sur la puce ;
  6. Le code CAV2/CVC2/CVV2/CID (appelé également cryptogramme visuel): code à 3 chiffres au dos de la carte utilisée pour les transactions à distance, type Internet (le nom diffère selon la marque de la carte) ;
  7. Bloc PIN (qui est une version chiffrée du code PIN).

Les données porteur sont sensibles pour plusieurs raisons :

- Elles peuvent permettre de passer des transactions de paiement (numéro, nom du porteur, date de validité, CVV2, PIN), et donc entraîner des fraudes. Parfois un simple PAN permet de réaliser une transaction ;
- Elles peuvent permettre d'identifier le porteur (nom du porteur, numéro de carte) et sont donc considérées comme des informations indirectement nominatives par la CNIL ;
- Le numéro de carte est parfois utilisé comme identifiant dans des applications, ce qui peut permettre de faire le lien avec des personnes ;
- Elles peuvent permettre de récolter des informations sur les cartes de paiement (type de transactions autorisées, pays émetteur, etc.) et donc de cibler des utilisations malveillantes.

Il est important d'avoir à l'esprit que ces données n'appartiennent ni au porteur ni au commerçant, mais à l'émetteur de la carte conformément au contrat porteur.

III - Présentation des acteurs

III.1 - Le PCI Security Standards Council (PCI-SSC)

En 2006, Visa, MasterCard, American Express, Discover et JCB ont fondé le Payment Card Industry Security Standards Council (PCI SSC) afin de maintenir des référentiels communs tels que les référentiels d'exigences des programmes PCI DSS, PCI PA-DSS et PCI PED.

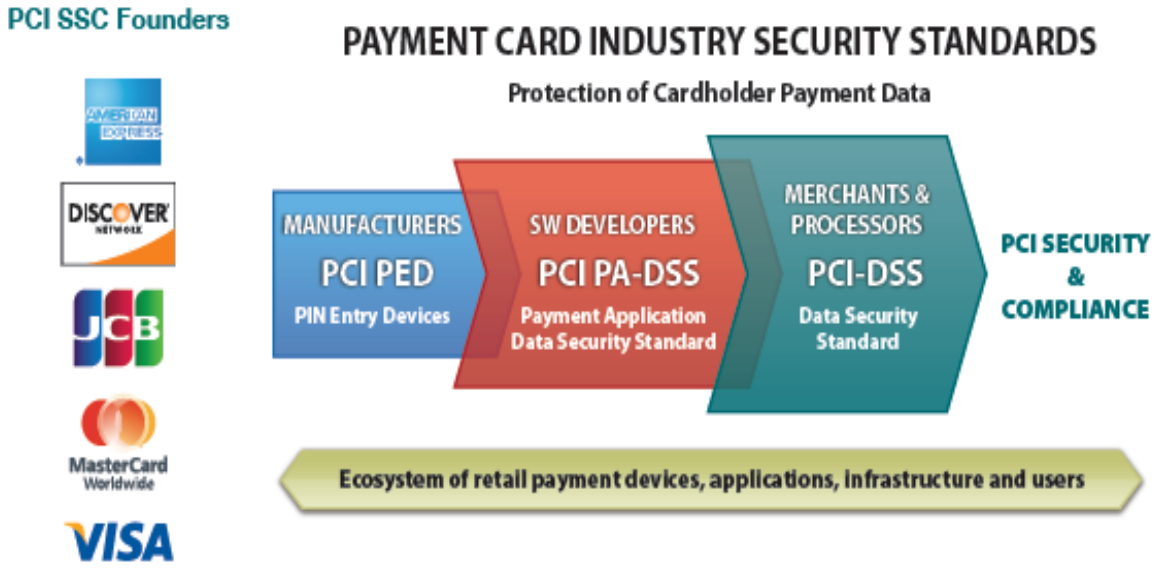
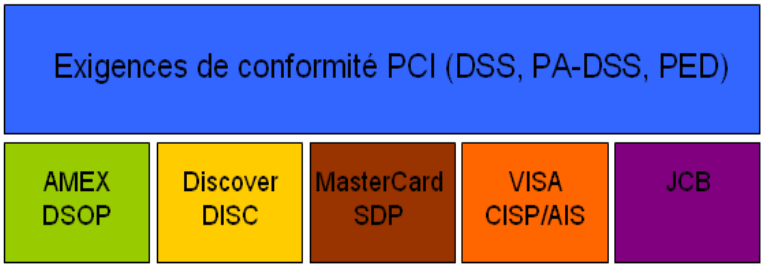


Figure 1 : source PCI SSC

Les exigences de conformité PCI sont en alignement avec les programmes de gestion des risques des réseaux cartes :

- American Express : Data Security Operating Policy (DSOP);
- Discover : Discover Information Security Compliance (DISC);
- JCB : Data Security Program ;
- MasterCard : Site Data Protection (SDP);
- Visa USA : Cardholder Information Security Program (CISP);
- Visa Europe : Account Information Security Program (AIS).



Si les réseaux se sont entendus pour définir une norme commune, ils gardent chacun la maîtrise de leurs risques. Chaque réseau a ainsi mis en place, dans le cadre de ses programmes

de gestion des risques, un programme spécifique chargé de la mise en application de la norme PCI-DSS au sein de son périmètre

Les **objectifs** du PCI SSC sont :

- Emettre et gérer le cycle de vie des standards PCI (PCI DSS, PCI PA-DSS, PCI PED) ;
- Améliorer la sécurité des paiements ;
- Susciter une prise de conscience et accélérer l'adoption des standards PCI ;
- Favoriser la participation des banques, marchands et *Payment Service Providers ;*
- Gérer le processus de qualification et de validation des QSA (Qualified Security Assesor), ASV (Approved Scan Vendor), et des laboratoires PED (Pin Entry Device) ;
- Maintenir les listes des QSA, ASV et PED certifiés.

Les **ressources** mises à disposition par le PCI SSC sont :

- Les standards PCI DSS, PCI-PA-DSS et PED-DSS et la documentation liée à ceux-ci :
  - PCI Data Security Standard ;
  - PCI DSS Security Audit Procedures ;
  - PCI DSS Security Scanning Procedures ;
  - PCI DSS Self Assessment Questionnaires (SAQ) ;
  - PCI PED Standard ;
  - PCI Payment Application Data Security Standard (PA-DSS).
- PCI SSC FAQ ;
- PCI SSC Education, ces cours s'adressent à l'ensemble des acteurs concernés ;
- Participation au PCI SSC (règles de fonctionnement, formulaire d'adhésion) ;

Ces documents sont disponibles sur le site Web du PCI SCC :
https://www.pcisecuritystandards.org

III.2 - Les réseaux cartes

Les réseaux cartes gèrent directement **:**

- Les modalités d'application des standards PCI ;
- Les frais, pénalités et échéances pour la conformité ;
- Le processus de validation ;
- L'approbation et publication des entités conformes à PCI DSS et PCI-PA-DSS ;
- La définition des niveaux des marchands et fournisseurs de services ;
- Les investigations (Forensics) et réponses aux compromissions.

Ces documents sont disponibles sur les sites Web des émetteurs de cartes :

http://www.visaeurope.com/aboutvisa/security/ais/aisprogramme.jsp

http://usa.visa.com/merchants/risk_management/cisp.html

http://www.mastercard.com/sdp/

http://www.americanexpress.com

http://www.discovernetwork.com/fraudsecurity/disc.html

http://www.jcb-global.com/english/jdsp/index.html

Voici une présentation synthétique des niveaux de marchands et de fournisseurs de services de paiement pour Visa, MasterCard et American Express prenant en compte les critères, les éléments nécessaires à la conformité ainsi que les acteurs qui doivent fournir ou valider ces éléments. Ces critères étant sujets à évolution, il est conseillé de se référer aux sites de différents réseaux cartes.

En cas de doute, un marchand ne doit pas hésiter à contacter sa ou ses banque(s) acquéreur(s).

Marchands :

