CESAG

Centre Africain d'études Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 4
(2009-2011)

Mémoire de fin d'étude

THEME

DIAGNOSTIC DE LA SECURITE SUR LES CARTES BANCAIRES CONFORMEMENT A LA NORME PCI DSS (Payment Card Industry Data Security Standard) : CAS DE LA STANDARD CHARTERED BANK CAMEROON

Présenté par :

M. EKOBE KAMBO Richard Alain

Dirigé par :

M. APLHA SY
Directeur de l'Audit interne à la Banque Atlantique Sénégal

M. DOLELE SYLLA
Information Analyst at World Bank in the United States of America

DEDICACE

Nous dédions ces recherches à :

- Dieu le Père Tout Puissant, qui nous a donné la grâce d'exister et d'accomplir ce travail, puisse-t-il continuer à faire de nous un instrument entre ses mains et pour sa gloire ;
- notre mère Olive KEDI ESSOH, notre père Daniel KAMBO LONGUE, qui n'ont jamais ménagé aucun effort et sacrifice pour faire de nous des hommes accomplis. Leurs conseils, encouragements et réprimandes ont efficacement contribué à la réussite aussi bien dans nos études que dans tous les autres aspects de la vie. Que chacun Considère ce mémoire comme un début de reconnaissance pour les efforts consentis. Que le Seigneur bénisse chacun de nous où qu'il soit ;
- nos sœurs et frères, Ernestine, Hortense, Marie-Brigitte, Gérard, Jules, Jean-Claude, Patrice et Emile KAMBO ; nos belles sœurs et beaux-frères, Laurentine LONGUE, Vanessa ESSOH, Erick ABIA et Mathieu ENONE, pour avoir si bien remplacé, continué et comblé l'œuvre de nos parents au moment opportun. Leurs encouragements et leurs soutiens nous ont toujours poussés à tirer le meilleur de nous ;
- la famille ELAME à Dakar, pour leur présence, réconfort et soutien qui nous ont été très bénéfiques.

REMERCIEMENTS

L'occasion nous est accordée d'exprimer nos remerciements et notre profonde gratitude à ceux qui ont rendu possible l'accomplissement de ce travail.

Ils vont à l'attention de :

- M. ALPHA O. SY, Directeur de l'Audit Interne de la Banque Atlantique du Sénégal, M. DOLELE SYLLA, Information Analyst (World Bank U.S.A), pour leurs encadrements, conseils et soutiens inestimables ;
- Mme Roselyne BONGNY, Directrice des Ressources Humaines de la Standard Chartered Bank Cameroon, qui nous a permis d'effectuer notre stage au sein de la Banque ;
- M. Mathieu EBAH, Chef du Département des Opérations et Mme Caroline LEMDJA, son adjoint, pour leurs encadrements et conseils ;
- le personnel de la Standard Chartered Bank Cameroon, pour leur soutien professionnel et leur apport inestimable ;
- mes amis de près ou de loin pour leurs encouragements ;
- la promotion MPACG 2 2009-2011, pour la collaboration durant ces années exceptionnelles de formation ;
- le personnel du Centre Africain d'Etudes Supérieures en Gestion aussi bien administratif que le corps professoral.

LISTE DES SIGLES ET ABBREVIATIONS

ACS : Access Control Server

ALC : African Leasing Company

ARPC : Authorization ResPonse Cryptogram

ARQC : Authorization ReQuest Cryptogram

ASV : Prestataire de services d'analyse agréé (Approved Scanning Vendor).

BAC : Banque Atlantique du Cameroun

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

BEAC : Banque des Etats de l'Afrique Centrale

BICEC : Banque Internationale du Cameroun pour l'Epargne et le Crédit

C.E.S.A.G : Centre Africain d'Etudes Supérieures en Gestion

CA-SCB : Crédit Agricole – Société Commerciale de Banque

CAV2 : Card Authentification Value

CBC : Commercial Bank of Cameroon

CDA : Combined Dynamic Data Authentication / Application Cryptogram Generation.

CDP : Commission des Données Personnelles

CEMAC : Communauté Economique et Monétaire de l'Afrique Centrale

CEMAC : Communauté Economique et Monétaire de l'Afrique Centrale

CFC : Crédit Foncier du Cameroun

CID : Card Idenfication Number

CISP : Cardholder Information Security Program

CNP : Card Not Present

COBAC : Commission Bancaire de l'Afrique Centrale

COBIT : Control Objectives for Information and Technology related

CVC2 : Card Validation Code

CVV2 : Card Verification Value 2

DAB : Distributeur Automatique de Billets

DDA : Dynamic Data Authentification

DMZ : Zone Démilitarisée

DSS : Normes de sécurité des données (Data Security Standard),

EMV : Europay MasterCard Visa

FRAP : Feuille de Révélation et d'Analyse des Problèmes

GAB : Guichet Automatique de Banque

GIM-UEMOA: Groupement Interbancaire Monétique - Union Economique et Monétaire Ouest Africain

GPRS : Service général de radiocommunication par paquets (General Packet Radio Service)

GSM : Global System for Mobile

HK$: Hong Kong Dollar

HTTPS : Protocole de transfert hypertexte sur SSL (Hypertext transfer protocole over secure socket layer)

ID : Identifiant d'un utilisateur ou d'une application spécifique

IFACI : Institut Français de l'Audit et du Contrôle Internes

IPSEC : Sécurité de protocole Internet (Internet Protocol Security)

ISACA : Information System Audit and Control Association

ISO : Organisation Internationale de Normalisation

ITIL : Information Technology Infrastructure Library

JCB : Japan Credit Bureau

Kbit/s : Kilobit par seconde

M C : Mesure Compensatoire

MHz : Megahertz

MPI : Merchant Plug In

NAC : Contrôle d'Accès Réseau

NFCB : National Financial Credit Bank

NIP : Numéro d'Identification Personnel

NIST SP : National Institute of Standard and Technology Special Publication

OTP : One-Time Password

PA-DSS : Payment Application Data Security Standard

PAN : Primary Account Number

PC : Personal Computer

PCI DSS : Payment Card Industry Data Security Standard

PCI SSC : Payment Card Industry Security Standards Council

PED : PIN Entry Device

PIN : Code d'identification personnel (Personal identification number).

PKI : Public Key Infrastructure

PROM : Programmable Read Only Mémory

PRO-PME : PRO-PME financement S.A
QSA : Évaluateur de sécurité qualifié (Qualified Security Assessor)
QSV : Qualified Security Vendors
RAM : Read Access Memory
RBAC : Contrôle d'accès en fonction du rôle (Role-Based Access Control)
ROM : Read Only Memory
RSA : Rivest-Shamir-Adleman (algorithme pour le cryptage de clé publique)
S.A : Société Anonyme
SAE : Système d'Autorisation Emetteur
SAQ : Questionnaire d'auto-évaluation (Self-Assessment Questionnaire)
SCB CL : Société Commerciale de Banque Crédit Lyonnais Cameroun
SCB : Standard Chartered Bank (Groupe)
SCBC : Standard Chartered Bank Cameroon
SCE : Société Camerounaise d'Equipement
SDA : Static Data Authentication
SGBC : Société Générale des Banques au Cameroun
SI : Système d'Information
SMS : Short Message Service
SNI : Société Nationale d'Investissement
SNMP : Simple Network Management Protocol
SMSI : Système de Management de la Sécurité d'Information
SOCCA : Société Camerounaise de Crédit Automobile
SRC : Société de Recouvrement des Créances du Cameroun
SSH : Secure SHell.
SSL/TLS : Secure Socket Layer
TC : Transaction Certificate
TFFA : Tableau de Forces et Faiblesses Apparentes
TIC : Technologie de l'Information et de la Communication
TPE : Terminaux de Paiement Electronique
UBA : United Bank for Africa
UBAC : United Bank for Africa Cameroon PLC
UBC : Union Bank of Cameroon Limited
UEMOA : Union Economique et Monétaire Ouest Africaine
UMAC : Union Monétaire de l'Afrique Centrale

URL : Universal Record Locator

USA : Etats Unis d'Amérique (United States of America)

USB : Universal Serial Bus

VA : Valeur d'Authentification

VAD : Vente A Distance

VLAN : Réseau local virtuel (Virtual LAN ou Virtual Local Area Network)

Vpp : Valeur de Haute tension de Programmation.

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

« Les banques sont des institutions financières qui acceptent les dépôts et qui font des crédits » (MISHKIN, 2007 : 10). Elles diffèrent selon leur objet : banque de dépôt, banque d'affaires, banques spécialisées dans un type de prêt, banque généraliste... Quelle que soit leur nature, l'existence des banques est fortement corrélée à celle de la monnaie. Définie comme étant tout ce qui est accepté pour le paiement des biens ou des services ou encore pour le remboursement de dette, la monnaie est donc un élément déterminant dans un système de paiement. Elle a connu une évolution très marquée due à ses limites et aux modifications du temps.

La lourdeur et la difficulté de transport surtout sur une grande distance de la monnaie marchandise ont conduit à la monnaie fiduciaire. Le coût de transport et le risque de vol de cette dernière ont conduit à la monnaie scripturale ; encore appelée quasi monnaie. La plus répandue est le chèque, qui impose une contrainte de temps et de coût pour un paiement ou un encaissement rapide.

C'est dans un contexte de modernisation des systèmes de paiement et du développement de l'activité économique que des autorités monétaires par le biais des banques ont décidé de promouvoir et intégrer dans l'environnement bancaire africain l'utilisation de la carte bancaire.

Selon ONU (2010 : 310), les Autorités Monétaires de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) à travers la Banque des Etats de l'Afrique Centrale (BEAC) ont initié en 2003, un projet d'envergure régionale visant la modernisation des systèmes de paiement dans les Etats membres de la zone. C'est ainsi que l'Office Monétique de l'Afrique Centrale (OMAC) a été fondée en 2005. L'OMAC est l'autorité de certification du système monétique de la zone CEMAC. Il est un organisme sous régional né de la volonté de mutualiser les moyens de paiement pour permettre le développement de la monétique en Afrique Centrale.

En 2002, la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initié un important projet de modernisation des systèmes de paiement des Etats membres de l'Union Economique et Monétaire Ouest Africain (Règlement N°15/2002/CM/UEMOA) relatif aux systèmes de paiement dans les Etats Membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA). C'est ainsi qu'en février 2003, le Groupement Interbancaire Monétique de l'Union Economique et Monétaire Ouest Africaine (GIM-UEMOA) fut créé.

Le point commun entre les projets est la promotion et la vulgarisation de nouveaux moyens de paiement tels que la carte de paiement.

Dans les pays développés contrairement aux pays africains, l'utilisation de la carte bancaire est à un stade très avancé. Elles sont de plus en plus répandues et variées. D'après SHERIF et SERHROUCHNI (2000 : 39), il existe 7 types de cartes de paiement qui varient en fonction du service offert : les cartes de garantie de chèques, les cartes bancaires de retrait de billets, les cartes bancaires de paiement qui comprennent la carte à débit immédiat, la carte à débit différé et la carte de crédit, les cartes à usage restreint, les cartes accréditives du type American Express ou Diner'scard, les cartes privatives et les cartes orientées entreprises.

L'observatoire de la sécurité des cartes de paiement (2010 : 91, 2009 : 69, 2008 : 91) établit en France respectivement en 2010, 2009 et 2008, qu'il y'a 88.6, 90.6 et 84.7 millions de cartes bancaires en circulation. Il retrace également le marché des cartes de paiement.

En 2010, selon l'Observatoire (2010 : 93), 6 453.78 millions d'opérations ont été réalisées pour des paiements de proximité sur automate et pour des échanges entre émetteur et acquéreur français soit 284.62 milliards d'euros ; 130.71 millions de paiements à distance hors internet d'une valeur de 11.47 milliards d'euros ; 324.03 millions d'opérations pour des paiements à distance sur internet, correspondant à 26.22 milliards d'euros et enfin 1 476.75 millions d'opérations pour des retraits ont été traitées soit en valeur 110,23 milliards d'euros.

En 2009, pour l'observatoire (2009 : 70), 6 118.98 millions d'opérations ont été réalisées pour des paiements de proximité sur automate et pour des échanges entre émetteur et acquéreur français ce qui représentent 271.57 milliards d'euros ; 123.28 millions de paiements à distance hors internet d'une valeur de 11.19 milliards d'euros ; 245.97 millions d'opérations pour des paiements à distance sur internet correspondant à 19.08 milliards d'euros et enfin pour des retraits 1 492.38 millions d'opérations ont été traitées soit en valeur 108.73 milliards d'euros.

Pour ce qui est de l'Afrique, Jusqu'en 2009, seuls trois pays africains utilisaient les cartes de crédit comme mode de paiement, l'Afrique du Sud : 5 millions de cartes, l'Egypte : 1, 1 million de cartes, le Maroc : 800.000 cartes.

Ces chiffres soulignent l'importance et le rôle grandissant que joue la carte de paiement. Fort heureusement ce rôle a été bien compris des dirigeants africains malgré quelques difficultés d'entrée de la carte de paiement dans le paysage bancaire africain. Ceci se justifie par

plusieurs raisons : la réticence des agents économiques qui lui accordent peu de confiance, l'inaccessibilité de la carte bancaire par toutes les classes de la population, la méconnaissance du rôle et de l'importance de la carte bancaire.

Force est de constater que la confiance que certains agents économiques ont placé en cet instrument de paiement en essor est entravée par divers maux tels que des piratages de données, des vols d'identité, des pertes lesquels laissent cours à des fraudes dont il fait l'objet.

En effet, l'on observe une croissance marquée de la fraude sur les cartes bancaires au fil des années. D'après l'observatoire de la sécurité des paiements (2010 : 23), le taux de fraude en France est en perpétuelle hausse ; respectivement en 2010, 2009 et 2008, il est de 0.074%, 0.072% et 0.070% pour un montant total de 351.5, 324.3 et 304.3 millions d'euros.

Pour répondre au besoin de développement du système de paiement africain en général et dans la sous-région en particulier, la Standard Chartered Bank Cameroun (SCBC) a mis au point plusieurs cartes bancaires. Il est vrai que la carte bancaire est en plein essor compte tenu de l'environnement africain en mutation, il n'en demeure pas moins que les fraudes aussi. De ce faite, la SCBC n'est pas en marge de multiples risques et insécurités inhérentes à l'utilisation frauduleuse et illégale des cartes bancaires.

L'insécurité en matière de carte bancaire dont font preuve la plupart des banques africaines pourrait s'expliquer entre autres par :

- la méconnaissance et le non-respect des standards internationaux en matière de protection des données des titulaires ;
- le standard international utilisé en matière d'authentification des transactions effectuées avec les cartes bancaires est complètement désuet ;
- les faiblesses des mesures de sécurité et de protection ;
- l'absence d'un système d'évaluation permanent de la sécurité ;
- la négligence de la part des détenteurs de la carte ;
- le coût élevé de la mise en œuvre des mesures de protection et de sécurité.

Toute cause produisant des effets, ceux énoncés ci-dessus peut entrainer des conséquences fâcheuses pour les détenteurs des cartes et par ricochet pour la banque. Il s'agit entre autres :

- des vols d'identité et des fraudes sur les cartes bancaires ;

- du piratage de numéros lors d'opérations effectuées par l'internet ;
- de la falsification des cartes de paiement ;
- de la perte d'argent due à l'utilisation de cartes volées, falsifiées ou perdues ;
- du paiement des intérêts et dommages en cas de responsabilité ;
- du vol de cartes ou de souches portant des numéros de cartes ;

Pour pallier aux insuffisances relevées ci – dessus, les solutions suivantes peuvent être envisagées :

- diagnostiquer la sécurité sur les cartes bancaires ;
- respecter un standard en matière de sécurité de l'information : cas du PCI DSS ;
- réviser les choix des types de garanties en cas de vol de carte ;
- concevoir et mettre sur pied un système de sécurité viable ;
- implémenter de nouvelles normes de sécurité.

Afin de répondre de manière adéquate et méthodique à la problématique de la sécurité sur les cartes bancaires, il faudrait au préalable faire un état des lieux au regard des standards internationaux. Ainsi, la solution la plus juste et importante que nous retenons est la somme des deux premières solutions possibles à savoir : « diagnostiquer la sécurité sur les cartes bancaires conformément au standard PCI DSS »

La solution ainsi retenue nous amène à nous poser la question de savoir à quelles fins diagnostique-t-on la sécurité sur les cartes bancaires ? D'où la question de savoir : Quelle est l'efficacité de la sécurité sur les cartes bancaires de la SCBC ?

De cette interrogation il découle les questions spécifiques suivantes :

- qu'est-ce qu'une carte bancaire et les différents types de cartes ?
- quelles sont les données à sécuriser ?
- qu'est-ce que le standard PCI DSS ?
- quelles sont les exigences de sécurité des cartes bancaires selon le standard PCI DSS ?
- comment évaluer l'efficacité de la sécurité de cartes bancaires ?
- quels sont les risques encourus en cas de non-conformité au standard ?

D'un point de vue pratique, l'on pourrait se demander :

- quels sont les types de cartes utilisées par la SCBC ?
- quel est le standard utilisé en matière de sécurité sur les cartes à la SCBC ?
- quel est l'état de la sécurité sur les cartes bancaires de la SCBC ?
- quelles sont les améliorations à entreprendre pour se conformer à la norme PCI DSS ?

Nous essayerons de répondre ces interrogations à travers la pose du diagnostic de la sécurité sur les cartes bancaires conformément au standard PCI DSS : cas de la Standard Chartered Bank Cameroun.

L'objectif principal de notre étude est de poser le diagnostic de la sécurité sur les cartes bancaires de la SCBC. Les objectifs spécifiques sont :

- évaluer la sécurité sur les cartes bancaires ;
- identifier les forces et les faiblesses ;
- établir un programme de travail basé sur les faiblesses ;
- faire des recommandations ;
- renforcer la sécurité sur les cartes bancaires.

Ce mémoire retracera l'organisation de la sécurité sur les cartes bancaires au sein de la Banque, analysera également le niveau d'efficacité de la sécurité liée aux cartes bancaires et enfin permettra de savoir si la dimension qualitative de la sécurité est perçue par l'application des bonnes pratiques admises.

L'intérêt de ce travail peut être perçu différemment selon les intervenants :

- pour la Banque

Ce travail servira de base dans la prise de décision. A travers la connaissance de l'état de leur sécurité, la Banque pourra mettre en œuvre les mesures appropriées pour améliorer cette sécurité. De manière indirecte, la Banque répondra aux objectifs définis par la BEAC ou la BCEAO en matière de modernisation des systèmes de paiement (la mise sur pied d'un système d'interbancarité et d'une stratégie de développement dynamique du secteur bancaire avec des moyens de paiement modernes exigeant l'adoption d'un cadre juridique rénové adéquat tant au niveau régional que national ; l'installation d'une architecture de paiement globale, moderne, conforme aux standards internationaux en la matière).

- Pour le C.E.S.A.G (Centre Africain d'Etudes Supérieures en Gestion) de Dakar-SENEGAL

Nous espérons que ce mémoire pourra constituer un point de départ à la recherche dans le domaine en ce qui concerne les promotions futures qui pourront l'approfondir et l'enrichir davantage.

- Pour le stagiaire

C'est l'oecasion de mettre en application au terme de deux années de formation l'ensemble des connaissances capitalisées et mieux les assoir.

Le présent travail s'articule autour de deux parties :

- la première consacrée au cadre théorique s'attèlera à examiner les notions de carte bancaire, de standard PCI DSS, des risques de non-conformité, des exigences en matière de sécurité. Elle permettra de faire ressortir les concepts fondamentaux et de nous accommoder aux expressions relevant de notre thème et enfin de définir un modèle d'analyse.

- La seconde partie nous permettra de présenter la SCBC, notre structure d'accueil, de faire une analyse des existants en matière de sécurité sur les cartes bancaires conformément au standard PCI DSS, et enfin de faire des recommandations.

PREMIERE PARTIE : CADRE THEORIQUE ET METHODOLOGIE

La modernisation des systèmes de paiement plonge les banques dans une course vers la recherche des parts de marché. De gros volumes de capitaux sont investis dans de nouveaux produits. C'est ainsi que les cartes bancaires voient le jour en réponse aux besoins exprimés ou latents des consommateurs. Comme tout produit, la carte bancaire doit générer des revenus pour rentabiliser les capitaux investis. Cette rentabilité dépend très fortement non seulement de la concurrence mais d'abord de la perception qu'ont les clients du nouveau produit. Un client satisfait serait susceptible d'influencer favorablement l'avenir d'un produit en le vantant à ses pairs et inversement. Il serait alors intéressant pour une banque d'accroître la confiance du client par sa satisfaction, ce qui nous amène à nous poser la question de savoir comment une banque pourrait augmenter elle la confiance d'un client dans une carte bancaire ?

Les banques sont généralement très enclins à présenter les avantages de la carte bancaire en omettant (de présenter) les risques et les inconvénients dont elle fait l'objet et qui généralement relèvent du domaine de la confidentialité, gage l'image de marque des établissements financiers. Ces risques et inconvénients remettent en question la sécurité dans l'usage de cet instrument de paiement. En réponse au besoin de confiance des consommateurs avertis, les émetteurs gagneraient à sécuriser d'avantages les transactions réalisées au moyen des cartes par l'utilisation des standards internationaux les plus récents. Le PCI DSS répond donc parfaitement à cette contrainte car il est le plus actuel.

Une banque certifiée PCI DSS garantit non seulement la sécurité des transactions exécutées par le client et par là même son chiffre d'affaires, mais couvre aussi sa responsabilité quand bien même le risque serait réalisé. Malheureusement, en Afrique en général et au Cameroun en particulier, plusieurs banques restent en marge de l'utilisation de ce standard pour diverses raisons, entre autres : la méconnaissance du standard PCI DSS ou autres, le manque de rigueur dans la surveillance de l'application par les autorités compétentes, l'absence d'évaluation continue de leur dispositif de sécurité en vue d'une mise à jour…

C'est dans une logique de prévention du risque et de ces insuffisances que notre mémoire s'inscrit. Notre cadre théorique nous permettra de présenter premièrement la carte bancaire et le standard PCI DSS (Chapitre 1) ; deuxièmement les modalités de l'évaluation du dispositif de sécurité sur les cartes bancaires en conformité avec le standard (chapitre 2) et enfin la méthodologie de l'étude (chapitre 3).

CHAPITRE 1 : LE PAYSAGE DE LA CARTE BANCAIRE ET LE STANDARD PCI DSS

« La monnaie électronique est un des moyens de circulation de la monnaie scripturale » (Y. Gauffriau, 1997 : 85). Le nombre croissant du volume de transactions effectuées ; l'importance des sommes engagées ; les données personnelles des porteurs de cartes ont conduit à s'interroger sur la sécurité et les garanties qu'offre cet instrument de payement en essor dans l'environnement bancaire africain. A travers ce chapitre, nous examinerons dans une première section le concept de carte bancaire, dans une seconde section le standard PCI DSS et ses exigences en matière de sécurité.

1.1 Le paysage des cartes bancaires

Par paysage des cartes bancaires nous comprenons : la définition et rôle de la carte bancaire, les différents types de cartes bancaires, la description et les aspects techniques liés aux cartes, les informations à sécuriser stockées sur les cartes bancaires, les risques liés aux cartes bancaires, les dispositifs de sécurité des cartes bancaires ainsi que les normes et régulations internationales.

1.1.1 Définition et rôle de la carte bancaire

Il n'est pas aisé de définir la carte bancaire, certains auteurs l'assimilent à la carte de débit, d'autres à une carte de paiement. D'après DANCETTE & al. (2000 : 52), « la carte bancaire, tout comme la carte de débit est une carte en plastique émise par un établissement bancaire ; elle permet au détenteur d'avoir accès à son compte en banque et d'y effectuer des opérations (virements, dépôts, retraits) ». Pour BI TRA (2011 : 76), une carte de paiement est « une carte bancaire qui, en plus de la fonction de retrait au distributeur de billets de banque, permet de régler des dépenses chez les commerçants agréés. Ces dépenses sont débitées soit en temps réel (débit immédiat), soit en une seule fois à la fin du mois (débit différé) ».

En somme, une carte bancaire est un moyen de paiement, une carte délivrée par un établissement de crédit comportant, le plus souvent, une puce électronique et une piste magnétique permettant, selon le cas, d'effectuer le paiement de biens et services, auprès de commerces physiques possédant un terminal de paiement ou virtuels sur internet ; le retrait d'espèces aux distributeurs automatiques de billets (DAB) et aux guichets automatiques de

banque (GAB). La carte de paiement est associée à un réseau de paiement, tel que Visa, MasterCard, JCB (Japan Credit Bureau), GIM-UEMOA, OMAC.

En fonction des différents besoins exprimés ou latents de leurs clients, les banques émettent diverses cartes de paiement.

1.1.2 Les différents types de cartes bancaires

Selon BERNET Luc-Rollande (2002 : 54), il existe deux types de cartes bancaires, les cartes de retrait et les cartes de paiement. DESMICHT (2007 : 84), considère deux autres types, d'une part les cartes nationales et les cartes internationales et d'autre part les cartes à débit immédiat et les cartes à débit différé.

En définitive, nous retiendrons la typologie proposée par SHERIF et SERHROUCHNI (2000 : 39-40), qui nous paraît la plus complète. Ils distinguent sept types de cartes bancaires : les cartes de garantie de chèques ; les cartes bancaires de retrait de billets ; les cartes bancaires de paiement (les cartes à débit immédiat, les cartes à débit différé et les cartes de crédit) ; les cartes à usage restreint ; les cartes accréditives (ou cartes internationales à débit différé) ; les cartes privatives ; et enfin, les cartes orientées entreprise.

Les cartes bancaires possèdent des spécificités qui leur sont propres, nous les décrirons et verrons leurs aspects techniques.

1.1.3 Descriptions et aspects techniques liés aux cartes

Une carte de paiement se présente en vertu de la norme ISO 2894 sous la forme d'une carte plastifiée mesurant « 85.60 mm de longueur, 53.98 mm de largeur et 0.76 mm d'épaisseur » (DRAGON & al., 2002 : 123), équipée d'une bande magnétique et/ou puce électronique (c'est donc une carte à puce).

Selon DRAGON & al. (2002 : 112), les cartes bancaires se présentent sous la forme d'un rectangle de plastique comportant : au recto, le nom de la carte, le numéro de la carte, la période de validité, le nom de banque qui a délivré la carte, le nom du titulaire et une puce électronique ; au verso, une bande magnétique et un spécimen de la signature du titulaire de la carte. Nous décrirons la carte à puce, car elle est prisée par les banques (voir annexe 2).

➢ **La carte à puce**

D'après GODART (2002 : 230-231), la carte à puce est une carte à circuit intégré de génération la plus récente de cartes contenant une puce capable d'effectuer des calculs complexes. Elle est encore appelée carte à microprocesseur. Selon SHERIF (2007 : 369), elle possède un système d'exploitation, un microprocesseur, une mémoire morte ROM (Read Only Memory), une mémoire vive RAM (Read Access Memory), une mémoire indélébile programmable PROM (Programmable Read OnlyMémory) et des circuits intégrés.

Les banques privilégient les cartes à puce parce qu'elles sont adaptées à une sécurisation avancée du fait de leurs caractéristiques. L'activité bancaire est réputée comme étant un domaine délicat compte tenu des enjeux. Ainsi les cartes bancaires comportent un certain nombre d'informations sensibles à sécuriser.

1.1.4 Les informations à sécuriser stockées sur les cartes bancaires

Dans les mémoires de sa puce, la carte bancaire stocke des informations permettant d'identifier la banque et le compte en banque. Elle possède également une clé privée pour signer. Enfin, elle contient la clé publique de la banque. D'après la description de la carte faite par DRAGON & al. (2002 : 123), voir annexe 2, en général les informations à sécuriser sont :

- les données des porteurs de carte telles que le numéro de compte primaire (PAN, Primary Account Number), le nom du titulaire de la carte de crédit, le code de service, la date d'expiration ;

- les données d'authentification sensibles dont le stockage est interdit après l'autorisation de la transaction telles que les données de bandes magnétiques complètes ou leurs équivalents stockés sur la puce, 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) et le bloc PIN (qui est une version chiffrée du code PIN).

La manipulation inappropriée de ces données peut entraîner de nombreux risques préjudiciables aussi bien pour la banque que pour le détenteur de la carte bancaire, sans toute fois omettre les autres acteurs de la chaîne.

1.1.5 Les risques liés aux cartes bancaires

MADERS et MASSELIN (2009 : 26), définissent le risque comme « une perte potentielle, identifiée et quantifiable (enjeux) inhérente à une situation ou une activité, associée à la probabilité de l'occurrence d'un événement ou d'une série d'événements ». Pour RENARD (2010 : 155), « le risque c'est la menace qu'un événement ou une action ait un impact défavorable sur la capacité de l'entreprise à réaliser ses objectifs avec succès ». En définitive, l'IFACI, dans son lexique « Les mots de l'audit », perçoit le risque comme étant « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ». En général, les risques liés aux cartes bancaires sont : le vol et la perte, l'utilisation frauduleuse, le piratage. De manière spécifique, nous distinguerons le risque à quatre niveaux : la banque, le porteur de la carte, le marchand et la carte.

- La banque et ses risques

En émettant les cartes, les banques sont sujettes à un certain nombre de risques, d'après L'HEUREUX et LANGEVIN (1991 : 49), la responsabilité de l'établissement émetteur peut être engagée en cas de perte ou de vol de la carte et du NIP (numéro d'identification personnel), en cas d'agression au terminal et en cas de mauvais fonctionnement. COLOMBANI (2004 : 23), distingue comme risques : le « retraits frauduleux par vraies ou fausses cartes dans les DAB avec des cartes perdues, volées, interdites ou non parvenues ; le retraits frauduleux par vraies ou fausses cartes dans les DAB avec des cartes contrefaites ».

- Le porteur de la carte et ses risques

D'après L'HEUREUX et LANGEVIN (1991 : 41), le titulaire de la carte bancaire à la responsabilité de la sécurité du système, ainsi que des risques de disparition des moyens d'accès, des risques d'utilisation abusive, des risques de falsification et de contrefaçon. Pour COLOMBANI (2004 : 20), être victime d'une fraude à la carte bancaire, cela peut être une petite perte sans grandes conséquences immédiates ; un préjudice important représentant « un coup dur », avec d'éventuelles conséquences financières : emprunt, litiges, justice… ; un préjudice grave, des répercussions mettant en jeu l'équilibre de la vie au quotidien : blocage de compte, interdictions bancaires… ; la destitution sociale et financière : surendettement, faillite… ; et enfin , « l'utilisation abusive par les porteurs » (COLOMBANI, 2004 : 22).

- Le marchand (commerçant) et ses risques

COLOMBANI (2004 : 23), le marchand peut être soumis aux risques suivants : le paiement frauduleux sur les terminaux de paiement avec des cartes perdues, volées, interdites ou non parvenues ; le paiement frauduleux sur les terminaux de paiement avec des cartes à puce contrefaites ; l'usurpation de numéros de cartes dans les commerces de vente à distance par courrier ou téléphone ; et enfin, l'usurpation de numéros de cartes dans les commerces de vente à distance par internet.

- La cartes bancaire et ses risques

Les cartes à piste sont particulièrement sensibles à la fraude, notamment si la technologie employée pour la piste magnétique est obsolète et permet en conséquence un ré-encodage de données encore plus aisé. L'impact en matière de fraude peut dans ce cas s'avérer conséquent, au regard de l'étendue du réseau d'acceptation dont bénéficient ces cartes. Ces cartes ont une capacité de stockage limitée et ne peuvent pas être programmées, ce qui les rend inadaptées à une sécurisation poussée. C'est ainsi que l'OCDE (2000 : 115), souligne « la nécessité de mettre au point un mécanisme sûr au niveau de la carte » d'où l'émergence des cartes à puce.

Dans la carte à puce à contact, la cadence d'horloge varie selon SHERIF (2007 : 367), entre 3.5 MHz et 5 MHz, son alimentation se fait au moyen d'une source de tension de 3 à 5 volts ce qui la rend moins sensible aux risques d'attaques par variation de tension. Elle peut est sujette aux risques d'usure et d'érosion provoquées par divers facteurs tels que l'abrasion, la corrosion, la sueur, la pollution, les substances chimiques qui pourraient endommager la carte et par là même les données stockées. L'émergence de ces multiples risques, a conduit à développer et à imaginer des moyens pour pallier à divers manquements et conséquences liés à l'utilisation des cartes bancaires.

1.1.6 Les dispositifs de sécurité liés aux cartes bancaires : cas de la carte à puce

« La sécurité est l'ensemble des mesures permettant d'assurer la protection des biens / valeurs » (GODART, 2002 : 17). La sécurisation des cartes de paiement vise d'une part la protection des données secrètes stockées sur les cartes, d'autre part les droits d'accès aux services. Son but renvoie à la prévention de la contrefaçon et ceci à toutes les phases de la production ;

l'interdiction de la subtilisation des progiciels relatifs aux applications et à la sécurisation ; la protection des données stockées ; ainsi que la détection et l'arrêt de tout usage illicite et abusif.

La sécurisation intervient tout au long du cycle de vie d'une carte qui va de la fabrication à la distribution en passant par la personnalisation. Selon SHERIF (2007 : 374), ce cycle comporte 7 étapes : la conception et le développement des circuits intégrés et des progiciels de la carte ; la fabrication des galettes de silicium ; l'insertion du progiciel et la mise sous boîtier du circuit intégré et le contrôle final ; la pré-personnalisation de la carte en ajoutant des programmes relatifs à l'usage final avec vérification de leur fonction ; la personnalisation des circuits intégrés c'est-à-dire l'enregistrement des noms de l'organisme émetteur et du porteur et l'insertion du logiciel des applicatifs ; et enfin l'émission de la carte sur support plastique après l'embossage, l'impression des logos en vue de sa distribution. A chaque étape intervient au moins un acteur qui participe à la sécurisation de la carte.

Pendant sa fabrication, la sécurisation (voir annexe 6) d'une carte bancaire fait intervenir différents acteurs. D'après SHERIF et SERHROUCHNI (2000 : 403), la sécurisation d'une carte à puce doit tenir compte des acteurs suivants : les concepteurs des circuits intégrés et des logiciels de sécurité ; les manufacturiers des circuits intégrés et les producteurs des logiciels de sécurité ; les autorités de certification ; les développeurs de l'applicatif ; les producteurs de carte (embosseurs, imprimeurs, encarteurs…) ; et enfin les émetteurs de carte.