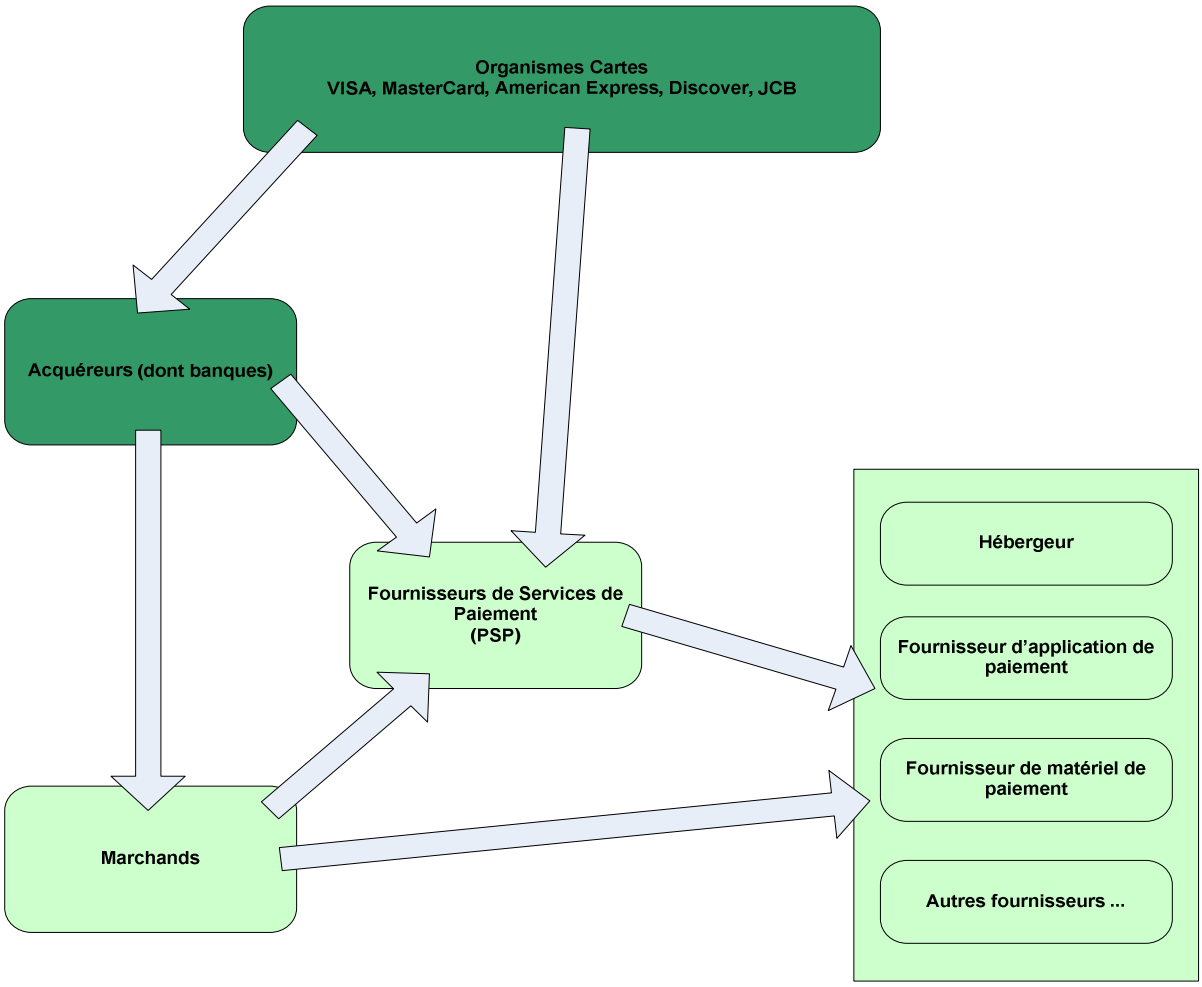
Type	Critères	Eléments nécessaires à la conformité :	Qui doit fournir/réaliser ces éléments :
• Marchand • (niveau 1)	Visa: plus de 6 M² (Millions) de transactions MasterCard: plus de 6 M² de transactions AMEX: plus de 2,5 M² de transactions JCB : plus de 1 M² de transactions DISCOVER : plus de 6 M² de transactions	• Audit sur site annuel récurrent • Scan ASV trimestriel	• QSA (Qualified Security Assessor) • ASV (Approved Scan Vendor)
• Marchand • (niveau 2)	Visa: 1 à 6 M² de transactions MasterCard: 1 à 6 M² de transactions AMEX: 0,05 M² à 2.5 M² de transactions JCB: moins de 1 M² de transactions	• Questionnaire annuel d'auto évaluation (SAQ) • Scan ASV trimestriel	• Marchand • ASV (Approved Scan Vendor)
• Marchand • (niveau 3)	Visa: e-commerce de 0,02 M² à 1 M² de transactions annuelles MasterCard: e-commerce de 0,02 M² à 1 M² de transactions annuelles AMEX: moins de 0,05 M² de transactions	• Questionnaire annuel d'auto évaluation (SAQ) • Scan ASV trimestriel	• Marchand • ASV (Approved Scan Vendor)
• Marchand • (niveau 4)	Visa: moins de 1M² de transactions tous canaux confondus ou moins de 0,02 M² de transactions e-commerce. MasterCard: tous les autres marchands.	• Questionnaire annuel d'auto évaluation (SAQ) • Scan ASV trimestriel	• Marchand • ASV (Approved Scan Vendor)

Fournisseurs de services de paiement (PSP) :

Type	Critères	Eléments nécessaires à la conformité :	Qui doit fournir/réaliser ces éléments :
• PSP • (niveau 1)	Visa: plus de 0,3 M² de transactions MasterCard: plus de 1M² de transactions AMEX : tous les PSP JCB: tous les PSP Discover: tous les PSP	• Audit sur site annuel récurrent • Scan ASV trimestriel	• QSA (Qualified Security Assessor) • ASV (Approved Scan Vendor)
• PSP • (niveau 2)	Visa: moins de 0,3 M² de transactions MasterCard: moins de 1 M² de transactions	• Questionnaire d'auto évaluation (SAQ) • Scan ASV trimestriel	• PSP • ASV

III.3 - Reports des contraintes PCI DSS entre les acteurs (schéma)

Les flèches indiquent le report de responsabilité d'un acteur sur un autre. Le rôle du QSA peut être d'accompagner ce report.



III.4 - Aperçu et cohérence des standards PCI

Le PCI Standard Security Council élabore et maintient l'ensemble de la documentation relative à la protection des données carte bancaires sur l'ensemble de la chaîne de paiement. Cette chaîne est différente selon que la carte est présente ou non et elle utilise différents maillons chez l'accepteur (le commerçant), l'acquéreur (la banque ou le fournisseur de services) ou le réseau de transport de la transaction.

A la fin 2009, PCI SSC maintient trois référentiels principaux qui s'appliquent aux trois maillons que sont le dispositif de saisie du code confidentiel, l'application de paiement et le système d'information gérant les données sensibles du porteur de carte bancaire.

Leurs dénominations sont les suivantes : (Cf. Fig1)

- PCI PED : PIN Entry Device ;
- PCI PA-DSS : Payment Application – Data Security Standard ;
- PCI DSS : Data Security Standard.

III.4.1 - PCI PED

Le référentiel PCI PED concerne les caractéristiques de l'équipement physique qui impactent la sécurité de la saisie du code confidentiel du porteur (PIN) lors d'une transaction de paiement. Ce référentiel concerne uniquement les constructeurs de dispositifs de saisie de code.

Les caractéristiques de sécurité portent principalement sur le clavier de saisie du code, l'enceinte contenant les clés cryptographiques, l'intégrité du firmware et l'afficheur.

Un constructeur de terminaux de paiement ou de bornes de distribution de produits peut intégrer un dispositif certifié PCI PED.

III.4.2 - PCI PA-DSS

Le référentiel PA-DSS s'applique aux sociétés ou prestataires qui développent des applications de paiement qui conservent, traitent ou transportent des données porteur dans le contexte des transactions d'autorisation ou de règlement, quand ces applications sont vendues ou distribuées à des tierces parties (il ne concerne pas les applications développées en un seul exemplaire pour un usage interne).

Ce référentiel rassemble un ensemble de règles de sécurité qui visent à minimiser les brèches de sécurité potentielles des applications de paiement.

Une application de paiement peut s'appuyer, entre autres, sur des composants de saisie de code PCI PED.

L'utilisation par un commerçant d'une application de paiement certifiée PA-DSS peut l'aider mais ne suffit pas à devenir conforme aux exigences PCI DSS.

III.4.3 - PCI DSS

Le référentiel PCI DSS s'applique aux systèmes d'information des différents acteurs de la chaîne de paiement, commerçant, banque acquéreur ou prestataire de services de paiement. Le SI concerné est celui qui conserve, traite ou transporte des données sensibles du porteur de carte. L'acteur concerné peut utiliser une application de paiement déjà certifiée PA-DSS afin de faciliter sa mise en conformité mais ceci ne suffit pas car des exigences complémentaires

portent en particulier sur les aspects de politique de sécurité de l'organisation et sur les habilitations des personnels.

Le référentiel PCI DSS V1.2 est constituée de 12 séries de clauses (exigences) réparties en 6 sections, formant ainsi 252 procédures de test avec contrôles (en place - pas en place - date cible / commentaires).

Création et gestion d'un réseau sécurisé
1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes. 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.
Protection des données des titulaires de cartes de crédit
3. Protéger les données des titulaires de cartes stockées. 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.
Mise à jour d'un programme de gestion des vulnérabilités
5. Utiliser des logiciels antivirus et les mettre à jour régulièrement. 6. Développer et gérer des systèmes et des applications sécurisés.
Mise en oeuvre de mesures de contrôle d'accès strictes
7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître. 8. Affecter un ID unique à chaque utilisateur d'ordinateur. 9. Restreindre l'accès physique aux données des titulaires de cartes.
Surveillance et test réguliers des réseaux
10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes. 11. Tester régulièrement les processus et les systèmes de sécurité.
Gestion d'une politique de sécurité des informations
12. Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants.

Figure 2 : Les 6 sections et les 12 séries de clauses de PCI DSS version 1.2

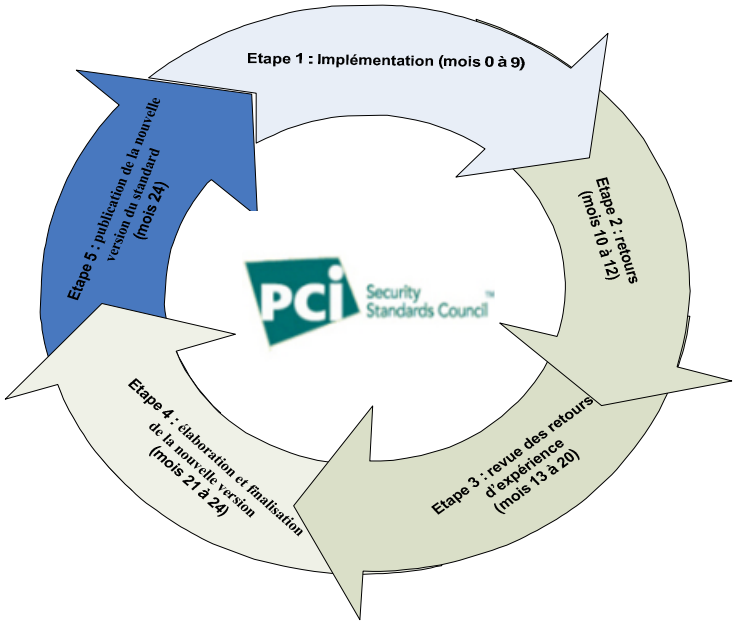
Clauses PCI DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
1.1 Définir des normes de configuration des pare-feu et des routeurs incluant les éléments suivants :	**1.1** Obtenir et vérifier les normes de configuration des pare-feu et des routeurs et autres documents spécifiés ci-dessous pour vérifier que les normes sont bien satisfaites. Procéder comme suit :			
1.1.1 Processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs	**1.1.1** Vérifier qu'un processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs est en place.			
1.1.2 Schéma de réseau actuel indiquant toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil	**1.1.2.a** Vérifier qu'il existe un schéma de réseau actuel (par exemple, illustrant les flux des données des titulaires de cartes) et que celui-ci indique toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil.			
	1.1.2.b Vérifier que le schéma est tenu à jour.			
1.1.3 Exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne	**1.1.3** Vérifier que les normes de configuration des pare-feu comprennent l'exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée et la zone de réseau Internet. Vérifier que le schéma de réseau actuel est conforme aux normes de configuration des pare-feu.			