Par analogie à la sécurité informatique, Il existe 2 types de sécurisation (voir annexe 8) pendant l'utilisation de la carte : « la sécurisation physique et la sécurisation logique » (CARPENTIER, 2009 : 39-40). La sécurisation physique se traduit en cas d'agression physique détectée, par des circuits résistant aux infractions de la carte à puce qui empêchent ses fonctions de sortie. Elle possède une couche diélectrique qui lui offre une résistance passive et la protège contre les impuretés, la poussière et les radiations. Des protections physiques de la mémoire peuvent aussi être employées pour empêcher un effacement sélectif de celle-ci. Enfin, des fusibles sont en place pour désactiver les modes tests utilisés par le fabricant avant la distribution.

La sécurisation logique de la carte se traduit par un contrôle logique pendant son utilisation à travers l'authentification de l'usager légitime (travers soit la carte d'identité et la signature du porteur), l'authentification de la carte (chiffrement symétrique/asymétrique), l'établissement

d'un canal logique de communication sécurisée entre la carte à puce et le système hôte en passant par la borne de lecture, le maintien de l'intégrité des données et les entrées/sorties sécurisées.

Des normes et régulation internationales existent pour réglementer la sécurité sur les cartes bancaires parmi les lesquelles le standard PCI DSS (Payment Card Industry Data Security Standard), notre référentiel pour notre étude car étant le plus récent en la matière.

1.2 Le standard PCI DSS

Le référentiel de sécurité PCI DSS a été élaboré par tous les principaux réseaux internationaux de cartes tels que « Visa, MasterCard, Discover, American Express, Japan Credit Bureau » (KIM et SOLOMON, 2010 : 395), pour établir des règles de protection des données liées aux cartes, à leur utilisation et à leur stockage. Il s'applique directement à tous ceux qui manipulent les données sur les cartes bancaires. Dans cette section, nous présenterons le PCI DSS et ses exigences.

1.2.1 Qu'est-ce que le PCI DSS ?

Le PCI SSC (Payment Card Industry Security Standards Council) a développé le PCI DSS. Le conseil a été fondé par des grands fabriquants de cartes bancaires et est aujourd'hui une société à responsabilité limitée immatriculée dans l'État américain du Delaware. Selon CALDER et CARTER (2008 : 1), le PCI DSS consiste en jeu normalisé, au niveau de toute l'industrie, en exigences et processus pour la gestion de la sécurité, des politiques, des procédures, en architecture réseau, conception de logiciel et mesures protectrices critiques. Le PCI DSS doit être respecté par toutes les organisations qui transmettent, traitent ou stockent des données de carte de paiement. Le PCI DSS est une obligation contractuelle appliquée et mise en application au moyen des amendes ou d'autres restrictions directement par des fournisseurs de paiement eux-mêmes. Le PCI DSS a connu plusieurs versions dues à de nombreuses révisions parmi lesquelles les versions 1.0 et 2.0. La version 2.0 du standard PCI DSS, la plus recente, a été finalisée en « octobre 2010 » (THOMAS & al. 2011 : 80).

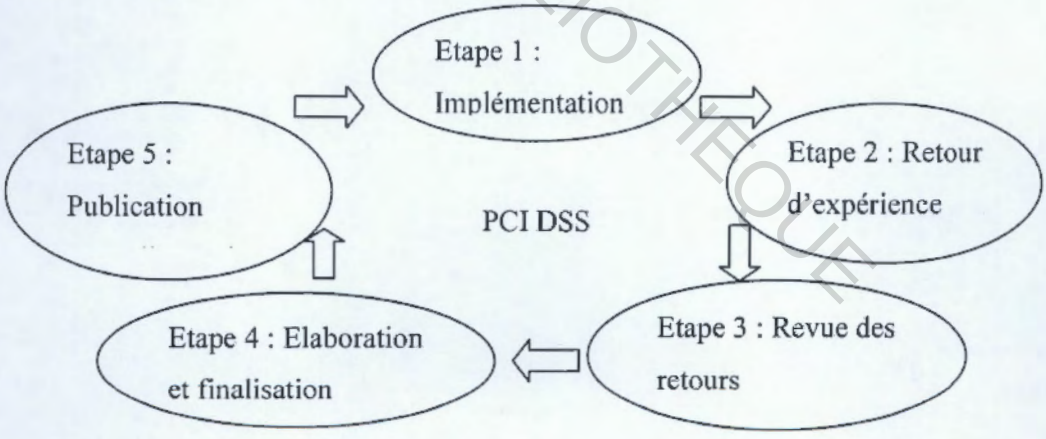
D'après American Bar Association (2008 : 66), le PCI DSS est un jeu de 12 exigences (conditions) de sécurité de base.

1.2.2 Les mesures compensatoires, le cycle de vie et les exigences de sécurité du PCI DSS

Le PCI DSS comprend des exigences qui impliquent un respect total, sinon des mesures compensatoires peuvent être admises. D'après la Payment Card Industry Standard Security Council (2008 : 13-14), « les mesures compensatoires peuvent être appliquées lorsqu'un pré-requis est inapplicable pour une raison technique forte ou remet en cause le modèle économique de l'entreprise ». Il est donc possible d'utiliser une mesure compensatoire pour toutes les exigences exceptée la clause 3.2 : « ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée) » (PCI SSC, 2008 : 13).

De sa mise en œuvre à ce jour le standard PCI DSS a connu une évolution due à ses multiples révisions. D'après CHUVAKIN et WILLIAMS (2009 : 35), le PCI DSS suit un cycle de vie de 24 mois se décomposant en 5 étapes : l'implémentation, le retour d'expérience, la revue des retours d'expérience, l'élaboration et la finalisation de la nouvelle version, la publication de la nouvelle version du standard (voir annexe 7). Graphiquement, il se présente ainsi :

Figure 1 : Cycle de vie du standard du PCI DSS



Source : nous-même d'après CHUVAKIN et WILLIAMS (2009 : 35)

Le PCI SSC définit les douze exigences des normes de sécurité des données de PCI DSS et explique l'objectif de chacune d'elles. Il vise à aider les commerçants, les prestataires de services et les établissements financiers qui souhaitent se faire une idée plus claire des normes de sécurité des données et mieux cerner la signification et l'intention de chaque exigence de sécurisation des composants du système (serveurs, réseau, applications, etc.) qui prennent en

charge les environnements des données de titulaire de carte. Selon WRIGHT (2011 : 20-21), les exigences des normes PCI DSS sont :

Tableau 1: Exigences du standard PCI DSS

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

Source : PCI SSC (2008 : 4-53)

Un ensemble d'acteurs intervient dans l'animation du PCI DSS, chacun joue un rôle précis en fonction de ses responsabilités (voir annexe 9). Il existe d'autres normes qui s'alignent en partie dans les mêmes objectifs que le PCI DSS.

1.2.3 Mappage : alignement avec les autres normes

Il existe un lien étroit entre le PCI DSS et d'autres normes ou référentiels tels qu'ISO 27001/27002, COBIT, ITIL

ISO 27001 : « L'ISO 27001 est la norme internationale pour des systèmes de management de la sécurité de l'information et elle fournit aux organisations les meilleurs conseils pratiques pour l'identification, l'évaluation et le contrôle des risques d'informations contenus dans les plans d'activité stratégiques et des environnements opérationnels quotidiens » (CALDER, 2006 : 12). Selon VON SOLMS et VON SOLMS (2008 : 46), ISO 27002 quant à lui, est un guide qui conseille les entreprises sur ce qu'elles devraient avoir mise en place en matière de gestion de la sécurité de l'information afin de suivre les meilleures pratiques.

Un alignement de PCI DSS avec d'autres normes peut être fait, nous avons comparé PCI DSS avec ISO 27001/27002, COBIT et ITIL (voir annexe 10).

Le PCI DSS, comme toute autre norme, a des avantages, mais aussi des difficultés et des limites qui peuvent être considérées comme ses inconvénients.

1.2.4 Avantages, difficultés et limites d'une démarche PCI DSS

Le PCI DSS, doit faire l'objet d'une utilisation adéquate, à défaut il risquerait d'être détourné de son objectif initial et voire être contre productif. Tout comme il pourrait avoir des avantages, de même il aurait des inconvénients et limites.

En raison du caractère obligatoire et rigide de ses mesures, le PCI DSS a pour avantage de débloquer des projets de sécurité déjà identifiés par les opérationnels mais non développés pour des raisons plus liées au contexte économique qu'à la gestion des risques ; le PCI DSS peut s'inscrire dans une démarche globale et cohérente de sécurisation des systèmes d'information ; dans le cadre des systèmes d'information jeunes à bâtir, le PCI DSS présente un référentiel de sécurité monétique.

Les difficultés liées à l'implémentation du PCI DSS sont de plusieurs ordres parmi lesquelles : le délai exigé par les organismes ne permettant 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 ; le PCI DSS nécessite parfois une adaptation non négligeable du système d'information et des métiers ; 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.

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

En Afrique en général, les structures de gestion des cartes bancaires sont quasiment inexistantes. Respectivement l'OMAC et GIM UEMOA, sont des structures créées par la BEAC et la BCEAO afin de développer et promouvoir l'utilisation de la carte bancaire dans les sous régions (Afrique centrale et Afrique de l'Ouest). A ce jour, Elles ont mis sur le marché des cartes répondant aux exigences de l'EMV. Ainsi on aura pour le cas de l'OMAC, les cartes CB OMAC et OMAC VISA (voir annexe 3) ; pour GIM UEMOA, les cartes GIM UEMOA (voir annexe 3). Quasiment aucune banque camerounaise et sénégalaise n'utilise encore le standard PCI DSS, ceci est dû au niveau de développement, à la règlementation du secteur bancaire et surtout au coût de l'investissement élevé pour les banques qui connaissent le standard. Des partenariats sont signés entre de nombreuses banques africaines et étrangères se traduisant par la présence des cartes de types Visa et Mastercard en Afrique.

L'information est un actif important pour les entités qui désirent être leader sur un marché concurrentiel. Les cartes bancaires émises sur le marché par les banques ne sont pas en marge de cette lutte âpre qu'impose l'activité bancaire. Il devient de ce fait, primordial pour les banques de disposer de meilleurs atouts afin de protéger l'information compte tenu de sa sensibilité. Raisonnablement, de nombreux outils en matière de sécurisation de l'information ont été développés, c'est ainsi que le PCI DSS entre en étroite ligne dans cette logique de protection. Pour les banques et autres organismes manipulant les données sensibles des porteurs de carte, l'obligation leur est faite de se conformer à ce standard. La question de savoir pourquoi à ce niveau ne se pose plus, le problème de l'heure est maintenant de savoir s'ils remplissent cette obligation. Pour ce faire, la nécessité d'évaluer l'entité concernée s'impose, mais comment ? C'est ce qui fera l'objet du prochain chapitre à savoir : l'évaluation de la conformité à la norme PCI DSS.

CHAPITRE 2 : EVALUATION DE LA CONFORMITE A LA NORME PCI DSS

Le PCI SSC, a mis au point un document qui constitue un outil d'évaluation de la sécurité sur les cartes de paiement. Cet outil combine à la fois les 12 conditions de la norme et les procédures de tests correspondantes. Il est utilisé dans le cadre du processus de validation d'une entité. En somme, il présente à une entreprise qui désire renforcer la sécurité des données des titulaires de cartes et adopter des mesures de sécurité uniformes à l'échelle mondiale, comment évaluer sa conformité à la norme PCI DSS.

Dans ce chapitre, nous aborderons tour à tour les objectifs de l'évaluation, le champ d'application couvert par le standard, la démarche d'évaluation (conditions et procédures) et enfin la présentation et la description du tableau d'évaluation.

2.1 Objectif de l'évaluation

Outre les objectifs déclinés dans l'introduction de notre mémoire, l'évaluation de la conformité à la norme PCI DSS a pour objectif ultime l'amélioration de la sécurité au tour de la carte bancaire. En effet, par la connaissance de l'état de leur dispositif de sécurité, les banques pourront connaître les points faibles de celui et trouver les dispositifs de contrôle interne adéquats et conforme aux bonnes pratiques pour combler les insuffisances.

2.2 Champ d'application de l'évaluation de la conformité aux conditions de la norme PCI DSS

D'après le PCI SSC (2010 : 10), « les exigences du PCI DSS s'appliquent à toutes les composantes du système ». Sont considérés comme composantes du système :

- tout composant réseau, serveur ou application inclus dans, ou connectés à l'environnement des données des titulaires de cartes ;
- tous les composants de virtualisation comme les machines, commutateurs/routeurs, outils, applications/bureaux virtuels ainsi que les hyperviseurs.

Afin de facilité l'évaluation, la segmentation réseau peut être envisagée.

2.2.1 La segmentation réseau

La recherche de pertinence peut conduire à décider d'une segmentation réseau. Ceci n'est pas une condition du PCI DSS. Cependant, « elle peut contribuer à réduire :

- le champ d'application de l'évaluation PCI DSS ;
- les coûts de l'évaluation PCI DSS ;
- les risques pour une entreprise (grâce au regroupement des données des titulaires de cartes dans un nombre plus restreint de sites mieux contrôlés) ;
- les coûts et les difficultés liés à la mise en œuvre et à la gestion des contrôles » (PCI SSC, 2010 : 10-11).

Compte tenu de l'importance des éléments à évaluer, l'échantillonnage offre de nombreux avantages.

2.2.2 L'échantillonnage des installations

« Tout comme la segmentation réseau, l'échantillonnage n'est pas une condition de la norme PCI DSS. Toutefois, après avoir considéré le champ d'application global et la complexité de l'environnement étudié, l'évaluateur peut sélectionner de manière indépendante des échantillons des installations de l'entreprise et des composants du système afin d'évaluer la conformité aux conditions PCI DSS» (PCI SSC, 2010 : 12).

Les échantillons choisis doivent représenter chaque installation. Que l'échantillonnage soit ou non utilisé, les conditions et les procédures d'évaluation de la norme PCI DSS s'appliquent à la totalité de l'environnement des données des titulaires de carte.

2.3 Conditions et procédures d'évaluation

La démarche d'évaluation est fonction des exigences formulées par la norme. Il convient de préciser que toutes les conditions n'ont pas été développées ici. Compte tenu de leur importance, nous avons privilégié la démarche et elle se caractérise par l'exigence, la condition à remplir et la procédure de test.

D'après le PCI SSC (2010 : 20-77), l'évaluation se fait de manière ci-après.

2.3.1 Création et gestion d'un réseau sécurisé

Cette condition comprend les exigences 1 et 2 à respecter.

Exigence 1 : Installer et gérer une configuration de pare-feux pour protéger les données des titulaires de cartes.

- **Conditions 1**

Selon VIRTUE (2008 : 72-80), la première condition pour assurer la conformité avec cette exigence PCI DSS est que les normes de l'organisation de configuration de pare-feu doit prendre en charge les configurations détaillées suivantes :

- les processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feux et des routeurs ;
- les schémas de réseau actuel indiquant toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil ;
- l'exigence de pare-feux au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne.

- **Procédure de test**

D'après le PCI SSC (2010 : 20-24), il s'agira de « procéder comme suit :

- vérifier qu'un processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feux et des routeurs est en place ;
- 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 ;
- vérifier que le schéma est tenu à jour ;
- vérifier que les normes de configuration des pare-feux comprennent l'exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée et la zone de réseau Internet ».

Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.

- **Conditions 2**

Selon HARWOOD (2010 : 256), la seconde condition pour assurer la conformité avec cette exigence PCI DSS serait de ne pas utiliser les mots de passe système et autres paramètres par défaut définis par les commerçants. Ces accès sont connus des harkers et faciles à déterminer.

- **Procédure de test**

Cette exigence est simple à respecter, selon le PCI SSC (2010 : 25-28), il s'agira « choisir un échantillon de composants du système et essayer de se connecter (avec l'aide de l'administrateur système) aux périphériques avec les comptes et mots de passe définis par défaut par le fournisseur, afin de vérifier que ceux-ci ont bien été changés (se référer aux manuels du fournisseur et aux sources disponibles sur Internet pour rechercher les comptes/mots de passe définis par le fournisseur) ».

La première catégorie d'exigence examinée, il convient de voir la seconde.

2.3.2 Protection des données des titulaires de cartes de crédit

Elle vise les exigences 3 et 4.

Exigence 3 : Protéger les données de titulaires de cartes stockées

- **Condition 3**

D'après CHAMP (2007 : 281), PCI DSS exige que les données des titulaires stockées soient rendues illisibles (cryptées). Dans le cas de l'incapacité de remplir cette exigence, des contrôles compensatoires doivent être mis en œuvre pour atténuer le risque.

- **Procédure de test**

Selon le PCI SSC (2010 : 29-36), pour se conformer à cette exigence, il s'agira d'obtenir et passer en revue les politiques, procédures et processus de l'entreprise relatifs à la conservation et l'élimination des données, et procéder comme suit :

- vérifier que les politiques et les procédures comprennent des dispositions légales, réglementaires et professionnelles sur la conservation des données, notamment des conditions spécifiques sur la conservation des données des titulaires de cartes ;
- vérifier que les politiques et les procédures comprennent des dispositions sur l'élimination des données qui ne sont plus requises à des fins légales, réglementaires ou professionnelles, notamment la suppression des données des titulaires de cartes ;
- vérifier que les politiques et procédures couvrent l'ensemble du stockage de données de titulaires de cartes ;
- vérifier que toutes les politiques et procédures comprennent au moins un des éléments suivants :
  - un processus programmé (automatique ou manuel) pour supprimer, au moins une fois par trimestre, les données de titulaires de cartes stockées, excédant les conditions définies dans la politique de conservation des données ;
  - l'obligation d'une vérification, au moins trimestrielle, afin de contrôler que les données de titulaires de cartes stockées n'excèdent pas les conditions définies dans la politique de conservation des données. ;
- sur un échantillon de composants de système stockant des données de titulaires de cartes, vérifier que les données stockées n'excèdent pas les conditions définies dans la politique de conservation des données.

Exigence 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.

➢ **Conditions 4**

Selon BRADLEY (2007 : 76-77), la manière la plus fiable et efficace pour veiller à ce que les données transmises ne soient pas interceptées ou modifiées, c'est de les crypter lors de la transmission.

➢ **Procédure de test**

Selon le PCI SSC (2010 : 37-38), pour remplir cette exigence, il s'agira de « vérifier l'utilisation de protocoles sécurisés chaque fois que les données des titulaires de cartes sont transmises ou reçues sur des réseaux publics ouverts. Vérifier qu'un cryptage robuste est utilisé pendant la transmission des données », comme suit :

- à la réception des transactions, choisir un échantillon et examiner les transactions pendant qu'elles s'exécutent afin de vérifier que les données des titulaires de cartes sont cryptées pendant le transfert ;
- vérifier que seuls des clés/certificats approuvés sont acceptés ;
- vérifier que le protocole est déployé de manière à n'utiliser que des configurations sécurisées et qu'il ne prend en charge aucune version ni configuration non sécurisées ;
- vérifier que le niveau de cryptage approprié est mis en œuvre pour la méthodologie de cryptage employée (Vérifier les recommandations/meilleures pratiques du fournisseur) ;
- pour les implémentations SSL/TLS : vérifier que la mention HTTPS apparaît dans l'adresse URL (Universal Record Locator) dans le navigateur ; vérifier qu'aucune donnée de titulaires de cartes n'est requise lorsque la mention HTTPS n'apparaît pas dans l'URL.

Il s'en suit dès lors la gestion d'un programme des vulnérabilités.

2.3.3 Gestion d'un programme des vulnérabilités

Les exigences 5 et 6 doivent être remplies pour gérer les vulnérabilités.

Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement

- **Conditions 5**

D'après CHUVAKIN & WILLIAMS (2009 : 164), le PCI DSS oblige les organisations à utiliser et mettre régulièrement à jour des logiciels anti-virus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).

- **Procédure de test**

Selon PCI SSC (2010 : 39-40), la procédure de mise en conformité PCI DSS est la suivante :

- vérifier que des logiciels antivirus sont déployés et, le cas échéant, qu'une technologie de protection antivirus est en place ;
- vérifier que tous les programmes antivirus détectent et éliminent tous les types de logiciels malveillants connus et constituent une protection efficace contre ces fléaux ;
- vérifier que tous les logiciels antivirus sont à jour, en cours d'exécution et génèrent des journaux en procédant comme suit :

- obtenir et passer en revue la politique, et vérifier qu'elle stipule la mise à jour des logiciels antivirus et des définitions de virus ;
- vérifier que l'installation principale du logiciel est configurée pour la mise à jour automatique et l'exécution d'analyses à intervalles réguliers ;

- . sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que les mises à jour automatiques et les analyses à intervalles réguliers sont activées ;
- sur un échantillon de composants du système, vérifier que la génération des journaux des logiciels antivirus est activée et que ceux-ci sont conservés conformément à la condition 10.7 de la norme PCI DSS.

Exigence 6 : Développer et gérer des systèmes et des applications sécurisés

➢ **Conditions 6**

Selon CENDROWSKI & MAIR (2009 : 108), l'organisation doit développer et gérer des systèmes et applications sécurisés afin de s'assurer que tous les logiciels et les composants du système sont dotés des derniers correctifs de sécurité.

➢ **Procédure de test**

La procédure selon le PCI SSC (2010 : 41-47), est la suivante :

- comparer la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur, afin de vérifier que les plus récents sont installés ;
- passer en revue les politiques relatives à l'installation des correctifs de sécurité afin de s'assurer qu'elles stipulent l'installation de tous les nouveaux correctifs de sécurité stratégiques dans un délai d'un mois.

Après la gestion d'un programme de vulnérabilités vient la mise en œuvre de mesures de contrôle d'accès strictes.

2.3.4 Mise en œuvre de mesures de contrôle d'accès strictes

Les contrôles d'accès stricts sont garantis si les exigences 7, 8 et 9 sont atteintes

Exigence 7 : Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître.

- **Conditions 7**

Selon AXELROD & al. (2009 : 67), la septième condition pour assurer la conformité avec cette exigence PCI DSS est que les normes de restriction de l'accès aux données des titulaires de cartes doivent prendre en charge les restrictions d'accès aux composants du système et aux données des titulaires de cartes aux seuls individus qui doivent y accéder pour mener à bien leur travail. Les restrictions d'accès doivent inclure ce qui suit :

- restriction des droits d'accès accordés aux ID d'utilisateur privilégiés en octroyant les privilèges les plus faibles qui sont nécessaires pour la réalisation du travail ;
- l'octroi des privilèges se fait sur la base de la classification et de la fonction professionnelles de chaque employé ;
- obligation d'une approbation documentée par les responsables spécifiant les privilèges requis ;
- mise en œuvre d'un système de contrôle d'accès automatique.

- **Procédure de test**

Pour le PCI SSC (20101 : 48-49), il s'agira de :

- se procurer et examiner la politique écrite de contrôle des données et vérifier que celle-ci comprend ce qui suit :
    - s'assurer que les droits d'accès accordés aux ID d'utilisateur privilégiés sont les plus faibles nécessaires à la réalisation des obligations professionnelles ;
    - s'assurer que les privilèges sont octroyés aux individus sur la base de leur classification et de leur fonction professionnelles (cette approche est également appelée « contrôle d'accès en fonction du rôle » (ou RBAC, Role-Based Access Control) ;

- confirmer que l'approbation documentée par les responsables est requise (par écrit ou par voie électronique) pour tout accès, et qu'elle spécifie les privilèges requis ;
- confirmer que les contrôles d'accès sont mis en œuvre par le biais d'un système de contrôle d'accès automatisé.

Exigence 8 : Affecter un ID unique à chaque utilisateur d'ordinateur

➢ **Conditions 8**

Selon AXELROD & al. (2009 : 67), la huitième condition pour assurer la conformité avec cette exigence PCI DSS est que les normes d'affectation d'ID unique à chaque utilisateur d'ordinateur doivent prendre en charge les éléments suivants :

- affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants du système ou aux données de titulaires de cartes ;
- employer au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs :
  - quelque chose de connu, comme un mot de passe ou une locution de passage ;
  - quelque chose de détenu, comme un dispositif token ou une carte à puce ;
  - quelque chose concernant l'utilisateur, comme une mesure biométrique.

➢ **Procédure de test**

Il est question selon le PCI SSC (2010 : 50-55), de :

- vérifier que tous les utilisateurs ont un ID unique pour accéder aux composants du système ou aux données de titulaires de cartes ;
- pour vérifier que les utilisateurs sont authentifiés à l'aide d'un ID unique et une autre méthode d'authentification (par exemple, un mot de passe) afin d'accéder à l'environnement des données de titulaires de cartes, procéder comme suit :
  - obtenir et examiner la documentation qui décrit les méthodes d'authentification utilisées ;
  - pour chaque type de méthode d'authentification employée et pour chaque type de composant du système, observer une authentification pour vérifier qu'elle se déroule conformément aux méthodes d'authentification décrites.

Exigence 9 : Restreindre l'accès physique aux données des titulaires de cartes.

➢ **Conditions 9**

Selon AXELROD & al. (2009 : 67), la neuvième condition pour assurer la conformité avec cette exigence PCI DSS est que la restriction de l'accès physique aux données des titulaire des cartes doit prendre en compte les éléments suivants :

- utiliser des contrôles d'accès aux installations appropriés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de cartes ;
- installer des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès pour surveiller l'accès physique des individus aux zones sensibles ;
- examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi.

➢ **Procédure de test**

Elle consiste d'après le PCI DSS (2010 : 56-60), à :

- vérifier que des contrôles de sécurité physiques sont en place dans chaque salle informatique, centre de données et autres zones physiques qui abritent des systèmes appartenant à l'environnement des données de titulaires de cartes ;
- vérifier que l'accès est contrôlé par des lecteurs de badge et autres dispositifs tels que des badges autorisés, des clés et des cadenas ;
- -observer un administrateur système pendant qu'il tente de se connecter sur les consoles de systèmes choisis de façon aléatoire dans l'environnement des données de titulaires de cartes, et vérifier que ces consoles sont « verrouillées » pour empêcher toute utilisation non autorisée ;
- vérifier que des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès sont en place pour surveiller les points d'entrée/de sortie des zones sensibles ;
- vérifier que les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont protégés contre la falsification ou la désactivation ;
- s'assurer que les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont sous surveillance et que les données enregistrées sont conservées pendant trois mois au moins.

La prochaine catégorie d'exigence est la surveillance et les tests réguliers sur les réseaux.

2.3.5 Surveillance et tests réguliers des réseaux

Cette catégorie couvre les exigences 10 et 11.

Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes.

- **Condition 10**

Selon WEISS & SOLOMON (2010 : 44), la dixième condition pour assurer la conformité avec cette exigence PCI DSS est d'effectuer le suivi et la surveillance de tous les accès aux ressources réseaux et aux données des titulaires de cartes de manière à définir un processus pour associer chaque accès aux composants du système (en particulier les accès avec des droits administrateurs) à chaque utilisateur individuel.

- **Procédure de test**

Il s'agira selon le PCI SSC (2010 : 61-65), d'assurer que les vérifications à rebours des composants du système sont activées et actives.

Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité.

- **Condition 11**

Selon WEISS & SOLOMON (2010 : 44), la onzième condition pour assurer la conformité avec cette exigence PCI DSS est le test régulier des processus et des systèmes de sécurité de manière à prendre en compte les points d'accès sans fil et à détecter les points d'accès sans fil non autorisés tous les trimestres.

- **Procédure de test**

La procédure consiste d'après PCI SSC (2010 : 66-70), à :

- vérifier que l'entreprise possède un processus documenté pour détecter et identifier les points d'accès sans fil, tous les trimestres ;

- vérifier que la méthodologie est appropriée et qu'elle permet de détecter et d'identifier tout point d'accès sans fil non autorisé, notamment les cartes WLAN insérées dans les composants du système ; les dispositifs sans fil portatifs connectés aux composants du système (par exemple, par USB, etc.) ; les dispositifs sans fil branchés sur un port réseau ou un périphérique réseau.
- vérifier que le processus documenté pour identifier les points d'accès sans fil non autorisés est exécuté au moins chaque trimestre pour tous les composants du système et toutes les installations.
- vérifier que la configuration déclenchera des alertes pour le personnel, si l'on utilise une surveillance automatisée (par exemple systèmes de détection et/ou de prévention d'intrusions sans fil, NAC, etc.),
- vérifier que le plan de réponse aux incidents de l'entreprise (condition 12.9) prévoit une réaction en cas de détection de périphériques sans fil non autorisés.

La surveillance et les tests réguliers des réseaux terminés ; intervient enfin, la gestion d'une politique de sécurité des informations.

2.3.6 Gestion d'une politique de sécurité des informations

La gestion d'une politique de sécurité d'information vise l'exigence 12 uniquement.

Exigence 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel.

- **Conditions 12**

Selon ROUNTREE (2010 : 7), la douzième et dernière condition pour assurer la conformité avec cette exigence PCI DSS est de gérer une politique de sécurité des informations pour l'ensemble du personnel de manière à définir, publier, gérer et diffuser une politique de sécurité qui :

- satisfait à toutes les conditions de la norme PCI DSS ;
- inclut un processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques ;
- comprend au moins un examen annuel avec une mise à jour chaque fois que l'environnement change.

➢ **Procédure de test**

Selon le PCI SSC (2010 : 77), il est question de :

- passer en revue la politique de sécurité des informations et vérifier qu'elle est publiée et diffusée à tout le personnel concerné.
- vérifier que la politique satisfait à toutes les conditions de la norme PCI DSS.
- vérifier que le processus annuel d'évaluation des risques qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques est documenté.
- examiner la documentation d'évaluation des risques, afin de vérifier que le processus (d'évaluation) est exécuté au moins une fois par an.
- vérifier que la politique de sécurité des informations est passée en revue au moins une fois par an et mise à jour le cas échéant, pour tenir compte des modifications apportées aux objectifs de l'entreprise ou à l'environnement de risque.
- Ainsi résumé la démarche d'évaluation de la conformité à la norme PCI DSS, il convient de voir la présentation du tableau d'évaluation mis au point par le PCI SSC.

Ainsi présenté la procédure d'évaluation, il convient de voir le tableau d'évaluation du PCI DSS et de le décrire.

2.4 Présentation et description du tableau d'évaluation du PCI DSS

Le PCI SSC a conçu un tableau spécifique pour une évaluation que nous présenterons.

2.4.1 Présentation du tableau

Le tableau permettant l'évaluation mis sur pied par PCI SSC se présente ainsi :

Tableau 2 : Tableau d'évaluation du PCI DSS

Conditions PCI DSS	Procédures de test	En place	Pas en place	Date cible / Commentaires

Source : PCI SSC (2010 : 19)

2.4.2 Description du tableau

« Les informations suivantes définissent les en-têtes des colonnes du tableau Conditions et procédures d'évaluation de sécurité de la norme PCI DSS » (PCI SSC, 2010 : 19) :

- **Conditions de la norme PCI DSS :**

Cette colonne définit la norme DSS (Data Security Standard) et indique les conditions à satisfaire pour être conforme à la norme PCI DSS. La conformité sera validée au regard de ces conditions.

- **Procédures de test** :

Cette colonne indique les processus que l'évaluateur doit suivre pour valider que les conditions de la norme PCI DSS sont « en place ».

- **En place** :

L'évaluateur doit se référer à cette colonne pour donner une brève description des contrôles validés comme étant « en place » pour chaque condition, y compris celle des contrôles déterminés comme en place à la suite de contrôles compensatoires, ou en raison d'une condition « sans objet ».

- **Pas en place** :

L'évaluateur doit se référer à cette colonne pour donner une brève description des contrôles qui ne sont pas en place. Notez qu'un rapport non conforme ne doit pas être envoyé à une marque de carte de paiement ou à l'acquéreur à moins que celui-ci n'en ait fait la demande explicite.

- **Date cible/Commentaires :**

Pour les contrôles qui ne sont « pas en place », l'évaluateur peut préciser la date cible à laquelle le commerçant ou le prestataire de services doivent avoir les contrôles « en place ». Les remarques ou commentaires éventuels peuvent être portés ici.

Au terme de ce chapitre, nous sommes à même de comprendre la démarche d'évaluation pour toute entité désirant se conformer au standard, et assurer le minimum de diligence en matière de protection données sensibles compte tenu des multiples risques que renferme le paysage de la carte bancaire. L'un des avantages qu'offre le standard PCI DSS réside dans le fait qu'il est développé par les acteurs centraux de la carte elle-même. Ceux-ci ont conçu et développé ce standard permettant de sauvegarder l'intégrité des données des détenteurs de carte. Ceci permet donc de leur transférer efficacement la responsabilité en cas de risque avéré le cas échéant et de justifier de l'adéquation de ce standard. Leur démarche d'évaluation nous a permis ainsi d'élaborer notre modèle d'analyse dans le cadre du traitement de notre thème, d'où le chapitre 3 intitulé : la méthodologie de l'étude.

CHAPITRE 3 : LA METHODOLOGIE DE L'ETUDE

Les chapitres précédents jetaient les bases de notre étude. Élaborer un diagnostic sur la sécurité des cartes bancaires conformément à une norme nécessite au préalable des connaissances théoriques à la fois sur les cartes bancaires et sur ladite norme. « En définitive, le modèle d'analyse est un modèle théorique se composant d'un ou de plusieurs concepts (un système de concepts organisé en théorie) soigneusement définis, et d'une ou de plusieurs hypothèses nécessairement liées entre elles (l'une peut être principale par rapport aux autres), afin de former un ensemble cohérent » (BOUTILLIER et al, 2005 : 81). Considérant que ces pré-requis ont été acquis, ils convient de ce fait de voir à présent comment le diagnostic sera exécuté en pratique. Le présent chapitre s'articulera donc autour de l'élaboration d'un modèle d'analyse ainsi que des outils de collecte et d'analyse de données.

3.1 Le modèle théorique d'analyse

Trois phases sous-tendent la base de notre modèle : la préparation, l'exécution et la finalisation.

3.1.1 Phase de préparation

Cette phase est composée de trois étapes : la prise de connaissance de l'entité, la prise de connaissance de la norme PCI DSS et enfin la préparation des outils et techniques de collecte de données.

- Etape 1 : la prise de connaissance de l'entité

Tableau 3 : Prise de connaissance de l'entité

La prise de connaissance de l'entité	
Objectifs	Il s'agira de se familiariser avec l'activité de l'organisation en recueillant dans un premier temps des informations générales sur son environnement, ensuite de s'informer sur ses aspects spécifiques.