Figure 3 : extrait des « Conditions et procédures d'évaluation de sécurité » PCI DSS version 1.2 (source : https://www.pcisecuritystandards.org/pdfs/pci_dss_french.pdf)

IV - Cycle de vie du standard PCI DSS

Le standard PCI DSS est actuellement dans sa révision 1.2 qui date d'octobre 2008.

Le standard PCI DSS suit des cycles de 24 mois qui se décomposent comme suit :



IV.1 - Etape 1 – Implémentation – mois 1 à 9

pour PCI DSS 1.2 : du 1/10/08 au 30/06/09

Les neuf premiers mois qui suivent la dernière révision du standard PCI DSS permettent la mise en place de celui-ci.

Cette période permet aux organisations d'adresser les changements apportés par cette nouvelle révision du standard. C'est durant cette étape que le PCI Council met à jour l'ensemble des documents en support du standard.

IV.2 - Etape 2 – Retours d'expérience – mois 10 à 12

pour PCI DSS 1.2 : du 1/07/09 au 30/09/09

Cette étape permet de prendre en compte des retours d'expérience qui participeront à l'évolution du standard à travers un processus formel.

IV.3 - Etape 3 – Revue des retours d'expérience – mois 13 à 20

pour PCI DSS 1.2 : du 1/10/09 au 31/05/10

Durant cette étape qui dure 8 mois, le PCI SSC compile des retours de la part de toutes les parties prenantes (organisations participantes, QSA, ASV, Board of Advisor, communauté).

Le groupe de travail technique du PCI SSC analyse ces retours et en fonction de ceux-ci prend l'une des mesures suivantes :

- Aucune action : si le retour n'est pas jugé pertinent ;
- Réalisation de documents complémentaires permettant de supporter la version actuelle (complément de FAQ, whitepaper, suppléments d'informations …) ;
- Edition d'une nouvelle révision de PCI DSS (eg : version 1.3) ;
- Edition d'une nouvelle version de PCI DSS (eg : version 2.0).

IV.4 - Etape 4 – Elaboration et finalisation de la nouvelle version – mois 21 à 24

pour PCI DSS 1.2 : du 1/06/10 au 30/09/10

Cette quatrième étape permet au PCI SSC de finaliser la nouvelle version ou révision de PCI DSS en vue de sa publication. Le PCI SSC fournit une liste des modifications (summary of changes) à la communauté ainsi que la date de publication de cette nouvelle version ou révision.

IV.5 - Etape 5 – Publication de la nouvelle version du standard

Cette dernière étape clôt le cycle par la publication de la nouvelle version du standard. Le cycle peut reprendre pour une nouvelle version.

V - Périmètre d'application du standard PCI DSS

V.1 - Définition du périmètre PCI DSS

Pour les entreprises soumises au standard PCI DSS, le périmètre d'application inclut tous les composants réseaux, systèmes et applicatifs qui traitent, stockent ou supportent les données des porteurs de carte ainsi que les éléments connectés à ceux-ci.

De ce fait, les éléments suivants sont impactés :

- Tous les systèmes, les serveurs, les applications ou les composants réseaux inclus dans, ou reliés à l'environnement de données de détenteurs de carte :
    - Les composants réseau, notamment les firewalls, les commutateurs, les routeurs, les points d'accès sans fil, les équipements de réseau, et les autres équipements de sécurité ;
    - Les serveurs, notamment les serveurs Web, de bases de données, d'authentification, de DNS, de courrier, et de synchronisation horaire (NTP) ;
    - Les applications, que ce soit les applications développées en interne ou les progiciels, qu'elles soient accessibles en interne ou externe.
- Tous les utilisateurs et postes utilisateurs accédant à ces composants, que ce soit pour des besoins métiers ou informatiques, depuis les points de vente, les datacenter ou des bureaux ;
- Tous les raccordements à l'environnement des données de porteur de carte, par exemple : accès à distance des employés, passerelles de paiement, banques, entreprises de cartes de paiement, centres d'appels, accès de tiers pour traitement, et tierce maintenance.

Ce dernier point fait apparaître la notion d'entreprises externes (type fournisseurs, partenaires, mainteneurs réseau/système/applicatif…) qui peuvent accéder logiquement ou physiquement à l'environnement des données des porteurs de cartes et peuvent donc éventuellement en affecter la sécurité en accédant par exemple à des numéros de cartes. Si ces entreprises ne respectaient pas les règles de sécurité demandées par le standard, elles pourraient constituer un maillon faible. Ces entreprises sont donc incluses dans le périmètre PCI DSS sous la notion de « Fournisseurs de Services » décrite plus loin.

V.2 - Echantillonnage

Les audits sur site et les scans depuis Internet ne portent pas sur la totalité du périmètre PCI DSS de l'entreprise, notamment pour des raisons de coût. Il existe donc la notion de « périmètre PCI DSS » déjà abordée et la notion « d'échantillon d'audit » que nous allons maintenant présenter.

Voici la définition de l'échantillonnage, telle qu'elle est proposée dans la version 1.2 du PCI DSS :

« L'évaluateur peut sélectionner des échantillons représentatifs des installations de l'entreprise et des composants du système en vue d'évaluer leur conformité aux clauses du standard PCI DSS.

Ces échantillons doivent inclure aussi bien des installations de l'entreprise que des composants du système, ils doivent représenter une sélection de tous les types et emplacements des installations de l'entreprise ainsi que des types de composants du système, et ils doivent être suffisamment nombreux pour garantir à l'évaluateur que les mesures de sécurités sont mises en œuvre comme prévu.

Les installations de l'entreprise comprennent, par exemple, les bureaux, les magasins, les commerçants franchisés et les installations à différents emplacements. L'échantillonnage doit inclure les composants du système de chaque installation de l'entreprise. Par exemple, pour chaque installation de l'entreprise, il convient d'inclure divers systèmes d'exploitation, fonctions et applications liés au domaine évalué. Au sein de chaque installation de l'entreprise, l'examinateur peut choisir les serveurs Sun exécutant le navigateur Web Apache, les serveurs Windows exécutant Oracle, les systèmes mainframe exécutant les applications traditionnelles de traitement de cartes, les serveurs de transfert de données exécutant HP-UX et les serveurs Linux exécutant MYSQL. Si toutes les applications s'exécutent à partir d'un système d'exploitation unique (par exemple, Windows ou Sun), l'échantillon doit tout de même inclure diverses applications (par exemple, serveurs de bases de données, serveurs Web et serveurs de transfert de données).

Lorsqu'ils choisissent des échantillons d'installations d'entreprise et de composants de système, les évaluateurs doivent prendre en compte les facteurs suivants :

- *Si chaque installation est tenue de respecter des processus PCI DSS obligatoires standard, l'échantillon peut être plus petit que celui nécessaire en l'absence de processus standard, afin de garantir que chaque installation est configurée conformément au processus standard.*
- *Si plusieurs types de processus standard sont en place (par exemple, pour différents types de composants du système ou d'installations), l'échantillon doit alors être suffisamment diversifié pour inclure les composants du système ou les installations sécurisés avec chaque type de processus.*
- *Si aucun processus PCI DSS standard n'est en place et si chaque installation est responsable de ses propres processus, l'échantillon doit être encore plus important de manière à s'assurer que chaque installation comprend et applique correctement les clauses du standard PCI DSS. »*

L'uniformisation des configurations et des architectures prend alors toute sa valeur, puisqu'elle permet de démontrer beaucoup plus simplement la conformité du périmètre PCI DSS de l'entreprise.

Il est également à noter que l'échantillon peut être revu à la hausse en cours d'audit si l'auditeur découvre un niveau d'homogénéité moindre que celui initialement escompté.

Il est important de noter que le choix de l'échantillon et de la taille de l'échantillon est de la responsabilité de l'auditeur. Le rapport de conformité doit préciser l'échantillon retenu et les raisons du choix de cet échantillon dans le respect du cadre défini par le standard.

V.3 - Les scans ASV

Ces scans doivent être réalisés par une entreprise agréée ASV (Approved Scan Vendor). La liste de ces entreprises est disponible sur le site du PCI SSC.

Le standard PCI DSS prévoit que toutes les adresses IP de l'entreprise visibles depuis Internet doivent faire l'objet d'un scan trimestriel destiné à détecter les vulnérabilités potentielles.

L’objectif est de minimiser les risques d’intrusion depuis Internet vers les systèmes contenant les données carte.

De manière générale, les méthodes de segmentation ci-après peuvent être utilisées pour réduire le périmètre du scan de sécurité ASV :

- la mise en œuvre d’une séparation physique entre le segment gérant les données de titulaire de carte et d'autres segments ;
- le recours à une segmentation logique appropriée lorsque tout trafic est interdit entre le segment ou réseau gérant des données de porteur de carte et d'autres réseaux ou segments.

Il incombe en dernier ressort aux commerçants et aux fournisseurs de services de valider le périmètre de leur scan de sécurité PCI en cohérence avec les procédures de scans.

Si une atteinte à la sécurité des données d’un compte survient par le biais d’une adresse IP ou d’un composant qui n’est pas inclus dans le balayage, le commerçant ou le prestataire de services est responsable.

VI - Réduction du périmètre PCI DSS

VI.1 - Principes de réduction du périmètre PCI DSS

La réduction du périmètre d'application du standard PCI-DSS consiste à identifier les 5 à 10% des composants du SI qui manipulent réellement des données sensibles de façon à réduire le périmètre du SI à auditer.