Source : Nous-même

Tableau 3 : Prise de connaissance de l'entité (Suite)

La prise de connaissance de l'entité	
Activités	Collecte de données, identification de l'entité, connaissance de l'historique de l'entité, connaissance de la situation de l'entité dans sa branche d'activité, connaissance des politiques, objectifs, missions et des activités stratégiques de l'entité, connaissance de l'organisation et de l'administration de l'entité.
Outils, supports méthodologiques	analyse documentaire (organigramme, manuel de procédure…), questionnaire, observation, entretiens.
Résultat attendu	Tirer un jugement des éléments qualitatifs et quantitatif de l'entreprise
Acteurs	Nous-même

Source : Nous-même

- Etape 2 : prise de connaissance de la norme PCI DSS

Tableau 4 : Prise de connaissance de la norme PCI DSS

Prise de connaissance de la norme PCI DSS	
Objectifs	La norme PCI DSS représente un ensemble minimum d'objectifs de contrôle. L'objectif exprime ce que l'on veut faire. Il formule les orientations à poursuivre et se décline en une ou plusieurs actions. Il est donc nécessaire de bien connaître la norme pour l'évaluation
Activités	Collecte de données, compréhension de la norme PCI DSS, des buts de chaque opération ainsi que des procédures et des conditions de l'évaluation.
Outils, supports méthodologiques	Analyse documentaire
Résultat attendu	définition des modalités de mise en œuvre du diagnostic.
Acteurs	Nous-même

Source : nous-même

- Etape 3 : la préparation des outils et techniques de collecte des données

Tableau 5 : Préparation des outils et techniques de collecte des données

La préparation des outils et techniques de collecte des données	
Objectifs	Capitaliser les informations disponibles afin de les exploiter
Activités	Consignation des données sur des fiches synthétiques, confection des tableaux.
Outils, supports méthodologiques	TFFA (Tableau de Forces et Faiblesses Apparentes), questionnaire d'évaluation
Résultat attendu	Tableaux, questionnaires
Acteurs	Nous-même

Source : Nous-même

Après la préparation vient la réalisation.

3.1.2 Phase de réalisation

Deux étapes la constituent : la description du dispositif et son évaluation.

- Etape 4 : la description du dispositif

Tableau 6 : Description du dispositif

La description du dispositif	
Objectifs	Connaître l'état des lieux
Activités	Collecter des données, analyser, classer et donner une vue synthétique de l'ensemble des informations collectées, décrire les processus et les tâches, modéliser le système existant pour émettre un diagnostic
Outils, supports méthodologiques	Entretien, questionnaires de prise de connaissance, analyse documentaire (tableaux de bord, catalogues, études, données statistiques…), observation.
Résultat attendu	Obtenir une vue d'ensemble de façon claire du fonctionnement de l'organisation (meilleure compréhension du système)
Acteurs	Nous-même et le personnel SCBC

Source : Nous-même

- Etape 5 : l'évaluation du dispositif

Tableau 7 : Evaluation du dispositif

L'évaluation du dispositif	
Objectifs	Evaluer le dispositif de sécurité
Activités	L'identification des opportunités des menaces, l'identification des forces et faiblesses
Outils, supports méthodologiques	Méthode SWOT, TFFA, questionnaire d'évaluation, tableau d'évaluation, matrice de criticité.
Résultat attendu	Obtenir un diagnostic de la sécurité de l'entité
Acteurs	Nous-même

Source : nous-même

La réalisation terminée, il s'en suit la finalisation.

3.1.3 Phase de finalisation

L'analyse des résultats et le plan d'action déterminent cette phase.

- Etape 6 : Analyse des résultats

Tableau 8 : Analyse des résultats

Analyse des résultats	
Objectifs	Il sera question de faire ressortir les dysfonctionnements, de les analyser afin d'y apporter des solutions adéquates.
Activités	Comparaison de l'existant et du système cible
Outils, supports méthodologiques	Rapprochement, référentiel
Résultat attendu	Force et faiblesse (Ecart) pour élaborer un plan d'actions.
Acteurs	Nous-même

Source : Nous-même

- Etape 7 : Plan d'action

Tableau 9 : Plan d'action

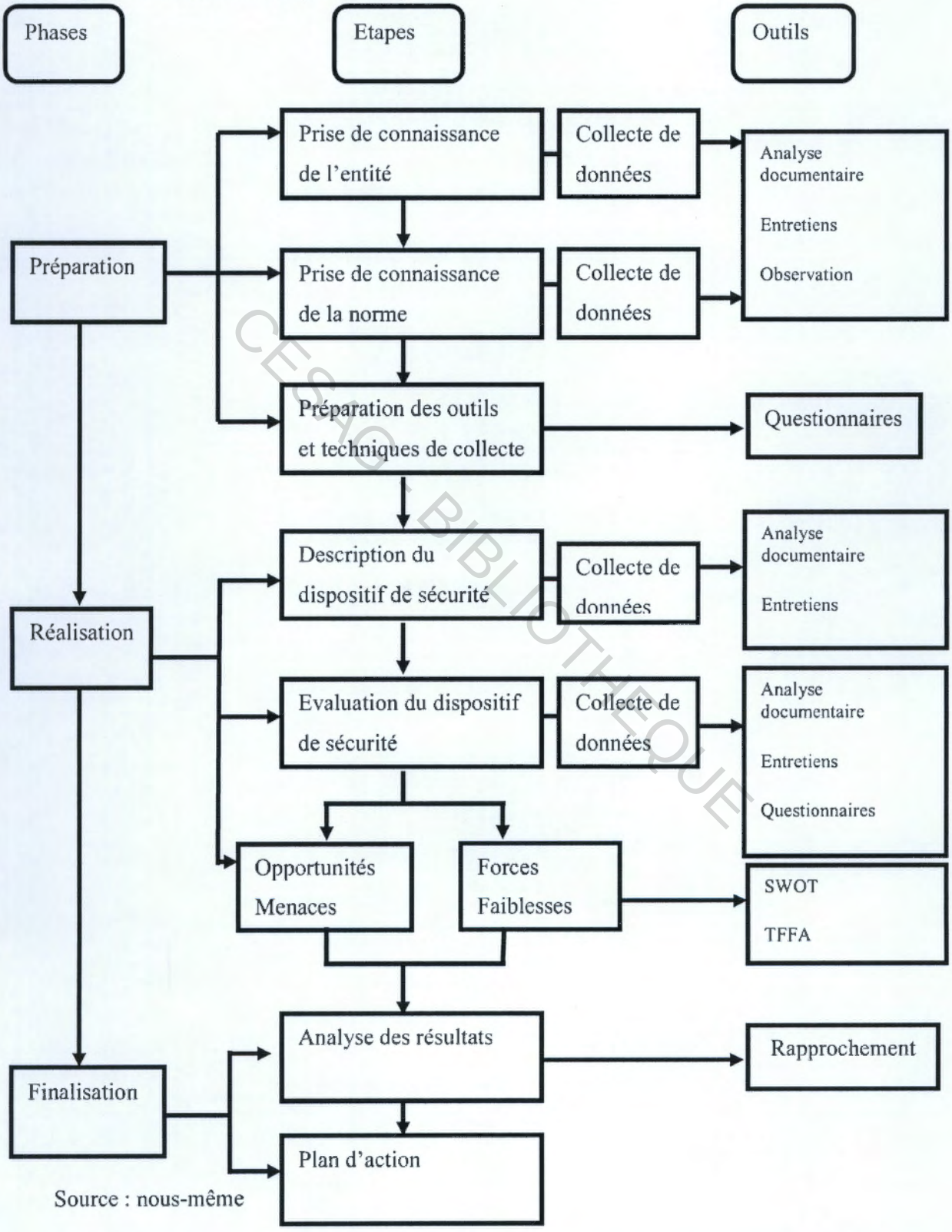
Plan d'action	
Objectifs	Il est question de rechercher des points d'amélioration qui permettront de satisfaire les objectifs.
Activités	Identification des solutions
Outils, supports méthodologiques	TFFA, Norme PCI DSS
Résultat attendu	Recommandations
Acteurs	Nous-même

Source : Nous-même

Nous présenterons ensuite schématiquement notre modèle d'analyse.

3.2 Présentation du modèle théorique d'analyse

Figure 2 : Modèle théorique d'analyse



Source : nous-même

3.3 Les outils de collecte et d'analyse de données

Les outils sont de deux ordres : de collecte et d'analyse.

3.3.1 Les outils de collecte des données

Afin de mener à terme notre étude, la nécessite de recueillir l'information s'est imposée à nous. Il nous est alors parut opportun d'user des trois grandes catégories d'outil de collecte des données.

Selon LESSARD-HERBERT & al. (1997 : 92), « ces trois catégories, que De Bruyne et al. nomment les modes de collecte des données sont :

- l'enquête, qui peut prendre une forme orale (l'entrevue ou l'entretien) ou écrite (le questionnaire) ;
- l'observation, qui peut avoir une forme directe systématique ou participante ;
- l'analyse documentaire ».

➢ L'entretien

Intervenant à plusieurs étapes de notre étude, l'entretien nous a permis de collecter des données nécessaires à :

- la prise de connaissance de l'entité : dès notre arrivée, pour se familiariser avec la Banque dans sa globalité, nous avons eu un entretien avec notre l'encadreur. Il s'effectuait oralement par un jeu de questions-réponses qui avait pour but de nous informer sur les aspects généraux de la société, c'est ainsi qu'ALBARELLO (2004 : 63), le qualifie d'entretien informatif ;
- l'évaluation : le but de l'entretien à ce niveau était de permettre une évaluation du dispositif de sécurité autour des cartes bancaires. il nous a fallu obtenir une description du dispositif de sécurité. Il s'est déroulé entre nous et les différents acteurs intervenant dans le processus de sécurisation par un échange oral et écrit au moyen d'un questionnaire d'évaluation.

- Le questionnaire

L'élaboration d'un questionnaire (voir annexe 4 et 5) est intervenue pour la phase de prise de connaissance et d'évaluation. Il avait pour but d'obtenir une meilleure compréhension de la SCBC, de son dispositif de sécurisation ainsi que de permettre l'évaluation de son degré de conformité à la norme PCI DSS. Il a été administré par nous même au moyen de formulaire à questions fermées. Les répondants étaient en ce qui concerne la prise de connaissance de la société, le Directeur des Ressources Humaines ainsi que le Chef du Département des Opérations. S'agissant de l'évaluation du dispositif de sécurité, les répondants étaient le personnel de des unités Information et Technologie ainsi que ceux du Contrôle et Support.

- L'observation

Durant notre passage dans l'entité, l'observation nous a permis pendant la prise de connaissance de voir son organisation, pendant réalisation du diagnostic de rapprocher la description faite par les documents d'usage à la réalité sur le terrain. Il s'agissait en effet de voir les employés exécuter diverses pratiques de sécurisation en matière de cartes bancaires. Nous avons pu également observer comment un client effectue une transaction de retrait de fonds dans un GAB sécurisé au moyen d'une carte bancaire.

- L'analyse documentaire

Elle est intervenue à plusieurs étapes de notre démarche et consiste à recueillir le maximum d'information au moyen des documents d'usage dans l'entité et d'autres documents de sources diverses. Elle a pour but de permettre une meilleure compréhension de l'organisation de la Banque ainsi que toutes les pratiques en matière de sécurité sur les cartes bancaires. Nous nous sommes intéressés à ce sujet entre autres au manuel de procédures relatif à la sécurisation d'une carte bancaire de sa commande à la livraison au client, au référentiel PCI DSS… « En fait, l'analyse documentaire, sorte d'analyse de contenu portant sur des documents relatifs à un site ou à une situation, correspond, du point de vue technique à une observation d'artéfacts écrits » (LESSARD-HEBERT & al, 1997 : 92).

3.3.2 Les outils d'analyse des données

Les données collectées feront l'objet d'une analyse au moyen d'outils spécifiques.

- SWOT

D'après MELOUX (2008 : 141), SWOT (voir annexe 11) est un : outil interne et externe de l'environnement d'un produit, d'un projet ou d'une entreprise. L'analyse SWOT (ou matrice SWOT), de l'anglais Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces), est un outil de stratégie d'entreprise permettant de déterminer les options critiques envisageables au niveau d'un domaine d'activité sensible.

La mise en œuvre de cet outil se fera dans notre étude à la phase de réalisation afin de procéder au diagnostic de l'existent. La construction d'une analyse SWOT s'effectue au moyen de deux diagnostics : un diagnostic externe : identification des opportunités et les menaces présentent dans l'environnement ; un diagnostic interne : identification des forces et faiblesses de la Banque.

- Tableau référentiel des forces et des risques ou Tableau des Forces et Faiblesses Apparentes (TFFA)

Le TTFA sera utilisé dans la phase de réalisation et finalisation, il servira à faire ressortir pour chaque tâche les objectifs, les risques, l'évaluation, le dispositif de contrôle interne. Son but sera de savoir si telle ou telle pratique en matière de sécurité est appliquée, dans ce cas il s'agira d'un point fort, dans le cas contraire d'une faiblesse. En définitif il est un préalable dans l'élaboration d'un plan d'action.

- Rapprochement

Une comparaison doit être faite dans la phase de finalisation entre le standard PCI DSS et la norme utilisée dans l'entité afin de déterminer les améliorations à opérer pour se conformer au standard international.

La méthodologie ainsi élaborée nous a conduit à construire notre modèle théorique d'analyse, à déterminer les outils adéquats, lesquels serviront à mettre sur pied un diagnostic fiable dans la deuxième partie de notre travail.

Au terme de notre première partie, il était question de jeter les bases permettant de poser un diagnostic efficace sur la sécurité de la carte bancaire en conformité avec la norme PCI DSS. Pour ce faire, il nous a préalablement été donné d'acquérir et de comprendre d'une part :

- l'ensemble des connaissances relatives à la carte bancaire,
- l'ensemble des connaissances relatives au Standard PCI DSS ainsi que ses exigences,

d'autre part : la démarche d'évaluation proposée par le Payment Card Industry Security Standard Council (PCI SSC).

Le décor étant planté, il convenait enfin de voir la démarche méthodologique de notre étude. Ainsi résumée la première partie dite théorique de notre mémoire, il convient à présent d'exécuter en conditions réelles le diagnostic posé d'où la partie pratique de l'étude.

DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE

La cadre théorique de notre étude nous a permis d'acquérir l'ensemble des connaissances nécessaires pour mettre en œuvre notre diagnostic. D'après PLAUCHU & al. (2008 : 8), « le diagnostic d'entreprise est un jugement porté sur la situation et la dynamique d'une entreprise ou d'une organisation en fonction de ses traits essentiels et des contraintes de son environnement et visant à identifier et améliorer la marge de manœuvre dont elle dispose pour atteindre ses objectifs, éventuellement alors redéfinis ». En d'autres termes, il s'agira non seulement d'opérer une évaluation interne (forces et faiblesses) de l'entreprise, mais également externe (opportunités et menaces) afin d'en tirer le maximum d'informations pour la prise de décision.

Le cadre pratique de notre étude portera au préalable sur la connaissance de l'entité à diagnostiquer (chapitre 4) ; sur la connaissance des processus à diagnostiquer c'est-à-dire les existants (chapitre 5) et enfin les comparer avec le standard adéquat et émettre des recommandations en d'autres terme prévoir un plan d'action (chapitre 6).

CHAPITRE 4: PRESENTATION DE LA STANDARD CHARTERED BANK CAMEROON

La monnaie étant l'élément principal dans le fonctionnement d'une économie, elle fait l'objet de plusieurs usages en fonction du besoin. Comme tout bien elle obéit à la loi de l'offre et de la demande. Son importance et son rôle ne sont plus à démontrer. Les banques l'ayant bien compris, se sont développées et manipulent avec tact cet instrument au combien prisé en la collectant et en la redistribuant contre un revenu pour ce service. Sous un aspect macro économique, le principal défi pour un pays est de stimuler la croissance afin de réduire la pauvreté. Sa stratégie serait alors de rendre le domaine bancaire compétitif en libéralisant le secteur privé ce qui permettrait l'émergence de plusieurs entreprises financées par les banques et autres établissements de crédit. L'Etat garderait toutefois un droit de regard grâce à un cadre règlementé et bien défini par des autorités monétaires en canalisant la quantité de monnaie en circulation gage du développement d'une économie. Le Cameroun, étant dans la perspective de devenir un pays émergent, il est donc important pour lui de se doter d'organismes capables de réguler le secteur bancaire, ainsi que de banques et établissement de crédits répondant aux normes internationales afin de faire face dorénavant à une concurrence non plus nationale mais internationale. Dans notre présentation, nous décrirons successivement la SCB et la SCBC ainsi que la Direction des Opérations qui nous a accueillie.

4.1 Présentation de la Standard Chartered Bank Group (SCB) et de la Standard Chartered Bank Cameroon (SCBC)

Le groupe Standard Chartered Bank est une banque fortement présente à l'échelle internationale. Son réseau offre des services bancaires dans les marchés les plus dynamiques du monde. Le slogan de la SCB, « Here for good », traduit sa volonté d'impacter positivement l'économie et les collectivités dans lesquelles elle exerce à travers la recherche de la satisfaction de ses clients. Cette Banque croit en la création de valeurs au-delà des profits et œuvre pour que chaque entreprise soit une occasion de faire du bien pour les communautés, et afin de construire une relation durable garantissant de réels avantages.

4.1.1 Historique et évolutions

Standard Chartered Bank a été créée en 1969 par la fusion de deux banques : la Standard Bank of British South Africa et le Chartered Bank de l'Inde, l'Australie et la Chine. L'expansion de ces banques s'articulait autour de l'explosion du commerce international (Europe, Asie et Afrique).

James Wilson a fondé la Chartered Bank en 1853 suite à l'octroi d'une charte royale de la reine Victoria. Tour à tour, la banque étend son réseau à Mumbai (Bombay), Calcutta et Shanghai en 1858 ensuite à Hong Kong et Singapour en 1859. La banque a joué un rôle majeur dans le développement du commerce avec l'Orient suite à l'ouverture du canal de Suez en 1869 et l'extension du télégraphe à la Chine en 1871. Traditionnellement, le commerce reposait sur le coton produit à Mumbai, l'indigo et le thé de Calcutta, le riz de la Birmanie, le sucre de Java, le tabac de Sumatra, le chanvre de Manille et la soie de Yokohama. En 1957, Chartered Bank a acheté la Banque de l'Est, ainsi que des succursales de la Banque de Chypre Ionienne et a établi une présence dans le Golfe.

La Standard Bank a été fondée dans la province du Cap en Afrique du Sud en 1862 par John Paterson, et a commencé ses activités à Port Elizabeth, l'année suivante. Elle s'est spécialisée dans le financement du développement des gisements de diamants de Kimberley à partir de 1867. Plus tard, elle a étendu son réseau plus au nord de la ville nouvelle de Johannesburg où de l'or a été découvert en 1885. En 1953, la Banque a élargi son réseau en Afrique australe, centrale et orientale et dénombrait 600 bureaux. En 1965, elle a fusionné avec la Banque de l'Afrique occidentale et étendue ses opérations au Cameroun, en Gambie, au Ghana, au Nigeria et en Sierra Leone.

4.1.2 Actionnariat et mission

C'est ainsi qu'en 1986, la Standard Chartered Bank Cameroun (SCBC) fut créée. Appartenant à la Standard Chartered Group d'origine anglaise sous la forme d'une société anonyme dont les actionnaires sont purement étrangers, son capital à sa création était supérieur à 1 000 000 000 de francs CFA. De nos jours, il s'élève à 7 000 000 000 de francs CFA en actions appartenant exclusivement aux actionnaires du Standard Chartered Group qui jugent le bilan de leur présence au Cameroun des dix dernières années comme étant satisfaisant.

4.1.3 Activités et réseau d'agences

Au sein du Groupe, plusieurs types de cartes bancaires sont émis : les cartes bancaires de retrait de billets, les cartes à débit, les cartes de crédit ... A la SCBC, seules les cartes bancaires de retraits de billets sont offertes aux clients pour des raisons liées à l'environnement économique. D'après les spécifications techniques la Banque utilise la carte à puce. C'est en 2001 que la SCBC a émis pour le compte de ses clients les premières cartes bancaires. Il y avait alors en circulation environ 1300 cartes bancaires. A la fin de l'année 2011 et à cette date l'estimation du nombre de cartes en circulation est de moins de 10 000.

Sur le territoire national comptant exactement 10 régions, le groupe est présent à travers 2 agences dans 2 régions stratégiques (le Centre et le Littoral) : la capitale politique et la capitale économique. Au niveau de la SCBC, le Service constate fréquemment des incidents sur les cartes bancaires ainsi que de la fraude. En matière de sécurité sur les cartes bancaires, le dispositif de contrôle interne pour contrer la fraude est l'application de la norme EMV (Europay, Mastercard et Visa). Outre les activités secondaires d'émission de cartes bancaires, comme toute autre banque, la Banque a pour principale activité la collecte et la distribution des crédits, particulièrement aux grandes entreprises. C'est ainsi que la contribution des revenus issus de la carte bancaire à la rentabilité ne peut être appréciée aisément car n'entrant pas dans la stratégie de la Banque.

Evoluant dans un marché à la fois international et national, au Cameroun, la SCBC est concurrencée principalement par la Citibank qui exerce son activité dans le même domaine d'activité stratégique : les grandes entreprises. Néanmoins, compte tenu du fait que la SCBC reste et demeure une banque émettant des cartes, ce qui constitue notre principal critère de comparaison, ses concurrents dans le domaine sont Afriland First Bank, BICEC, Ecobank Cameroun, UBA, SCBC, SCB CL, UBC... En terme de cartes bancaires émises, la SCBC ne peut être appliquée au classement, par contre elle occupe le dernier rang en ce qui concerne les GAB ou DAB et de couverture du territoire.

4.1.4 Structure organisationnelle et fonctionnement

Le groupe Standard Chartered Bank est organisé en société mère et ses filiales, la SCBC (voir organigramme en annexe 1) est structurée comme suit :

➢ Le Conseil d'Administration

La SCBC est gouvernée par un Conseil d'Administration composé du Président du Conseil d'Administration, du Directeur Général, du Comité d'Audit et des actionnaires. Le Conseil est en charge de la définition des grandes orientations stratégiques de la Banque, il rend compte aux actionnaires et est le conseiller du Directeur Général. C'est également à lui de s'assurer que le travail est exécuté selon les normes et politiques stratégiques de la maison mère. Il se réuni au moins une fois par an pour des raisons telles que approuver l'organigramme de la Banque, définir des orientations de la politique générale, approuver et apprécier des différents budgets, s'assurer de l'assurance de la réalisation de la politique générale.

➢ Le Directeur Général et son Adjoint

Le Directeur Général est en charge de l'application de la politique et de la stratégie définies par le groupe. Il est responsable du pilotage quotidien de la Banque, du respect de la réglementation en vigueur et de la réalisation des objectifs en accord avec les orientations stratégiques fixées par le conseil d'administration. il est nommé par ce même Conseil.

Le Directeur Général Adjoint seconde le Directeur dans l'accomplissement de ses fonctions, supervise et coordonne les activités de la Banque. Il est responsable des Institutions financières.

➢ Les directions

La SCBC renferme plusieurs directions au sein desquelles le personnel est reparti en Unités ayant des activités distinctes contribuant à la réalisation de buts communs. Ainsi, la Banque comprend :

- une direction des opérations responsable de la qualité. C'est la direction au sein de laquelle nous avons effectué notre stage. Elle fera l'objet d'une brève présentation ;
- une direction de l'audit et du contrôle interne, chargée de s'assurer que les activités se déroulent conformément aux normes prévues ;
- la direction du contentieux et du recouvrement qui gère les recouvrements des crédits douteux ;
- une direction de la conformité et de l'assurance ;

- une direction de la bonne gouvernance comprenant les ressources humaines et les affaires juridiques ; qui gèrent respectivement le personnel et les litiges ;
- une direction des affaires administratives et financières
- une direction de la clientèle chargée de gérer le portefeuille des entreprises locales et internationales.

4.2 Présentation de la Direction des Opérations

Elle est chargée de gérer les transactions des banques, le commerce extérieur, la gestion des crédits à la clientèle et les problèmes liés à l'informatique. Elle renferme en son sein plusieurs unités que sont :

- C.S.G (Client Services Group ou Service Client groupe), qui est chargé de centraliser et de répondre à toutes les réclamations des clients ;
- I.P.U (Item Processus Unit) responsable des payements locaux, internationaux ainsi que de la compensation ;
- Informatique, il est en charge de tout ce qui a trait à l'informatique, réseau, machine… en vue de maintenir l'activité de l'entreprise. Il est également responsable des activités liées aux cartes bancaires ;
- Control and support (support et contrôle), il s'occupe de la réconciliation et de l'investigation en ce qui concerne les réclamations des clients. C'est l'unité chargée du volet monétique ;
- Trade, chargé du commerce international, de gérer les transactions liées aux lettres de crédit, de garantie, et des cautions ;
- Operational risk ou risque opérationnel, s'occupant d'évaluer le risque lié aux transactions ;
- Financial market operational, concerné par les opérations liées au marché financier.

Présente dans un secteur bancaire concurrentiel, l'organisation décentralisée ainsi retracée de la SCBC, lui confère une grande flexibilité. Bien que ses différentes directions détiennent chacune des activités spécifiques, elles travaillent en synchronisation en vue d'offrir des services de qualité à ses clients. C'est ainsi que malgré que le fait que la monétique ne soit pas à la base de son métier, elle a pu émettre des cartes bancaires pour le compte de ses clients. C'est dans une logique de protection que la Banque a mis en œuvre des dispositifs de sécurité en la matière. Il convient de voir à présent quels sont ces dispositifs.

CHAPITRE 5 : DESCRIPTION DU DISPOSITIF DE SECURITE SUR LES CARTES BANCAIRES A LA STANDARD CHARTERED BANK S.A

La concurrence interbancaire pousse les banques à développer et à offrir à leurs clients plusieurs types de cartes bancaires. L'expansion de ce support électronique résulte entre autre de la confiance qu'ont ses utilisateurs. Cette confiance se trouve renforcée par un ensemble de dispositifs de contrôle interne et de protection des données des détenteurs des cartes dont les émetteurs usent. Nous verrons dans ce chapitre comment les cartes sont émises et les processus utilisés en matière de sécurité des cartes bancaires à la Standard Chartered Bank S.A Cameroon.

5.1 Les types de cartes utilisées à la Banque

La Standard Chartered Bank Group émet une gamme variée de cartes bancaires (voir annexe 12) utilisables partout dans le monde. La SCBC quant à elle offre une gamme limitée de carte permettant le retrait de billets de banque dans les DAB ou GAB uniquement contrairement à celles de la SCB qui permettent en plus les paiements en ligne et via les TPE chez les commerçants, la possibilité d'effectuer des virements… Les cartes émises par la SCB sont à puce et sont les suivantes :

- la Standard Chartered Priority Bankng Credit Card ;
- la Standard Chartered Preferred Banking Credit Card ;
- la Standard Chartered executive platinum Credit Card ;
- la Standard Chartered executive Credit Card ;
- la Standard Chartered Platinum Credit Card ;
- la Standard Chartered Titanium Credit Card ;
- la MANHATTAN Platinum Credit Card ;
- la MANHATTAN Titanium Credit Card ;
- la MANHATTAN id Platinum Credit Card ;
- la MANHATTAN id Credit Card.

Plusieurs mesures de sécurité sont utilisées pour faire face aux risques dont ces cartes peuvent faire l'objet.

5.2 Les processus utilisés en matière de sécurité sur les cartes bancaires à la Standard Chartered Bank S.A

Pour faire face aux risques sur les cartes bancaires ainsi qu'aux éventuelles fraudes dont les banques sont susceptibles de faire l'objet, la Banque a opté pour les contremesures suivantes :

- les solutions techniques caractérisées par l'utilisation des procédés cryptographiques, des audits des systèmes d'informations, des audits des équipements réseaux ;
- les solutions fonctionnelles caractérisées par l'utilisation du standard EMV pour des transactions physiques, du standard 3DSecure pour des transactions de commerce électronique, et l'authentification forte ;
- les solutions organisationnelles caractérisées par la mise en œuvre des normes internationales telles qu'ISO 27001, 27002 et 27003.

La sécurisation est fonction du type de transaction :

- sécurisation d'une transaction financière réalisée en VAD ou Internet (3DSecure) ;
- sécurisation d'une transaction financière de retrait dans un GAB : authentification de la carte et du porteur pendant la transaction ;
- sécurisation d'une transaction financière de paiement dans un TPE ou un automate de paiement ;
- gestion des transactions offline sur un TPE - Sécurité et avantage économique.

5.2.1 Sécurisation d'une transaction financière réalisée en VAD ou Internet (3DSecure)

L'utilisation du code confidentiel sur Internet n'est pas possible à ce jour car le coût d'un lecteur cryptographique côté porteur connecté à un ordinateur est rédhibitoire. Il est difficile d'assurer la confidentialité du PIN sur le poste du porteur (virus, trojan, etc.). Le PIN a une forte probabilité d'être volé en ligne. De ce fait, les institutions bancaires ont mis en place un système d'authentification du porteur différent du code confidentiel basé sur l'architecture 3D Secure.

D'après DRAGON et Al. (2002 : 81), ce système a été décidé par VISA et MASTERCARD pour éviter les fraudes de type CNP (Card Not Present). Ce sont les paiements frauduleux par carte bancaire sans présence réelle de la carte sur réseau ouvert type Internet (numéros de carte volés, par exemple).

L'objectif de 3DSecure est de réduire la fraude pour les commerçants et de sécuriser les paiements des clients. Son concept de base est de lier le processus d'autorisation financière avec une authentification en ligne. Cette authentification est basée sur un modèle comportant 3 domaines (d'où le nom 3D) qui sont le commerçant et la banque qui recevra les fonds (Acquirer Domain), la banque qui a délivré la carte de paiement (Issuer Domain) et le système de carte bancaire (Interoperability Domain)

Un paiement par carte sur internet nécessite généralement le numéro de la carte, la date d'expiration et le cryptogramme visuel.

Le cryptogramme visuel, est composé de 3 chiffres au dos de la carte qu'on vous demande généralement de saisir lors d'un achat sur internet. Ces informations peuvent être lues visuellement sur la carte et recopiées, permettant ainsi le paiement sans présence de la carte, et donc la fraude.

Avec 3DSecure, des informations complémentaires sont demandées au porteur pour l'informer, l'identifier et l'authentifier correctement, avant de valider le paiement. Par conséquent, quelqu'un qui recopierait les informations de votre carte ou même qui vous la volerait ne pourrait pas effectuer des achats chez les commerçants utilisant 3DSecure, car il ne connaît pas ces informations complémentaires.

Pour qu'un paiement soit en mode 3DSecure, il faut que la carte le soit et que le commerçant le supporte. Une carte dans ce mode peut être utilisée hors des 3 domaines. Dans ce cas, ces achats ne seront pas sécurisés. Une carte non 3DSecure, peut ou ne pas être acceptée chez les Acquirer Domain ceux-ci étant libres d'accepter ou non les paiements.

La sécurisation d'une transaction en mode 3DSecure se fait avant et pendant la transaction :

Avant la transaction, le commerçant adhère au système chez VISA ou MasterCard. Il est enregistré dans le « Brand Repository » (appelé « Directory Server »). L'Emetteur met en place ses outils : CES et ACS, il enregistre ses porteurs et donne les consignes pour

l'authentification en ligne, différente selon les systèmes. La protection est meilleure avec une authentification forte.

Un Merchant Plug In (MPI) est un logiciel qui s'interface avec le site e-Commerce pour piloter la transaction monétique pour le compte du commerçant. Pendant la transaction, le MPI va vérifier l'enregistrement des données du commerçant auprès du Directory Server. Il récupère son identifiant et les données de l'émetteur à appeler, puis effectue une demande d'authentification à l'ACS de l'Emetteur. L'ACS applique les procédures en ligne d'authentification du porteur en présentant les écrans associés (plusieurs variantes). Quand le porteur est authentifié, l'ACS calcule un cryptogramme d'authentification (jeton) et rend au MPI qui effectue sa demande d'autorisation avec les données fournies par l'ACS.

5.2.2 Sécurisation d'une transaction financière de retrait dans un GAB ou DAB : authentification de la carte et du porteur pendant la transaction

Le détenteur d'une carte bancaire peut effectuer des retraits dans un GAB ou DAB dans la mesure où son compte est approvisionné. Lorsque s'effectue la transaction, il s'opère une authentification aussi bien pour la carte que pour son porteur. Le principe est simple. La carte, étant personnalisée avec des secrets connus du seul Emetteur, elle calcule avec des clés secrètes un cryptogramme qui l'authentifie et lui donne ainsi l'autorisation de prétendre au retrait puisqu'elle aurait été reconnue comme une carte valide du système. Ce n'est que lorsque le porteur fournit son code confidentiel que la demande est remontée de manière cryptée vers l'Emetteur. Ce dernier l'analyse et vérifie le statut c'est-à-dire que, le code entré correspond bien à la carte authentifiée. Si oui la transaction est finalisée et le porteur dispose du montant souhaité. Autrement une procédure de codes erronés est déclenchée et la carte est définitivement bloquée après un certain nombre d'erreurs (généralement 3essais). Le chiffrement et le déchiffrement lors de l'échange des messages s'opèrent à travers la méthode cryptographique dite asymétrique.

5.2.2.1. Authentification de la carte EMV

« La cryptographie est la science permettant de protéger des données pour que toute personne non autorisée ne puisse lire ces données » (HUET et VERHILLE, 2007 : 172). Une carte EMV est celle qui permet la sécurisation au moyen de la norme EMV. Celle-ci définit trois

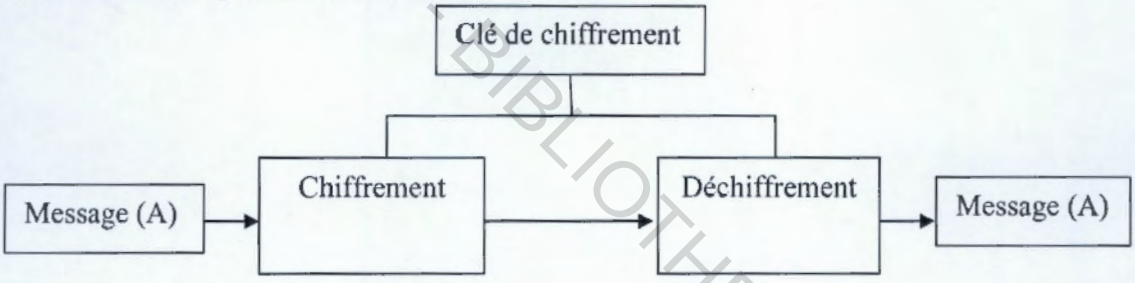
méthodes d'authentification s'appuyant sur l'algorithme à clés publiques RSA : SDA - Static Data Authentication, DDA - Dynamic Data Authentication et CDA - Combined Dynamic Data Authentication / Application Cryptogram Generation.

Un système de cryptographie basé sur la carte à puce présente deux méthodes classiques de chiffrement : soit symétrique, soit asymétrique.

Selon HUET et VERHILLE (2007 : 174-173), la cryptographie symétrique consiste pour un expéditeur et un destinataire d'un message d'utiliser la même clé respectivement pour chiffrer et déchiffrer. L'échange de clé est un préalable avant la communication. Cet échange s'effectuera au moyen d'autres canaux de communications sécurisés. Cette méthode est encore appelée algorithme à clé privée.