Afin de réduire le périmètre de PCI DSS, plusieurs actions sont mises en œuvre séparément ou conjointement :

- Isoler les applications et composants qui manipulent des données sensibles à l'aide d'un cloisonnement approprié (voir plus loin) ;
- Chiffrer les flux afin de permettre d'exclure tous les composants intermédiaires du réseau (switchs, routeurs) du périmètre. Exemples : IPSec ou SSL utilisés pour chiffrer les échanges entre serveurs ou entre les postes clients et les serveurs ;
- Tronquer le PAN de façon à le rendre inexploitable (supprimer du PAN les chiffres significatifs) ou le remplacer par un identifiant unique (par exemple un hash). Les applications qui utilisent ou stockent cette valeur tronquée sont alors exclues du périmètre PCI DSS. En France, pour tronquer un PAN, il faut garder les six premiers chiffres et les quatre derniers, ce qui peut être différent pour d'autres réglementations ;
- Masquer l'affichage du PAN aux utilisateurs pour une application qui le stocke de façon intégrale (en France, n'afficher que les six premiers chiffres et les quatre derniers) permet d'exclure l'environnement des postes clients qui n'ont alors plus accès aux données sensibles ;
- Chiffrer les données dans les bases de données d'un point de vue applicatif permet de réduire le périmètre concernant les administrateurs. L'application est toujours incluse dans le périmètre mais son exploitation est écartée ;
- Chiffrer ou tronquer les données dans les sauvegardes permet d'exclure le stockage des sauvegardes du périmètre d'audit ;
- Transférer le risque vers des prestataires externes en externalisant certaines prestations. L'entité doit néanmoins s'assurer contractuellement et par contrôle de la conformité de son prestataire. Il est important de vérifier que la responsabilité ainsi transférée au prestataire n'a plus besoin d'être assurée en interne. Dans le cadre d'un audit, le QSA devra pouvoir auditer le prestataire ;
- Utiliser des matériels et logiciels « certifiés » (essentiellement pour les terminaux de saisie des codes PIN ou certaines applications de paiement) afin de reporter la responsabilité sur ce prestataire (en ayant pris soin de formaliser sa conformité et un droit d'audit).

Pour rappel, le standard PCI DSS se focalise sur les risques de capture en masse de données sensibles. C'est-à-dire qu'un poste isolé en centre d'appel qui ne peut capturer qu'une donnée isolée suite à l'appel d'un utilisateur mais ne peut pas extraire des données d'une application est exclu du périmètre d'audit.

La réduction du périmètre implique de revoir les processus métiers car très souvent le numéro de carte est utilisé par commodité ou habitude et non par besoin.

La mise en œuvre de PCI DSS est l'opportunité de revoir cette utilisation et de remplacer le PAN par un masquage (relation client en général) ou bien par un hash unique (réconciliation financière ou Back Office par exemple) et par là même de réduire les risques.

VI.2 - Notion de segmentation réseau appropriée

Le périmètre PCI DSS inclut donc tous les systèmes connectés au même segment réseau que l'environnement des données porteur. Ceci peut éventuellement inclure des systèmes « annexes » qui ne traiteraient aucunement de données cartes mais qui seraient simplement sur le même LAN.

On comprend qu'avec cette définition, si une entreprise dispose d'un réseau interne « à plat » (i.e. non cloisonné), alors la totalité de son système d'information pourrait se retrouver inclus dans le périmètre PCI DSS. Ceci n'est absolument pas le but recherché par le standard.

Rappelons que l'objectif de ce standard est de sécuriser les données cartes contenues dans le système d'information et non l'intégralité de celui-ci.

Alors pourquoi imposer toutes les exigences du standard à ces systèmes « annexes » alors qu'ils ne traitent pas de données cartes et ne risquent donc pas de se les faire voler ? En réalité, l'objectif est de limiter les risques de rebond depuis ces systèmes « annexes » vers les systèmes manipulant les données cartes.

En effet, dans de nombreux cas réels de compromissions de données par des pirates, ceux-ci sont passés dans un premier temps par des serveurs « annexes » moins sécurisés pour rebondir ensuite vers les serveurs manipulant les données cartes.

Ceci est par exemple le cas des codes malveillants ciblés (vers) ayant pour but de chercher l'information (coordonnées bancaires) et de la transférer vers des personnes malintentionnées.

Néanmoins, la mise en conformité de ces systèmes annexes n'est pas toujours souhaitée (pour des raisons de coût, contraintes métier…) et le standard offre la possibilité de les exclure du périmètre PCI DSS en mettant en place une « segmentation réseau appropriée » entre ces systèmes et les systèmes contenants les données de porteur de carte. Cette segmentation doit permettre d'isoler les serveurs PCI DSS sensibles de ces autres systèmes annexes. Les risques de rebond précédemment mentionnés sont alors réduits.

Sous réserve de la mise en place d'une segmentation réseau appropriée, l'expérience montre que le périmètre PCI DSS ne devrait représenter plus de 5 à 10% du système d'information de l'entreprise.

Néanmoins, ce cloisonnement peut représenter à lui seul des chantiers très conséquents. Les firewalls ont un coût initial et récurrent (maintien à jour des équipements et gestion des règles de filtrage) non négligeable. Certaines structures avec de nombreux points de vente peuvent être confrontées à de très gros chantiers. Il est alors parfois tentant d'utiliser des systèmes existants en leur rajoutant quelques règles de filtrage pour apporter un premier niveau de cloisonnement. Jusqu'où peut-on aller dans les compromis technologiques tout en restant dans les limites d'une « segmentation réseau appropriée » demandée par le standard sans pour autant se laisser aller à des solutions « rustines » difficilement maintenables dans le temps ?

Le standard ne précise pas techniquement cette notion de « segmentation réseau appropriée » et laisse une part importante à l'appréciation de l'auditeur sur l'efficacité des technologies pouvant être employées pour atteindre ce but.

Parmi les technologies envisageables, on retrouve les firewalls dits « stateful », les proxy applicatifs, les routeurs avec ACL, les VLAN, les VRF pour les réseaux MPLS, voire des tunnels IPSEC/SSL pour chiffrer les données sur un segment du réseau qui n'aurait pas besoin d'accéder aux données en clair… Toutes ces technologies n'ont pas les mêmes objectifs, ni le même niveau de sécurité et l'évaluation de leur efficacité pour réaliser une « segmentation réseau appropriée » est très spécifique au contexte du marchand. Le standard conseille de se rapprocher d'un auditeur certifié QSA pour faire valider que la méthodologie de mise en œuvre des solutions permet de répondre aux exigences du standard.

VI.3 - Fournisseurs de services et reports de responsabilités

Le marchand peut sous-traiter certaines tâches à une entreprise externe telles que :

- Opérations liées à la monétique : le stockage, le traitement ou la transmission des données des titulaires de cartes. Ceci inclut les fournisseurs, partenaires, fournisseurs de services monétiques, passerelles de paiement, services postaux en charge de version papier des données cartes, entreprise stockant les sauvegardes sur bande ;
- Opérations pouvant impacter la sécurité de l'environnement des données de porteur de carte : ceci inclut les fournisseurs de « services managés » en charge de l'exploitation et surveillance des firewalls, IDS, réseaux, systèmes, applicatifs, bases de données… Globalement, ceci inclut tous les tiers qui accèdent à l'environnement des données de porteurs de cartes.

Si ces fournisseurs de service ne respectaient pas les règles de sécurité demandées par le standard, ils pourraient constituer un maillon faible dans la sécurité des données des porteurs de carte. Ces entreprises sont donc incluses dans le périmètre PCI DSS sous la notion de « Fournisseurs de Services ». Elles ont l'obligation de se mettre en conformité avec le standard dans le cadre de leurs interventions sur le marchand en question. Cette obligation doit apparaître formellement dans le contrat de services avec le marchand.

Il existe deux options de validation de la conformité des prestataires de services tiers :

- ils peuvent procéder à leur propre évaluation PCI DSS et en apporter la preuve à leurs clients pour démontrer leur conformité ;
- s'ils ne procèdent pas à leur propre évaluation PCI DSS, ils devront faire examiner leurs services pendant les évaluations PCI DSS de chacun de leurs clients.

En outre, les commerçants et les prestataires de services doivent gérer et contrôler la conformité au standard PCI DSS de tous les prestataires tiers qui ont accès aux données des titulaires de cartes auxquels ils sont associés.

En raison de ce caractère transitif (« les fournisseurs de mes fournisseurs sont mes fournisseurs ») et de la définition large du fournisseur de services (« toute entreprise qui pourrait accéder aux données cartes du marchand »), leur nombre peut devenir rapidement très important. L'identification de ces fournisseurs et le suivi de leur mise en conformité sont un chantier à part entière. Cette notion de fournisseur de services peut rapidement devenir un point majeur dans la mise en conformité de l'entreprise, surtout si ceux-ci ne sont pas très enclins à se mettre en conformité.

VI.4 - Dérogation pour certifications de périmètres spécifiques

Contrairement à la norme ISO 27001 qui permet de définir un périmètre du SMSI[1] comme un sous-ensemble d'une entreprise, la notion de périmètre dans PCI DSS est définie par des règles qui ne permettent pas de faire moins que le périmètre entrant dans le scope, ou a minima son environnement PCI éventuellement cloisonné.

Au sens strict du standard, il n'est donc pas possible pour une entreprise de faire certifier un certain produit ou service seul en marge du reste de l'entreprise. Une entreprise ne peut pas non plus « commencer par certifier telle ou telle partie de son SI » puis aborder la certification du reste ultérieurement.

Néanmoins, si on considère ces approches pragmatiques comme transitoires vers la certification totale, il apparaît qu'elles ont un sens puisqu'elles contribuent à diminuer les risques de fraude. Il y a donc un mécanisme prévu pour pouvoir aborder cette approche : il s'agit des négociations avec les banques acquéreur.

En effet, l'acceptation de ces certifications partielles relève de la notion de « mise en application du standard » (« *enforcement* » en anglais). Ce sont les banques et les réseaux internationaux qui sont responsables de cette partie du programme PCI DSS. Ce sont donc ces entités qui peuvent décider d'accepter une mise en conformité partielle de façon temporaire. Ce caractère transitoire est très important : il est fortement conseillé d'adjoindre un planning de mise en conformité totale de l'entreprise à ces demandes de dérogation.