La figure ci-après illustre cette méthode :

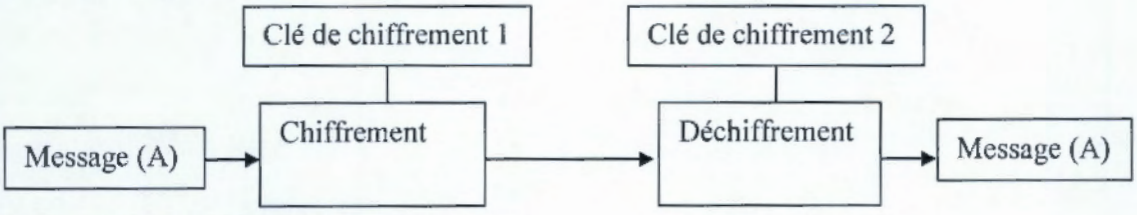
Figure 3 : Cryptographie symétrique



Source : HUET et VERHILLE (2007 : 172)

La cryptographie quant à elle nécessite une paire de clés générée par une procédure mathématique comme dans l'algorithme RSA. L'une des clés est utilisée pour le chiffrement et l'autre pour le déchiffrement. L'une peut être rendu publique et l'autre gardé secrète d'où le nom d'algorithme à clé publique.

Figure 4 : Cryptographie asymétrique



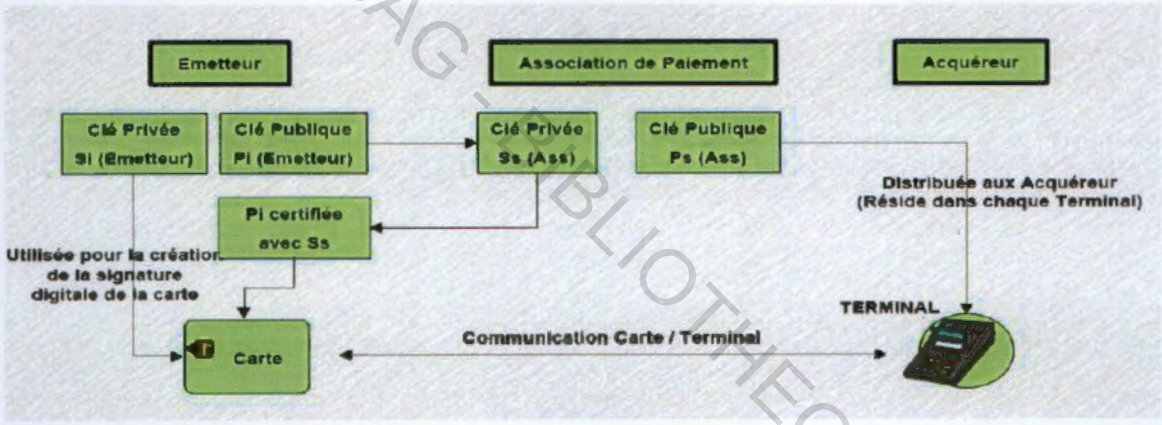
Source : HUET et VERHILLE (2007 : 172)

Ces méthodes imposent la mise en œuvre d'une infrastructure à clés publiques (PKI) par les systèmes de paiement. Elles ont pour but de garantir à l'Acquéreur que la carte a été émise par un membre du système de paiement (SDA / DDA / CDA), que les données financières lues dans la carte sont celles définies par l'Emetteur (SDA / DDA / CDA), que la carte est bien délivrée par l'Emetteur (DDA / CDA), et enfin de permettre à l'Acquéreur d'authentifier les échanges de données entre la carte et les terminaux (CDA).

5.2.2.1.1 Authentification de la carte à EMV / SDA

Le processus SDA (Static Data Authentication) consiste pour le terminal à vérifier une donnée signée inscrite dans la carte durant sa personnalisation. Il se présente ainsi :

Figure 5 : Processus SDA



Source : RAO & Al. (2007 : 183)

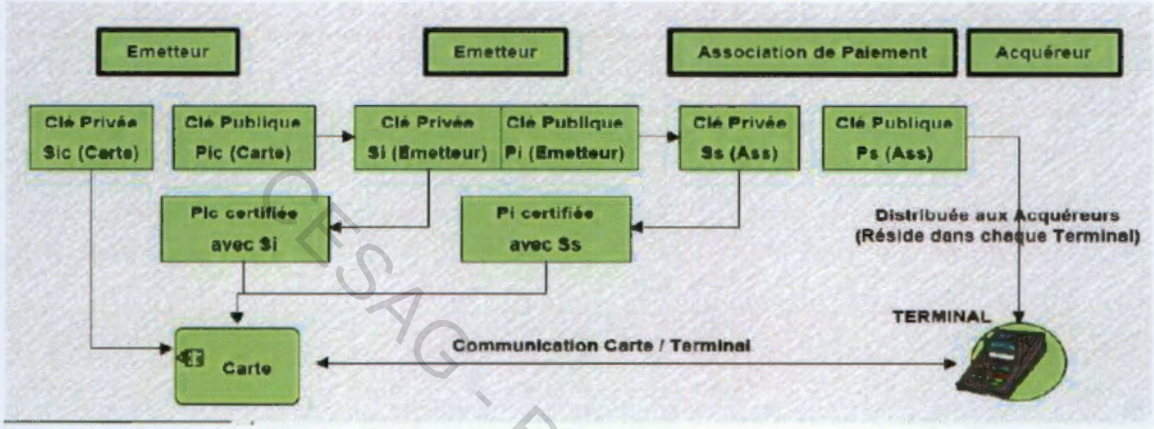
Pendant la phase de personnalisation, la carte reçoit les informations suivantes: le nom du porteur, le numéro de la carte ou encore la date limite de validité de celle-ci (notés « Information »), la valeur d'authentification (noté VA), la signature numérique RSA d'Informations générée avec la partie privée de la clé de l'émetteur VA=SigEpriv (Information), le certificat électronique de l'émetteur (Ecert) contenant sa clé publique signée par une autorité de certification, et le code PIN transmis au porteur de cette carte.

Avant toute transaction, la carte fournit au terminal « Informations », le certificat ECert de la banque émettrice, ainsi que la valeur d'authentification VA. Le terminal vérifie Ecert avec la clé publique de l'autorité de certification (CApub) et vérifie VA avec la clé publique de la banque émettrice. Il demande à l'utilisateur le code confidentiel (PIN) et le transmet (en clair c'est-à-dire sans chiffrement électronique) à la carte pour qu'elle le vérifie.

5.2.2.1.2 Authentification de la carte à EMV / DDA

Le processus DDA (Dynamic Data Authentication) vérifie en plus d'une authentification statique (vérification d'une donnée inscrite durant la personnalisation), si la carte possède un secret délivré par l'émetteur de la carte. Il se présente ainsi :

Figure 6 : Processus d'authentification DDA



Source : RAO & Al. (2007 : 183)

Pendant la phase de personnalisation, la carte reçoit comme informations le nom du porteur, le numéro de la carte ou encore la date limite de validité de celle-ci (notés « Information »), une paire de clés RSA (Cpub, Cpriv), un certificat (Ccert) contenant Cpub signé par l'émetteur, le certificat de l'émetteur (Ecert) contenant sa clé publique Epub signé par une autorité de certification et le code confidentiel PIN transmis au porteur de cette carte.

Avant toute transaction la carte fournit au terminal « Informations », le certificat « Ecert » de la banque émettrice, et son certificat Ccert. Le terminal génère une valeur aléatoire « Talea » et l'envoie à la carte qui génère une valeur aléatoire « Calea » puis, elle signe « Talea » et « Calea» avec sa clé privée « Cpriv ». Elle envoie le résultat de la signature et « Calea » au terminal lequel vérifie « Ecert » avec « Capub », « Ccert » avec « Epub » et la signature des aléas avec « Cpub ». Le terminal demande à l'utilisateur le code confidentiel (PIN) et le transmet (chiffré par « Cpub ») à la carte pour qu'elle le vérifie. Le code PIN est d'abord concaténé avec deux nouvelles valeurs aléatoires fournies par la carte et le terminal, afin d'éviter les attaques par « rejeu ».

5.2.2.1.3 Authentification de la carte à EMV / CDA

Le processus CDA (Combined Data Authentication) prend en compte la variante de DDA et utilise TC (Transaction Certificate) qu'il inclut dans le bloc de données signé par la carte.

La transaction est finalisée soit en ligne ou hors ligne, ce choix est fait par la carte et le terminal selon une politique de gestion de risques (sélection aléatoire, validation en ligne pour N validations hors ligne, en fonction du montant de la transaction, en fonction du montant cumulé des transactions déjà effectuées hors ligne ou d'un plancher fixé par le marchand).

Si la transaction doit être approuvée en ligne, le terminal envoie à la banque émettrice le cryptogramme généré par la carte

- ARQC Authorization ReQuest Cryptogram.

La banque le vérifie et génère un cryptogramme réponse envoyé à la carte via le terminal

- ARPC Authorization ResPonse Cryptogram

Le terminal redemande alors à la carte de lui générer un certificat de transaction qui inclut l'autorisation de la Banque.

5.2.2.2. Authentification du porteur de la carte.

L'objectif visé pendant la transaction est de vérifier que celui qui utilise la carte est son véritable possesseur ayant signé le contrat porteur. L'authentification du porteur de la carte se fait au moyen d'un code confidentiel (Transactions Physiques) appelé PIN : Personal Idenfier Number et l'utilisation de données personnelles connues du seul porteur ou lui appartenant : Authentification forte.

5.2.2.2.1 Sécurisation au moyen d'un code confidentiel

Le code confidentiel (PIN) est généré par l'Emetteur soit automatiquement lors de la personnalisation de la carte, soit en demandant au Porteur de faire le choix de son code confidentiel. Les systèmes d'émission instantanée se prêtent au choix du code par le porteur. Il existe également des systèmes avancés de changement de code confidentiel au cours du cycle de vie de la carte. Un processus complexe et sécurisé calcule puis enregistre sur la carte

et dans les serveurs centraux, les cryptogrammes permettant de vérifier un PIN. Le Porteur entre son code confidentiel soit lors d'un retrait sur les DAB : grâce à un clavier sécurisé, soit lors d'un paiement sur les Terminaux de paiement électronique (TPE) : grâce à un PIN PAD sécurisé. Le code confidentiel saisi est immédiatement encodé dans un PIN BLOCK, puis chiffré avant d'être transporté comme l'indique la figure en annexe 14.

Après le transport, vient la vérification du PIN effectuée par les SAE (Système d'Autorisation Emetteur). Le PIN et le PIN BLOCK ne sont jamais décodés ; un module cryptographique contenant les bonnes clés de l'émetteur se charge de reconstituer, à partir du PIN BLOCK, un cryptogramme de référence qui sera comparé à celui enregistré dans les bases centrales lors de la génération du PIN.

5.2.2.2.2 Sécurisation au moyen d'une authentification forte.

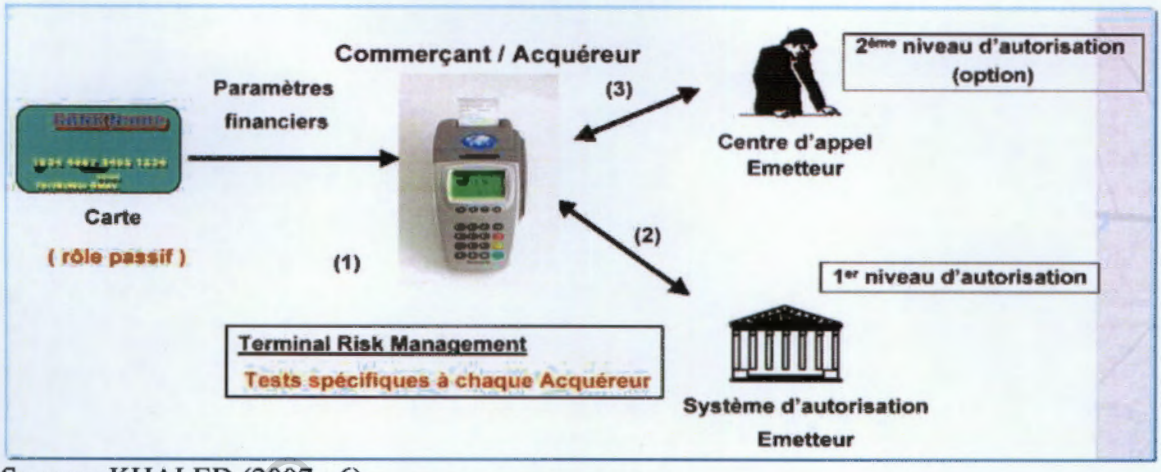
Plusieurs modes d'authentification forte peuvent être utilisés :

- utilisation d'une carte matricielle (voir figure 10 en annexe 13) ;
- utilisation du téléphone mobile (sms) ou du mail. Le porteur saisit son login et mot de passe, la demande est transmise à l'émetteur, l'émetteur fait des vérifications nécessaires, un OTP est envoyé au porteur par son mobile ou par internet, le porteur utilise l'OTP pour la transaction ;
- utilisation d'un token basé sur le temps (voir figure 11 annexe 13) ;
- utilisation d'un token basé sur le compteur (voir figure 12 en annexe 13) ;
- utilisation d'un token basé sur un mécanisme de challenge/réponse (voir figure 13 en annexe 13).

5.2.3 Sécurisation d'une transaction financière de paiement dans un TPE ou un automate de paiement

Le traitement de la transaction au niveau du terminal s'appuie sur les règles définies par les systèmes de paiement et sur la politique de gestion du risque de l'acquéreur. La sécurisation se traduit par deux niveaux d'autorisation comme le montre le schéma suivant :

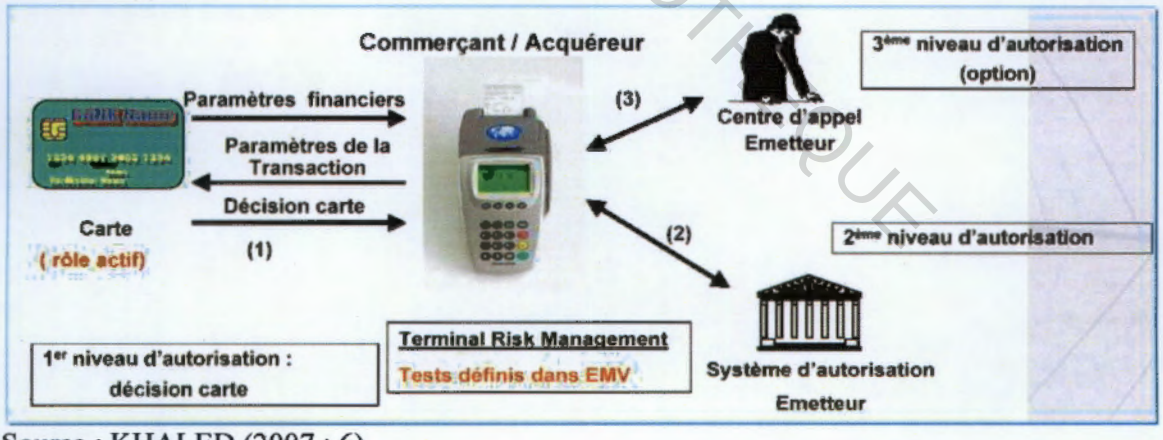
Figure 7 : Traitement d'une transaction sur TPE



Source : KHALED (2007 : 6)

Le traitement de la transaction au niveau du TPE s'appuie également à la fois sur la politique de l'émetteur (basé sur des recommandations de systèmes de paiement) et sur la politique de l'acquéreur (conforme aux règles des Systèmes de Paiement). La sécurisation se traduit par trois niveaux d'autorisation comme le montre le schéma suivant :

Figure 8 : Niveau d'autorisation lors d'une transaction sur TPE



Source : KHALED (2007 : 6)

L'évolution de l'environnement a induit l'émergence de nouveaux risques sur les cartes bancaires. Tout comme les principaux acteurs de lutte contre la fraude travaillent pour mettre sur pied des dispositifs efficaces, de même les fraudeurs imaginent des scénarii pour les contourner. Etant développé par les trois grands groupes de fabricants de cartes (Europay, Mastercard et Visa) en 1994, la norme EMV prend donc en considération leurs différents programmes avec parfois des incohérences. Ceci implique des limites à l'harmonisation des politiques de sécurité, puisque tous les acteurs n'étaient pas réunis. C'est pour remédier à ce manquement que le standard international PCI DSS a vu le jour. L'obligation est donc faite à tous les Emetteurs de cartes appartenant à ces différents grands réseaux de se conformer à ce standard sous peine de sanctions. Les banques en général et en particulier la Standard Chartered bank devraient se conformer à ce standard afin de disposer des meilleures pratiques reconnues sur le plan international. Il serait donc nécessaire pour atteindre cet objectif de connaître l'état des lieux de la SCBC dans le domaine afin de savoir si les dispositifs en place sont fiables, efficaces et adéquats, c'est ce à quoi nous allons nous atteler dans le prochain chapitre à savoir : L'évaluation du niveau de conformité à la norme PCI DSS et le plan d'action à la SCBC.