VI.5 - Autres aspects concernant la réduction du périmètre

La mise en place d'un chiffrement impose de mettre en place une organisation pour gérer les clés de chiffrement. Pour cela, on peut par exemple s'appuyer sur une Infrastructure de Gestion de Clés Publiques (PKI en anglais).

La gestion des droits applicatifs permet de mettre en œuvre le cloisonnement opérationnel des rôles. Elle doit être précise et si possible séparée des droits d'accès au réseau hors du périmètre de PCI DSS.

En cas d'utilisation de comptes génériques, des mesures compensatoires doivent être mises en œuvre pour maîtriser les risques liés à l'absence de traçabilité de ces comptes (par exemple : connaître à un moment donné les opérateurs pouvant utiliser des comptes génériques).

L'application de PCI DSS est compatible avec les environnements virtualisés qui doivent faire l'objet d'une démarche adaptée auprès du QSA. Des mesures de sécurité doivent être mises en œuvre sur les interconnexions entre environnements virtualisés, les systèmes hôtes

[1] Système de management de la sécurité de l'information

(hyperviseurs) et les systèmes de contrôle (consoles). En particulier l'environnement hôte et les consoles de contrôles sont incluses dans le périmètre.

VI.6 - Responsabilité vis-à-vis des prestataires

Dans le cadre d'une externalisation des problématiques de systèmes d'information, un grand nombre de sociétés (en particulier les marchands) se tourne aujourd'hui vers des prestataires offrant des services allant de l'hébergement à l'installation, en passant par le support de premier niveau, le développement et le maintien en condition opérationnelle.

Les engagements entre le prestataire et son client sont en général couverts par des clauses de confidentialité, sans pour le moment, et si nécessaire, intégrer systématiquement des clauses ou des références à PCI DSS, ce qui va à l'encontre du standard. En effet, le standard mentionne dans sa condition 12.8.2 que l'accord de prestation doit intégrer la reconnaissance de responsabilités sur les données traitées.

On voit, dans des pays anglo-saxons, des offres « Data Center PCI Compliant » qui permettraient de rassurer les éventuels clients concernant les mesures prises par le Data Center pour héberger et traiter des données carte, tant sur les aspects organisationnels que sur les aspects techniques.

Cette référence de conformité permet aux prestataires de démontrer à leurs clients la gestion appropriée des informations cartes sensibles au sein de l'environnement externalisé.

Cependant la conformité d'un prestataire de services ne dédouane pas le marchand de sa responsabilité sur le sujet, il doit notamment référencer, sur le processus de gestion des cartes, la liste des prestataires, leurs champs d'activité, etc. – tout cela étant vérifié dans le cadre de l'audit annuel réalisé par le QSA au travers des conditions 12.8.x.

A ce jour, un prestataire (hébergeur par exemple) peut faire réaliser en son nom propre une évaluation de conformité qu'il peut présenter à ses clients comme preuve de sa gestion appropriée du processus de traitement cartes et qui sert de base à l'auditeur QSA – ou en cas de non validation ou conformité PCI DSS, le prestataire doit répondre à chaque demande de ses clients concernant ses processus de traitements des données carte dans le cadre des évaluations des marchands.

En bout de chaîne, l'appréciation du niveau de sécurité d'un environnement carte externalisé ou non, en reviendra toujours au QSA qui a la charge et la responsabilité dans son évaluation.

Le marchand qui externalise ce type de services porte toujours la responsabilité de la mise en conformité de la tierce partie – un QSA notant des faiblesses ou des contre-mesures non appropriées lors de son évaluation le reporte au client qui doit de son propre chef intervenir auprès de son prestataire pour que celui-ci se mette en conformité sous peine de non validation PCI DSS.

Pour mémoire, les contrôles s'appliquant à un marchand ayant externalisé des opérations incluant des processus cartes, sont présentés au chapitre 12.8 de la norme PCI DSS v1.2.

VII - Stratégie de conservation des données carte

La conservation des données carte est au cœur de PCI DSS, ainsi un pré-requis spécifique traite de ce sujet, il s'agit du chapitre 3 du standard.

VII.1 - Quelles données conserver ?

Les données autorisées en termes de stockage ainsi que les données dont le stockage est prohibé ont déjà été mentionnées dans le chapitre « Notions de données porteur ». Plusieurs points du chapitre 3 de PCI DSS concernent la vérification de ce principe au niveau documentaire mais aussi de son application sur le système d'information.

VII.2 - Motivation et durée de stockage de ces données

S'il est possible de conserver certaines données carte comme le PAN ou la date d'expiration de la carte, **il est nécessaire de réduire cette conservation à ce qui est strictement nécessaire et de justifier la durée de celle-ci**.

Ainsi le pré-requis 3.1 du standard PCI DSS demande que la politique de conservation des données sensibles traite des points suivants :

- Motivation du stockage et de sa durée en précisant le type de contrainte associée qu'elle soit légale, règlementaire ou liée à l'activité de l'entreprise (contrainte business forte) ;
- Précision sur la nécessité de supprimer la donnée une fois que celle-ci n'est plus nécessaire aux besoins cités ;
- Vérification que la politique de stockage adresse l'ensemble des stockages réalisés par l'entreprise ;
- Vérification que la politique prévoit un processus automatisé de suppression des données une fois que celles-ci ne sont plus nécessaires et que celui-ci est appliqué au moins trimestriellement.

VII.3 - Conditions de stockage et d'utilisation de ces données

Les données doivent être accédées conformément au strict besoin d'en connaître des utilisateurs du système d'information et être protégées de manière efficace.

Les données carte doivent être protégées dès lors qu'elles sont stockées, ainsi la mesure de sécurité 3.4 précise les mesures de protection acceptables pour ces données :

- Hachage unilatéral s'appuyant sur une méthode cryptographique robuste (one way strong hash including salt) ;
- Troncature : il s'agit ici de ne stocker que les données en respectant la même règle que pour le masquage ;
- Index tokens et Index pads (les pads doivent être stockés de manière sécurisée) ;
- Chiffrement robuste associé à des processus et à des procédures de gestion de clés.

Il faut donc privilégier le masquage, la troncature, et le hachage déjà évoqués dans le chapitre traitant de la réduction du périmètre car le stockage permettant une récupération de la donnée utilisable pour un paiement soulève un niveau de risque plus important et impose des contraintes strictes en particulier en termes de procédures de gestion de clés et de secrets.

VIII - Les mesures compensatoires

VIII.1 - Qu'est ce qu'une mesure compensatoire ?

Conscient du caractère très prescriptif du standard PCI DSS, le PCI SSC a prévu un mécanisme permettant aux entités concernées de répondre aux objectifs de sécurité recherchés avec la même rigueur, en utilisant une autre approche que l'approche initiale.

Les mesures compensatoires peuvent être utilisées lorsqu'un pré-requis est inapplicable pour une raison technique forte ou remet en cause le modèle économique de l'entreprise.

Il est en effet possible d'utiliser une mesure compensatoire pour toutes les exigences du standard, excepté la clause 3.2 : « Ne stocker aucune donnée d'authentification sensible après autorisation (même chiffrée) ».

Le principe est de proposer, pour certaines exigences jugées inapplicables dans un contexte particulier, des mesures de sécurité différentes et qui iraient globalement « plus loin » que les mesures initiales.

La validité d'une mesure compensatoire dans un contexte donné est encadrée par 4 conditions (voir ci-dessous) et est laissée à l'appréciation de l'auditeur QSA qui évalue la capacité de la mesure compensatoire à couvrir les risques.

Cette notion de mesure compensatoire renforce donc la notion d'analyse de risques dans la mise en œuvre et l'évaluation de la conformité PCI DSS.

Une fois par an, toutes les mesures compensatoires doivent être documentées, examinées et validées par l'auditeur, puis incluses dans le Rapport sur la Conformité. Les résultats de l'évaluation annuelle de ces mesures compensatoires doivent être documentés dans le Rapport de Conformité, dans la section de l'exigence PCI DSS correspondante. Ils font partie des informations pouvant être passées en revue dans le cadre des contrôles Qualité effectués par le PCI SSC.

VIII.2 - Conditions de légitimité d'une mesure compensatoire

Premièrement, des mesures compensatoires peuvent être envisagées lorsqu'une entité ne peut pas se conformer aux exigences PCI DSS telles qu'elles sont stipulées, soit :

1. en raison de contraintes commerciales documentées (coût excessif de la mise en œuvre face au risque à couvrir)

ou

2. de contraintes techniques légitimes et documentées.

L'une de ces raisons devra donc être démontrée lors de l'audit et réévaluée annuellement. En effet, le contexte peut changer et une contrainte légitime une année, peut disparaître l'année suivante. L'exigence initiale du standard PCI DSS devra alors être appliquée.

VIII.3 - Conditions de validité d'une mesure compensatoire

Ensuite, les mesures compensatoires doivent satisfaire aux 4 critères suivants :

1. Respecter l'intention et la rigueur de la clause initiale du standard PCI DSS ;
2. Fournir une protection similaire à celle de la clause initiale du standard PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par la clause initiale. On retrouve ici la notion d'analyse du risque initial ;
3. Aller au-delà des autres clauses PCI DSS. Les mesures compensatoires ne consistent pas simplement en la conformité avec d'autres clauses PCI DSS, il faut aller au-delà ;
4. Être proportionnelles aux risques supplémentaires qu'implique le non-respect de la clause PCI DSS. On retrouve ici le besoin de savoir calculer le risque résiduel.

VIII.4 - Illustration d'une mesure compensatoire

Il est très important de comprendre que l'exemple ci-dessous est une illustration en dehors de tout contexte.

Une appréciation des risques est spécifique à une entreprise, à un contexte, à un moment, et à ce titre, n'est pas transposable automatiquement d'une entité à une autre. De même, une mesure compensatoire n'est pas valable pour toute entité indépendamment de son contexte, ni transposable aveuglément. Il ne semble pas pertinent à ce titre de construire un « référentiel des mesures compensatoires » avec des formules « clefs en mains » valables partout. C'est également pourquoi une mesure compensatoire peut être valable pour un concurrent et pas pour votre entité.