CHAPITRE 6: EVALUATION DU NIVEAU DE CONFORMITE A LA NORME PCI DSS ET PLAN D'ACTION A LA STANDARD CHARTERED BANK CAMEROON S.A

Le chapitre précédent nous a permis de dresser un état des lieux de la sécurité sur les cartes bancaires à la SCBC, ce qui est un préalable à l'évaluation. Ainsi, les transactions réalisées à partir de la carte bancaire émise par la SCB sont sécurisées grâce à la norme EMV (Europay Mastercard et Visa). Il convient donc à présent de voir si les dispositifs de sécurité en matière de cartes bancaires à la Banque permettent d'atteindre les objectifs pour lesquels ils ont été mis en place. Notre travail consistera donc en général à procéder à un audit de conformité en comparant les standards EMV et PCI DSS. Il en résultera tour à tour une énumération des forces et des faiblesses de la sécurité des cartes bancaires, les risques qui en découlent ainsi que l'évaluation de ceux-ci, enfin le plan d'action des mesures à prendre pour se conformer au standard PCI DSS.

6.1 Les forces et les faiblesses de la sécurité des cartes bancaires au sein de la Standard Chartered Bank Cameroun

En se servant de l'outil SWOT (voir annexe 11) présenté dans la méthodologie de l'étude et du questionnaire d'évaluation PCI DSS, nous avons fait ressortir les forces et les faiblesses de la sécurité sur les cartes bancaires classées selon les exigences du standard PCI DSS.

6.1.1 Forces de la sécurité sur les cartes bancaires selon le PCI DSS

- **Création et gestion d'un réseau sécurisé (Exigence 1)**

La Banque utilise des pare-feux nécessaires à la gestion d'un réseau sécurisé comme l'exige la norme PCI DSS. La configuration de pare feux limite les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données des titulaires de cartes à la Banque. Nous avions effectuer un test de permanence à ce niveaux.

L'interdiction d'accès public direct entre internet et tout composant du système dans l'environnement des données des titulaires des cartes est effective car à la Banque, internet n'est pas dans le même réseau que tous les autres composants du système (Condition 1).

Les normes de configuration couvrent toutes les vulnérabilités pour tous les composants du système (Condition 2).

- **Gestion d'un programme de vulnérabilités (Exigence 3)**

La Banque utilise des logiciels antivirus et les met à jour régulièrement tel que le stipule le standard PCI DSS. Elle développe et gère des systèmes basés sur des applications sécurisés tel que NORTON. Un test de permanence à été effectué durant notre séjour dans la Banque.

- **Mise en œuvre de mesures de contrôle d'accès strictes (Exigence 4)**

En général pour cette exigence toutes les conditions énumérées par le standard sont appliquées par le dispositif EMV de la Banque. En particulier, en ce qui concerne la gestion des mots de passe et l'authentification des utilisateurs, tous les mots de passe sont changés par les informaticiens systématiquement et régulièrement sans distinction. Les paramètres d'authentification sont configurés pour exiger un verrouillage d'un compte d'utilisateur après 3 tentatives de connexion non valides au lieu des 6 tentatives prévues par le standard PCI DSS. Les mots de passe sont valides pour une durée de 90 jours et leur composition dépend de l'utilisateur (Condition 2 : 8.5 ; W)

- **Surveillance de tests réguliers des réseaux (Exigence 5)**

La Banque définit un processus pour associer chaque accès aux composants du système à chaque utilisateur individuel tel que le demande la norme (Condition 1 :10.1). Elle met en œuvre des vérifications à rebours automatisées pour tous les composants du système (Condition 1 :10.2). Elle consigne dans les vérifications à rebours les ID d'utilisateurs, les types d'évènement, l'horodatage, l'indication de succès ou d'échec, l'origine de l'évènement, l'identité ou le nom des données (Condition 1 :10.3).

- **Gestion d'une politique de sécurité des informations (Exigence 6)**

La Banque gère une politique de sécurité des informations pour l'ensemble du personnel. En plus de la possibilité d'examiner la documentation de l'évaluation des risques requise (12.1, D) la personne examinatrice doit avoir une autorisation. Elle élabore des politiques d'utilisation des technologies stratégiques (12.2), et pour les fournisseurs et partenaires

commerciaux, ils n'ont pas d'accès à distance car ils ne sont même pas connectés au système (Condition 1).

6.1.2 Faiblesses de la sécurité sur les cartes bancaires selon le PCI DSS

Les faiblesses liées au dispositif de sécurité de la banque sont les suivantes :

- **création et gestion d'un réseau sécurisé (Exigence 1)**

Le cryptage de tous les accès administratifs ne se faisant pas via une fenêtre graphique type invite de commande windows (non-console) à l'aide d'une cryptographie robuste n'est pas appliqué à la Banque (Condition 2 :2.3).

- **protection des données des titulaires des cartes de crédit (Exigence 2)**

Les cartes ne sont pas fabriquées localement et répondent en principe aux exigences EMV, de ce fait, le système EMV n'empêche pas toujours l'accès inapproprié aux données ainsi que la protection de la confidentialité des données du titulaire ou les informations d'identification sensibles. En effet, le PAN, la date d'expiration et d'autres données sont rendus lisibles lors d'une transaction non-EMV sur le terminal (Condition 1 : 3.3 ; 3.4)

- **surveillance de tests réguliers des réseaux (Exigence 5)**

L'on ne peut s'assurer tel que l'exige la norme que :

- tous les systèmes d'horloge et temporels critiques sont mis en œuvre pour l'acquisition, la distribution et l'enregistrement du temps (Condition 1 : 10.4) ;
- les vérifications à rebours sont protégées de sorte qu'elles ne puissent pas être modifiées (Condition 1 : 10.5).

Les systèmes d'horloge et temporels critiques, ainsi que les vérifications à rebours sont gérés par la Standard Chartered Bank Afrique du Sud. Elle s'occupe de toutes les questions d'ordre technique (maintenance et gestion de la plate forme…) du groupe concernant la zone Afrique.

L'on ne peut tester la présence de points d'accès sans fil et détecter les points d'accès sans fil non autorisés tous les trimestres selon la norme car le dispositif de test n'existe pas dans la Banque (Condition 2 : 11.1).

L'On ne peut s'assurer :

- d'analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux (Condition 2 : 11.2) ;
- si les tests de pénétration sont effectués (Condition 2 : 11.3) ;
- si des systèmes de détection d'intrusions ou de prévention d'intrusion sont utilisés (Condition 2 : 11.4) ;
- que des logiciels de contrôle de l'intégrité des fichiers pour alerter le personnel de toute modification non autorisés des fichiers de configuration sont déployés (Condition 2 : 11.5).

L'analyse des vulnérabilités (autres que les antivirus), les tests de pénétration, les systèmes de détections d'intrusions et les logiciels de contrôle d'intégrité sont quasi inexistants car la SCBC ne dispose pas sur place du matériel adéquat. Le rôle des gestionnaires de réseau se limite à la maintenance des systèmes.

6.1.3 Opportunités

En général, toutes les exigences en matière de sécurité définies par le standard PCI DSS sont en partie couvertes par la SCBC. Dans un souci de s'aligner avec les standards internationaux, il serait donc plus facile de se conformer totalement à la norme PCI DSS car 4 exigences sur 6 sont plus ou moins respectées. Mais il est à noter que malgré cette majorité, l'exigence la plus sensible à savoir la protection des données des titulaires de carte de crédit, n'est pas remplie à la Banque.

6.1.4 Menaces

Les menaces dont la Banque est susceptible de faire l'objet sont :

- **création et gestion d'un réseau sécurisé (Exigence 1)**

Le changement des mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur du mot de passe n'est pas garanti. Dans ses relations avec ses clients, la Banque échange des informations via des dossiers zippés et cryptés. Les codes d'accès fournis par la Banque aux clients ne sont généralement par changés par ces derniers, ceux-ci demandent souvent le rappel de ces accès en cas d'oubli par conséquent, un intrus connaissant ces mots de passe par défaut peut entrer se connecter au réseau interne de la Banque.

- **protection des données des titulaires des cartes de crédit (Exigence 2)**

Les cartes bancaires de la SCBC n'étant pas fabriquées localement, elles ne prennent pas en compte l'évolution de l'environnement. Bien plus, entre leur commande et leur livraison aux clients, leur intégrité ne peut être totalement garantie. En effet, le client qui désire disposer d'une carte, se rend à l'Agence et adresse une demande accompagnée d'un formulaire à compléter mis à sa disposition par la Banque. La SCBC fait donc suivre la demande à son service technique en Afrique du Sud lequel passe commande auprès de son fournisseur qui fabrique la carte selon les spécificités de la Banque. Ensuite intervient le processus qui va de la conception à la personnalisation. Après fabrication, la carte fait le chemin inverse jusqu'au client. Ce processus étant long la carte peut être volée ou dupliquée.

- **mise en œuvre de mesures de contrôle d'accès strictes (Exigence 4)**

Pour la condition2, point 8.4 à savoir rendre tous les mots de passe illisibles pendant la transmission et le stockage, pour les prestataires de service uniquement, l'on ne peut vérifier que les mots de passe des clients sont cryptés car non applicable à la Banque.

- **Surveillance de tests réguliers des réseaux (Exigence 5)**

Il serait possible de modifier l'intégrité des fichiers de configuration, des fichiers de contenu ou fichiers système stratégiques en cas d'absence de logiciel de contrôle. La modification de

l'environnement technologique pourrait entraîner de nouvelles menaces, qui rendraient l'infrastructure ou l'application désuète.

Ces faiblesses et menaces rendent ainsi vulnérables la Banque qui devient alors sujette à de nombreux risques.

6.2 Univers de risques liés aux cartes bancaires : maîtrise des risques et de la fraude

L'analyse précédente portant sur l'examen de la conformité de la Banque au standard PCI DSS, fait ressortir des faiblesses et menaces ci-dessus citées. Il s'en suit un TFFA qui présente pour chacune des exigences de la norme, les objectifs, les risques, leur évaluation, le dispositif de contrôle interne pour pallier au risque, son existence dans la Banque et l'interprétation.

Tableau 10 : Tableau des forces et faiblesses apparentes

Tâches	**Objectifs**	**Risques**	**Evaluation**	**Dispositifs de contrôle interne**	**Existence**	**Interprétation**
Création et gestion d'un réseau sécurisé	Protéger les données des titulaires de cartes	Piratage, harking, accès non autorisé, virus.	Important	Pare-feu, antivirus, ne pas utiliser les mots de passe par défaut	M.C	
Protection des données des titulaires des cartes de crédit	Impossibilité de lire ou utiliser les données en cas de piratage	Stockage des données d'authentification sensibles après autorisation, duplication des cartes	Important	Cryptage, troncature, hachage, masquage	M.C	
Gestion d'un programme de vulnérabilités	Protéger contre les menaces logicielles actuelles ou futures. Empêcher l'altération et l'exploitation des données des titulaires de carte	Transmission des PAN par email, intrusion, reproduction des cartes, vente des données codes confidentiels	Important	Logicielles antivirus, Correctifs logiciels appropriés les plus récents.	M.C	
Mise en œuvre de mesures de contrôle d'accès strictes	Rendre l'accès aux données stratégiques au seul personnel autorisé.	Utilisation frauduleuse du compte utilisateur	Important	Droit d'accès, système de contrôle automatique, formulaire d'autorisation, ID unique à chaque utilisateur.	M.C	

Tableau 10 : Tableau des forces et faiblesses apparentes (suite)

Tâches	**Objectifs**	**Risques**	**Evaluation**	**Dispositifs de contrôle interne**	**Existence**	**Interprétation**
Surveillance de tests réguliers des réseaux	Prévenir, détecter, minimiser l'impact d'une altération, s'assurer que les contrôles de sécurité reflètent toujours les nouveaux environnements.	Impossibilité de suivre les activités, Absence d'alerte, absence de journaux retraçant les activités du système	Important	Système de détection d'intrusion, mécanismes de journalisation, tests fréquent des composants du système	M.C	
Gestion d'une politique de sécurité des informations	Définir la sécurité mise en œuvre à l'échelle de l'entreprise, et indiquer aux employés ce qu'on attend d'eux.	Emergence de nouveaux risques et menaces, méconnaissance de la portée globale des tâches, utilisation des technologies contrevenant à la politique de l'entreprise en cas d'absence de politique.	Important	Sensibilisation des employés au caractère sensible des données, mise à jour de la politique de sécurité.	M.C	

Source : nous-même

6.3 Evaluation des risques sur les cartes bancaires à la SCBC

Dans cette section nous verrons le tableau d'évaluation des risques proprement dites ainsi que la matrice de criticité.

6.3.1 Tableau d'évaluation des risques

Les risques étant identifiés, il est question de les évaluer. L'évaluation des axes probabilité et gravité est faite sur une échelle de 0 à 10 pour chaque risque par nous-même comme évaluateur 1 et par un pair pour l'évaluateur 2.

Eléments d'évaluation

La probabilité moyenne est la moyenne des probabilités données pour un risque et par chaque évaluateur. Elle est obtenue par la formule suivante :

Moyenne des probabilités = 1/N * (probabilité 1 + probabilité 2 + …+ probabilité n)

Avec N, le nombre d'évaluateurs et n, le rang du score.

La gravité moyenne est la moyenne des gravités données pour un risque par chaque évaluateur. Elle est obtenue par la formule suivante :

Moyenne des gravités = 1/N * (gravité 1 + gravité 2 + … + gravité n)

La criticité moyenne est le produit de la probabilité et la gravité moyenne c'est-à-dire :

Criticité moyenne = probabilité moyenne * gravité moyenne

L'écart-type de la probabilité ainsi que celui de la gravité sont données par les formules suivantes :

Ecart-type des probabilités = 1/N * (probabilité 1 + probabilité 2 + …+ probabilité n)

Moyenne des gravités = 1/N * (gravité 1 + gravité 2 + … + gravité n)

En définitif, le tableau d'évaluation des risques est le suivant :

Tableau 11 : Evaluation des risques à la SCBC

C.E	Exigence	C.R	Libellé du risque	E1		E2		Synthèse des évaluations				
				P	G	P	G	P.M	E.P	G.M	E.G	C.M
C.1	Création et gestion d'un réseau sécurisé	R.1.1	Piratage	3	7	2	8	2,5	0,71	7,5	0,71	18,75
C.1	Création et gestion d'un réseau sécurisé	R.1.2	Harking	7	8	5	7	6	1,41	7,5	0,71	45
C.1	Création et gestion d'un réseau sécurisé	R.1.3	Accès non autorisé	2	8	3	7	2,5	0,71	7,5	0,71	18,75
C.1	Création et gestion d'un réseau sécurisé	R.1.4	Virus	8	7	6	6	7	1,41	6,5	0,71	45,5
C.2	Protection des données des titulaires des cartes de crédit	R.2.1	Stockage des données d'authentification sensibles après autorisation	2	9	3	8	2,5	0,71	8,5	0,71	21,25
C.2	Protection des données des titulaires des cartes de crédit	R.2.2	Duplication des cartes	1	10	2	9	1,5	0,71	9,5	0,71	14,25
C.3	Gestion d'un programme de vulnérabilités	R.3.1	Transmission des PAN par email	5	7	5	8	5	0	7,5	0,71	37,5
C.3	Gestion d'un programme de vulnérabilités	R.3.2	Intrusion	1	8	1	10	1	0	9	1,41	9

Source : nous-même

Tableau 11 : Evaluation des risques à la SCBC (suite)

C.3	Gestion d'un programme de vulnérabilités	R.3.3	Reproduction des cartes	1	9	1	10	1	0	9,5	0,71	9,5
	Gestion d'un programme de vulnérabilités	R.3.4	Vente des données codes confidentiels	1	10	1	10	1	0	10	0	10
C.4	Mise en œuvre de mesures de contrôle d'accès strictes	R.4	Utilisation frauduleuse du compte utilisateur.	2	6	4	7	3	1,41	6,5	0,71	19,5
C.5	Surveillance de tests réguliers des réseaux	R.5.1	Impossibilité de suivre les activités	6	5	4	7	5	1,41	6	1,41	30
C.5	Surveillance de tests réguliers des réseaux	R.5.2	Absence d'alerte	7	8	6	9	6,5	0,71	8,5	0,71	55,25
C.5	Surveillance de tests réguliers des réseaux	R.5.3	Absence de journaux retraçant les activités du système	7	8	4	8	5,5	2,12	8	0	44
C.6	Gestion d'une politique de sécurité des informations	R.6.1	Emergence de nouveaux risques et menaces	7	5	8	6	7,5	0,71	5,5	0,71	41,25
C.6	Gestion d'une politique de sécurité des informations	R.6.2	Méconnaissance de la portée globale des tâches	6	8	7	7	6,5	0,71	7,5	0,71	48,75
C.6	Gestion d'une politique de sécurité des informations	R.6.3	Utilisation des technologies contrevenant à la politique de l'entreprise en cas d'absence de politique	4	9	5	8	4,5	0,71	8,5	0,71	38,25

Source : nous-même

Dans ce tableau, C.E est le code de l'exigence ; C.R, le code du risque ; E.1, l'évaluateur 1 ; P, la probabilité ; G, la gravité ; P.M, la probabilité moyenne ; G.M, la gravité moyenne ; E.P, l'écart-type probabilité ; E.G, l'écart-type gravité ; C.M, la criticité moyenne. Il en résulte la matrice de criticité.

6.3.2 Matrice de criticité

Le tableau précédent nous à permis d'évaluer les risques. La prochaine étape consistera à la restitution sous forme de nuage de point dans une matrice de criticité. Selon AUTISSIER & Al. (2007: 227), les risques identifiés sont ensuite placés dans la matrice de criticité selon leur probabilité et leur probabilité d'occurrence. Pour ce faire, le tableau ci-dessous résume cette évaluation.