C'est pour cela que le PCI SSC n'endosse aucune mesure compensatoire générique, et laisse systématiquement l'auditeur QSA les évaluer dans le contexte de leur client.

Voici donc un exemple de mesure compensatoire qui pourrait être valide dans un certain contexte : (extrait de PCI DSS 1.2)

« Exigence impactée : §8.1 - Tous les utilisateurs sont-ils identifiés avec un nom d'utilisateur unique qui les autorise à accéder aux composants du système ou aux données de titulaires de cartes ?

1. Contraintes – La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « root ». La société XYZ ne peut pas gérer le nom d'utilisateur « root » ni consigner toutes les activités de chaque utilisateur « root » ;
2. Objectif - L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des informations d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière ;

3. Risque identifié - L’absence d’identifiant utilisateur unique et le fait de ne pas pouvoir tracer les informations d'identification introduisent des risques supplémentaires dans le système de contrôle d’accès ;
4. Définition des mesures compensatoires - Une société XYZ va demander à tous les utilisateurs de se connecter aux serveurs à partir de leur environnement à l’aide de la commande SU. Cette commande autorise les utilisateurs à accéder au compte « root » et à exécuter des actions sous ce compte, tout en permettant de consigner leurs activités dans le répertoire du journal SU. Il est ainsi possible de suivre les actions de chaque utilisateur utilisant le compte « root » par ce biais ;
5. Validation des mesures compensatoires - La société XYZ démontre à l'évaluateur l’exécution de la commande SU et lui montre que celle-ci permet d’identifier les utilisateurs connectés qui exécutent des actions sous le compte « root » ;
6. Gestion - La société XYZ décrit les processus et les procédures mis en place pour éviter la modification, l’altération ou la suppression des configurations SU de sorte que des utilisateurs individuels puissent exécuter des commandes root sans que leurs activités soient consignées ou suivies ».

IX - PCI DSS, vérités et contre vérités

IX.1 - Matériel ou logiciel « certifié » PCI DSS

Si des logiciels ou des équipements sont vendus comme conformes PCI DSS, cela n'implique pas une conformité automatique pour celui qui utilise ces éléments.

En effet, si le matériel ou le logiciel ne doit pas intrinsèquement empêcher la conformité, c'est l'utilisation de celui-ci qui est soumise aux mesures de sécurité, il est donc impropre de dire qu'un logiciel ou matériel est PCI DSS.

A noter que dans certains cas très précis le matériel est soumis à PCI-PED, et le logiciel à PA-DSS.

IX.2 - Débat EMV contre PCI DSS

EMV a été mis en place pour réduire la fraude au niveau des points de paiement vis-à-vis des cartes contrefaites (Fraudes technologiques, celles-ci concernent des volumes plutôt faibles).

PCI DSS a été mis en place dans la même optique pour la partie piste, mais adresse surtout la fraude liée au traitement (pendant et surtout après transaction). PCI DSS adresse des fraudes massives.

Les risques identifiés par chaque standard étant différents, les mesures demandées le sont également, même si un certain niveau de recouvrement peut-être identifié (protection des données lors de la transaction 'carte présente').

Un système de paiement EMV n'est pas exempté de la protection des données carte hors du point de paiement.

Concernant la comptabilisation des transactions, le principe de déduire le nombre de transactions EMV du nombre total de transactions pour évaluer le niveau de marchand peut-être pertinent dans le cas ou ces données ne sont pas stockées. Aucun organisme carte n'a à ce jour statué clairement concernant ce point.

Si ce débat peut se comprendre concernant les motivations des investissements liés à la sécurité ces dernières années, il n'est techniquement pas fondé.

IX.3 - Fraude déclarée

Les informations obtenues sur les fraudes de type vol de données cartes sont biaisées du fait que certains pays ont l'obligation légale de déclarer ce type de fraude, ce qui n'est pas le cas en France.

Des fraudes avérées de type vol de données carte existent en France et en Europe, cependant ces informations ne sont pas divulguées et aucune statistique officielle n'est disponible à jour.

X - Liens avec les autres normes, standards, référentiels et réglementations

X.1 - ISO 27001

PCI DSS à la différence de l'ISO 27001 peut être considéré comme le résultat d'une analyse de risques effectuée par les organismes cartes. L'ISO est assez souple quant au périmètre, aux mesures de sécurité, à la conformité et à la mise en place. En effet, il a été construit de façon à pouvoir s'adapter à des entreprises d'activités très différentes et à des risques variés. Son but premier est d'adresser l'organisation de la sécurité. PCI DSS concerne quant à lui le niveau de sécurité lié à la carte bancaire.

Les exigences et pré-requis PCI DSS sont obligatoires, alors qu'avec ISO 27001 les mesures de sécurité sont suggérées - laissant ainsi à chaque organisation - la possibilité de décider des mesures de sécurité à mettre en place en fonction de sa sensibilité aux risques. Comparées aux mesures de sécurité de l'ISO 27001, celles de PCI DSS sont plus spécifiques. En théorie cette granularité permet un audit plus simple sur PCI DSS que pour ISO 27001.

Quand on se pose la question d'une certification ISO 27001, le planning peut permettre d'obtenir une conformité ISO et PCI avec un seul effort de mise en place. En effet, il existe un certain nombre de complémentarités entre ces deux approches pour autant que le périmètre du SMSI englobe au moins celui de PCI DSS et que les mesures de sécurité sélectionnées lors de l'élaboration de la Déclaration d'Applicabilité (DdA) contiennent celles de PCI DSS. Ainsi une démarche commune permettra un grand nombre de synergies et donc des économies importantes à condition de bien comprendre et de maîtriser les différences entre les deux approches.

Différences entre ISO 27001 et PCI DSS

Différences	PCI DSS	ISO 27001
Sélection des mesures de sécurité	Imposée	Principalement basée sur l'appréciation des risques
Niveau de granularité	Important	Libre
Niveau de flexibilité	Faible	Important
Périmètre	Défini par le standard	Défini par l'audité
Exigibilité	Contrainte externe	Démarche spontanée
Objectif principal	Niveau de sécurité de la carte bancaire	Organisation de la sécurité
Aide au management du SI	Faible contribution	Contribution majeure

X.2 - Cobit, ITIL et ISO 27002

Cobit n'est en effet pas à comparer à PCI DSS, mais peut en revanche être utilisé pour mettre en œuvre un modèle de maturité et mesurer l'état de sa conformité aux exigences PCI DSS. Outre la capacité de mesurer sa conformité, les processus Cobit identifiés peuvent être

intégrés dans une démarche d'audit interne dans le cadre du maintien de sa conformité aux exigences par exemple, et ou mutualisés à une démarche existante pour répondre aux exigences de contrôles internes.

Le tableau de l'annexe 2 permet d'identifier quels contrôles ou mesures de sécurité Cobit, ITIL et ISO 27002 couvrent les exigences PCI DSS afin de rationnaliser ces dernières (et de ne pas créer de nouveaux contrôles et donc de rationnaliser les coûts de mise en conformité par exemple). Enfin une démarche Cobit permet d'adopter la démarche processus absente de PCI DSS, et de bénéficier de l'organisation et du pilotage de la sécurité que peut apporter Cobit dans une démarche globale.

X.3 - CNIL et autres lois

Le vol de données informatiques est encadré sur le plan légal par la loi Loi n° 88-19 du 5 Janvier 1988 - dite loi Godfrain - qui a modifié le code pénal dans le titre II du livre III en insérant un chapitre III, articles 462-2 à 462-9 sur les infractions en matière informatique.

Au titre de ces articles, l'accès et le maintien dans un système d'information d'une entité non autorisée est répréhensible en particulier s'agissant de la modification ou de la suppression. Le vol en lui même, à savoir une copie n'altérant pas les données, n'est abordé qu'au sens de l'article 162-6 en évoquant […] l'usage de documents informatisés […] de nature à causer un préjudice à autrui.

La loi n° 78-17 du 6 Janvier 1978, modifiée par la loi n° 88-227 du 11 mars 1988, article 13 relative à la transparence financière de la vie politique (J.O. du 12 mars 1988), concerne la protection des données personnelles. Cette loi est la plus proche des intentions du programme PCI DSS sachant que les données sensibles cartes bancaires sont bien considérées par la CNIL comme des données indirectement nominatives.

Quiconque ayant volé des données carte tombe donc sous le coup de ces deux lois.

Notons qu'en aucun cas les exigences de PCI DSS, règles purement de droit privé, ne peuvent se substituer à la loi en vigueur sur le sol français. A ce titre le dépositaire des données sensibles doit se conformer aux exigences dictées par la CNIL afin de protéger, selon les critères clairement établis, les données sensibles des porteurs de cartes.

X.4 - Référentiels techniques

De nombreux organismes fournissent des référentiels de sécurité et en particulier des procédures de sécurisation techniques des systèmes d'exploitation, des serveurs d'application et des applications et réseaux.

Ce chapitre présente quelques uns de ces organismes qui proposent des documents de sécurisation utiles pour votre démarche PCI DSS.

- L'OWASP (Open Web Application Security Project) est une organisation à but non lucratif dont l'objectif est la promotion de méthodes et d'outils de conception et de développement sécurisés dont des outils d'audit et de formation. Elle maintient en particulier un top 10 des principales erreurs de développement rencontrées avec les mesures de sécurité associées.

  https://www.owasp.org/images/a/a4/OWASP_Top_10_2007_-_French.doc

http://www.owasp.org/

- Le SANS (SysAdmin, Audit, Network, Security) Institute : organisme qui fournit des ressources et des formations de sécurité informatique

  www.sans.org.

- le NIST (Network Information Security & Technology News) : site de nouvelles sur les technologies et la sécurité des SI

  http://www.nist.org/

- le CIS (Center for Internet Security) : entreprise à but non lucratif de promotion de la sécurité sur Internet

  http://www.cisecurity.org/

- Les principaux constructeurs et éditeurs (ex : Cisco, IBM, Microsoft, Oracle, SAP, Sun) fournissent également des documentations pour leurs solutions, parfois ils ont même été jusqu'à faire évaluer celles-ci. A noter, comme cela a déjà été évoqué que c'est l'implémentation de la solution qui est conforme et non une brique logicielle ou matérielle en elle-même.

XI - Avantages, difficultés et limites d'une démarche PCI DSS

PCI DSS est un standard de conformité, son application par les sociétés est le fruit d'une relation le plus souvent contractuelle entre les différents acteurs. Conformité n'est pas forcément synonyme de sécurité; comme les autres standards, normes ou référentiels, il doit être manié avec doigté; à défaut il risque d'être détourné de son but initial et pourrait même s'avérer contre productif.

XI.1 - Avantages

Plusieurs avantages liés à une telle démarche peuvent être identifiés, on peut citer par exemple :

- Le caractère obligatoire et la rigidité des mesures peut permettre de débloquer des projets de sécurité déjà identifiés par les opérationnels et RSSI mais jusque là repoussés pour des raisons d'économies plus liées au contexte économique qu'à la gestion des risques.
- Comme cela a été identifié dans le chapitre traitant des normes, standards, référentiels et réglementation, PCI DSS peut s'inscrire dans une démarche globale et cohérente de sécurisation des systèmes d'information.
- Dans le cadre de systèmes d'information jeunes ou à bâtir, PCI DSS présente un référentiel de sécurité monétique.

XI.2 - Difficultés

Les difficultés liées à l'implémentation de PCI DSS sont de plusieurs ordres parmi lesquels :

- Le délai exigé par les organismes ne permet pas forcément d'inscrire les contraintes liées à PCI DSS dans le cycle de vie initial des projets de l'entreprise. Il faut alors s'engager dans une négociation qui peut s'avérer plus ou moins complexe avec celui qui exige cette conformité ;
- PCI DSS nécessite parfois une adaptation non négligeable du système d'information et des métiers, comme cela a déjà évoqué dans le chapitre traitant de la réduction du périmètre ;
- Les mesures compensatoires nécessitent une anticipation en amont de l'audit, car les conditions de validité sont strictes et évaluées par le QSA, dans le cadre de l'audit, qui engage sa responsabilité.

XI.3 - Limites

Comme toute démarche de standardisation, PCI DSS a ses limites :

- PCI DSS est un standard unique qui s'applique à l'ensemble des entreprises qui traitent des données carte indépendamment de leur secteur d'activité ;
- L'agrément n'est pas une garantie absolue contre l'ensemble des menaces de vol, compromission ou fraude.

XII - Conclusion du document

Ce document de présentation du standard PCI-DSS vise à apporter la compréhension nécessaire pour aborder un tel projet dans son entreprise.

Les sujets orientés mise en œuvre pratique ont été volontairement écartés, tel que l'approche par priorité ou des aspects techniques qui pourront être développé ultérieurement.

Le groupe de travail accueillera toute remarque ou suggestion à l'adresse : doc-pcidss@clusif.asso.fr.

XIII - Annexe 1 : Glossaire

XIII.1 - Termes PCI DSS

- ASV (Approved Scanning Vendor) : prestataire autorisé par le PCI SSC pour la réalisation de recherches automatisées de vulnérabilités sur des machines connectées à un réseau public ;
- PCI (Payment Card Industry) : acteurs qui interviennent dans l'industrie de paiement par carte (banques, prestataires de paiement, émetteurs de carte, commerçants) ;
- PCI SSC (PCI Security Standards Council) : organisme responsable du maintien des standards PCI DSS, de leur promotion et de leur encadrement ;
- PCI DSS (PCI Data Security Standard) : standard de sécurité qui s'applique aux systèmes d'informations qui manipulent des données sensibles au sens PCI (essentiellement les données des porteurs de carte comme le numéro de carte) ;
- PCI PA-DSS (ou appelé PA-DSS) (PCI Payment Application Data Security Standard) : variante du standard PCI DSS qui s'applique aux applications de paiement ;
- PCI PED (PCI Pin Entry Device Data Security Standard) : variante du standard PCI DSS qui s'applique aux périphériques de saisie du code PIN qui protège les cartes de paiement ;
- PSP (Payment Service Provider) : prestataire qui joue le rôle d'intermédiaire entre les commerçants, les banques et les émetteurs de cartes pour réaliser (traiter et/ou stocker et/ou transmettre et/ou en support) des opérations de paiement par carte ;
- QSA (Qualified Security Assessor) : prestataire habilité par le PCI SSC pour réaliser des audits PCI DSS ;
- RoC (Report on Compliance) : rapport décrivant le niveau de conformité d'une entité vis-à-vis de PCI DSS ;
- RoV (Report on Validation) : rapport décrivant le niveau de conformité d'une application de paiement vis-à-vis de PCI-PA-DSS ;
- SAQ (Self Auditing Questionnaire) : questionnaire d'auto évaluation de la conformité à PCI DSS. Il permet à toute entité d'auto évaluer le niveau de conformité de son système d'information à PCI DSS. Il est destiné aux entités qui n'ont pas l'obligation d'être évaluées par un auditeur QSA.

Source : https://www.pcisecuritystandards.org/security_standards/docs/glossary_fr.pdf

XIII.2 - Termes liés à d'autres normes, standards ou référentiels

- DdA (Déclaration d'Applicabilité) : Terme utilisé dans la norme ISO 27001, qui désigne le document listant et justifiant les mesures de sécurité applicables et non applicables au SMSI d'un organisme. La DdA est souvent appelée SoA (Statement of Applicability) qui vient de la version anglaise de la norme ISO 27001 ;
- EMV (Europay MasterCard Visa) : Standard international de sécurité des cartes de paiement à puce. EMV est régi par l'EMVCo, organisme administré par American Express, JCB, MasterCard et Visa.

XIII.3 - Termes de monétique

- Accepteur : Entité ayant passé un accord avec un acquéreur pour accepter les cartes bancaires et qui présente à l'acquéreur les données des transactions faites avec ces cartes. En paiement de proximité l'accepteur est le commerçant avec son TPE, en relation VAD/MOTO c'est le commerçant via l'interface Web ou le PSP qui agit pour le compte du commerçant. En retrait c'est le DAB/GAB de la banque ;
- Acquéreur : Organisme financier ou assimilé ayant passé un accord avec un accepteur en vue de l'acquisition des données des transactions faites par carte, qui introduit ces données dans les systèmes d'échanges des émetteurs. C'est la banque domiciliataire du commerçant. Un organisme financier peut être à la fois acquéreur et émetteur ;
- CHD (CardHolder Data) : Ce sont les données du porteur de carte. Elles comprennent en particulier le PAN, la date de fin de validité de la carte et le CVx2 ;
- CNP (Card Non Present) : Situation dans laquelle l'initialisation de la transaction de paiement est réalisée sans que la carte soit physiquement présente au point d'acceptation. Cette situation correspond au paiement sur internet ou en VAD/MOTO ;
- Commerçant : C'est l'entité qui délivre un bien ou un service en échange d'un paiement, dans notre cas par carte bancaire. Il a signé un contrat commerçant avec son acquéreur qui décrit les règles et responsabilités mutuelle pour l'acceptation d'un paiement par carte bancaire ;
- CVx : (CVC, CVC) Cet acronyme désigne les codes CVV (Card Verification Value pour Visa) ou CVC (Card Verification Code pour MasterCard) inscrit dans les données discrétionnaires de la piste ISO 2 pour sceller celle-ci ;
- CVx2 : (CVC2, CVV2) cryptogramme visuel – Le CVx2 est un numéro spécifique à chaque carte, correspondant aux 3 derniers chiffres du numéro inscrit au verso sur le panneau de signature. Le CVx2 est utilisé en paiement sur internet ;
- DAB/GAB : Distributeur de billets, guichet automatique de banque ;
- Données discrétionnaires : Champ des pistes ISO 1 et 2 contenant des données relatives aux contrôles de sécurité ;
- Emetteur : Organisme financier ou assimilé qui émet une carte au profit d'un porteur. C'est la banque du porteur. Un organisme financier peut être à la fois émetteur et acquéreur ;

- Monétique : (Source : Wikipédia) La monétique désigne l'ensemble des traitements électroniques, informatiques et télématiques nécessaires à la gestion de cartes bancaires ainsi que des transactions associées ;
- PAN : Personal Account Number – C'est ce qu'on appelle le numéro de carte bancaire composé généralement de 16 chiffres. Il est embossé sur la face avant de la carte, il fait partie des données figurant sur la piste ISO2 au dos de la carte et également dans les données de la puce ;
- Pistes **(ISO 1, ISO 2) (F)** : Pistes magnétiques au dos de la carte (partie foncée) comportant des informations sur la carte et sur le porteur. Elles sont utilisées pour l'international et les retraits :
  - ISO 1: utilisée à l'étranger ;
  - ISO 2: éléments fixes d'identification du numéro du porteur, date de validité et valeurs de référence ;
- TPE: Terminal de paiement électronique – De nombreuses variantes existent selon les types de commerçants, terminaux grappés, terminaux points de vente ;
- VAD/MOTO: Vente à distance – Mail Order Telephone Order. Situation dans laquelle la carte n'est pas présente lors de l'établissement de la transaction de paiement ;
- POS : Point of sale, point de vente ;
- TPE : terminal de paiement électronique.

XIII.4 - Autres termes

- Forensics (investigations après incident) : ensemble des opérations réalisées à la suite d'un incident ou d'une fraude pour en déterminer la cause, l'origine, l'historique et toutes les informations utiles ;
- Compromission : événement qui se produit lorsqu'une personne non autorisée a eu accès à des informations sensibles.

XIV - Annexe 2 : Analyse comparative PCI DSS, ISO 27001, COBIT

Le tableau suivant permet de voir que la majeure partie des exigences PCI DSS v1.2 est couverte par les mesures de sécurité décrites dans les paragraphes A10 (Gestion de l'exploitation et des télécommunications), A11 (contrôle d'accès) et A12 (acquisition, développement et maintenance des systèmes d'information) de l'annexe 1 de l'ISO 27001:2005.

PCI DSS	Annexe A de l'ISO 27001										
	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
Exigence 1			√			√	√	√			
Exigence 2							√	√			
Exigence 3				√				√			√
Exigence 4			√					√			
Exigence 5						√					
Exigence 6						√		√			
Exigence 7							√				
Exigence 8				√			√				
Exigence 9			√		√	√	√				
Exigence 10						√					√
Exigence 11						√					√
Exigence 12	√	√	√	√		√	√	√	√		√

Figure 4 : Matrice des Relations PCI DSS & ISO 27001

Le tableau suivant présente les correspondances entre PCI DSS v1.2, ISO/IEC 27001:2005 et CobiT v 4.1 :

PCI DSS	ISO/IEC 27001 (Clauses 4 à 8)	ISO/IEC 27001 (Annexe A)	CobiT (version 4.1)
Exigence 1 Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes.		A.11.4.1 Politique relative à l'utilisation des services en réseau A.10.1.2 Management des modifications A.10.6.1 Mesures sur les réseaux A.11.4.6 Mesure relative à la connexion réseau A.11.4.5 Cloisonnement des réseaux A.10.6.2 Sécurité des services réseau A.11.4.1 Politique relative à l'utilisation des services en réseau A.7.1.2 Propriété des actifs A.12.4.1 Mesure relative aux logiciels en exploitation A.11.4.5 Cloisonnement des réseaux A.11.7.1 Informatique et communications mobiles A.11.7.2 Télétravail A.11.6.2 Isolement des systèmes sensibles	AI3.3 Infrastructure maintenance AI6.1 Change standards and procedures AI7.6 Testing of changes AI7.7 Final acceptance test DS5.10 Network security
Exigence 2 Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.		A.11.2.3 Gestion du mot de passe utilisateur A.12.4.1 Mesure relative aux logiciels en exploitation A.12.6.1 Mesure relative aux vulnérabilités techniques A.11.6.2 Isolement des systèmes sensibles A.11.4.4 Protection des ports de diagnostic et de configuration à distance A.11.1.1 Politique de contrôle d'accès A.11.2.2 Gestion des privilèges A.11.5.4 Emploi des utilitaires système	

PCI DSS	ISO/IEC 27001 (Clauses 4 à 8)	ISO/IEC 27001 (Annexe A)	CobiT (version 4.1)
Exigence 3 Protéger les données des titulaires de cartes stockées.		A.15.1.1 Identification de la législation en vigueur A.15.1.4 Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information A.15.2.1 Conformité avec les politiques et les normes de sécurité A.15.2.2 Vérification de la conformité technique A.15.1.6 Réglementation relative aux mesures cryptographiques A.12.3.2 Gestion des clés A.8.1.1 Rôles et responsabilités	PO2.3 Data classification scheme DS5.8 Cryptographic key management DS11.2 Storage and retention arrangements DS11.4 Disposal
Exigence 4 Chiffrer la transmission des données des titulaires de cartes sur les réseaux publics ouverts.		A.7.2.2 Marquage et manipulation de l'information A.12.3.1 Politique d'utilisation des mesures cryptographiques	DS5.11 Exchange of sensitive data
Exigence 5 Utiliser des logiciels antivirus et les mettre à jour régulièrement.		A.10.4.1 Mesures contre les codes malveillants	DS5.9 Malicious software prevention, detection and correction
Exigence 6 Développer et gérer des systèmes et des applications sécurisés.		A.12.6.1 Mesure relative aux vulnérabilités techniques A.12.5.2 Réexamen technique des applications après modification du système d'exploitation A.12.4.1 Mesure relative aux logiciels en exploitation A.12.5.5 Externalisation du développement logiciel A.10.1.4 Séparation des équipements de développement, d'essai et d'exploitation A.10.1.3 Séparation des tâches A.12.4.2 Protection des données système d'essai A.12.5.1 Procédures de contrôle des modifications A.12.2.1 Validation des données en entrée	PO4.11 Segregation of duties DS5.9 Malicious software prevention, detection and correction AI2.3 Application control and auditability AI2.4 Application security and availability AI3.3 Infrastructure maintenance AI3.4 Feasibility test environment AI6.1 Change standards and procedures AI6.2 Impact assessment, prioritisation and authorisation AI7.2 Test plan AI7.4 Test environment AI7.6 Testing of changes AI7.7 Final acceptance test

PCI DSS	ISO/IEC 27001 (Clauses 4 à 8)	ISO/IEC 27001 (Annexe A)	CobiT (version 4.1)
Exigence 7 Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître.		A.11.1.1 Politique de contrôle d'accès A.11.2.2 Gestion des privilèges A.11.2.4 Réexamen des droits d'accès utilisateurs A.11.6.1 Restriction d'accès à l'information	
Exigence 8 Affecter un ID unique à chaque utilisateur d'ordinateur.		A.11.2.1 Enregistrement des Utilisateurs A.11.5.2 Identification et authentification de l'utilisateur A.11.2.3 Gestion du mot de passe utilisateur A.11.4.2 Authentification de l'utilisateur pour les connexions externes A.11.5.1 Ouverture de sessions Sécurisées A.11.5.3 Système de gestion des mots de passe A.11.2.2 Gestion des privilèges A.8.3.3 Retrait des droits d'accès A.11.2.4 Réexamen des droits d'accès utilisateurs A.11.5.6 Limitation du temps de connexion A.11.3.1 Utilisation du mot de passe A.11.5.5 Déconnexion automatique des sessions inactives	PO7.8 Job Change and termination DS5.4 User account management
Exigence 9 Restreindre l'accès physique aux données des titulaires de cartes.		A.9.1.2 Contrôles physiques des accès A.9.1.5 Travail dans les zones sécurisées A.9.1.3 Sécurisation des bureaux, des salles et des équipements A.9.1.4 Protection contre les menaces extérieures et environnementales A.10.5.1 Sauvegarde des Informations A.7.1.2 Propriété des actifs A.11.3.3 Politique du bureau propre et de l'écran vide A.10.7.1 Gestion des supports amovibles A.10.8.1 Politiques et procédures d'échange des informations A.10.8.2 Accords d'échange A.10.7.3 Procédures de manipulation	PO7.8 Job Change and termination DS11.3 Media library management system DS11.4 Disposal DS12.2 Physical security measures DS12.3 Physical access

PCI DSS	ISO/IEC 27001 (Clauses 4 à 8)	ISO/IEC 27001 (Annexe A)	CobiT (version 4.1)
		des informations A.7.1.2 Propriété des actifs A.10.8.3 Supports physiques en transit A.7.1.1 Inventaire des actifs A.10.7.3 Procédures de manipulation des informations A.10.7.2 Mise au rebut des supports	
Exigence 10 Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes.		A.10.10.1 Journaux d'audit A.10.10.2 Surveillance de l'exploitation du système A.10.10.4 Journal administrateur et journal des opérations A.10.10.3 Protection des informations Journalisées A.10.10.6 Synchronisation des Horloges A.15.1.3 Protection des enregistrements de l'organisme	AI2.3 Application control and auditability DS5.5 Security testing, surveillance and monitoring
Exigence 11 Tester régulièrement les processus et les systèmes de sécurité.		A.15.2.2 Vérification de la conformité technique A.10.4.1 Mesures contre les codes malveillants A.10.6.1 Mesures sur les réseaux A.10.6.2 Sécurité des services réseau A.10.9.3 Informations à disposition du public	DS5.5 Security testing, surveillance and monitoring
Exigence 12 Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants.	4.2.1 d) identifier les risques : 1) à 3) 4.2.1 e) analyser et évaluer les risques : 1) à 4) 4.2.1 c) définir l'approche d'appréciation du risque de l'organisme : 1) à 2) 4.2.3 d) réexaminer les appréciations du risque à intervalles planifiés et réexaminer le niveau de risque résiduel et le niveau de risque	A.5.1.1 Document de politique de sécurité de l'information A.5.1.2 Réexamen de la politique de sécurité de l'information A.10.1.1 Procédures d'exploitation documentées A.15.1.5 Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information A.7.1.3 Utilisation correcte des actifs A.11.5.2 Identification et authentification de l'utilisateur A.11.4.2 Authentification de l'utilisateur pour les connexions externes A.7.1.1 Inventaire des actifs A.7.1.2 Propriété des actifs A.11.5.5 Déconnexion automatique des	PO4.8 Responsibility for risk, security and compliance PO6.3 IT policies management PO6.4 Policy, standard and procedures rollout PO7.3 Staffing of roles PO7.4 Personnel training PO7.6 Personnel clearance procedures PO9.4 Risk assessment AI1.2 Risk analysis report AI5.2 Supplier contract management DS2.1 Identification of all supplier relationships DS5.1 Management of IT

PCI DSS	ISO/IEC 27001 (Clauses 4 à 8)	ISO/IEC 27001 (Annexe A)	CobiT (version 4.1)
	acceptable identifié, compte tenu des changements apportés : 1) à 6) 4.2.3 b)	sessions inactives A.12.4.1 Mesure relative aux logiciels en exploitation A.8.1.1 Rôles et responsabilités A.8.2.1 Responsabilités de la direction A.6.1.2 Coordination de la sécurité de l'information A.13.1.1 Remontée des événements liés à la sécurité de l'information A.6.1.7 Relations avec des groupes de spécialistes A.13.2.1 Responsabilités et procédures A.8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information A.8.1.3 Conditions d'embauche A.8.1.2 Sélection A.6.2.1 Identification des risques provenant des tiers A.6.2.3 La sécurité dans les accords conclus avec des tiers A.6.1.5 Engagements de Confidentialité A.13.2.2 Exploitation des incidents liés à la sécurité de l'information déjà survenus	security DS5.2 IT security plan DS5.6 Security incident definition DS11.6 Security requirements for data Management

XV - Annexe 3 : Bibliographie

http://www.cartes-bancaires.com/spip.php?article28

http://www.cartes-bancaires.com/spip.php?article20&var_recherche=pci

https://www.pcisecuritycouncil.org

http://www.visaeurope.com/aboutvisa/security/ais/aisprogramme.jsp

http://usa.visa.com/merchants/risk_management/cisp.html

http://www.mastercard.com/sdp/

http://www.americanexpress.com

http://www.discovernetwork.com/fraudsecurity/disc.html

http://www.jcb-global.com/english/jdsp/index.html

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr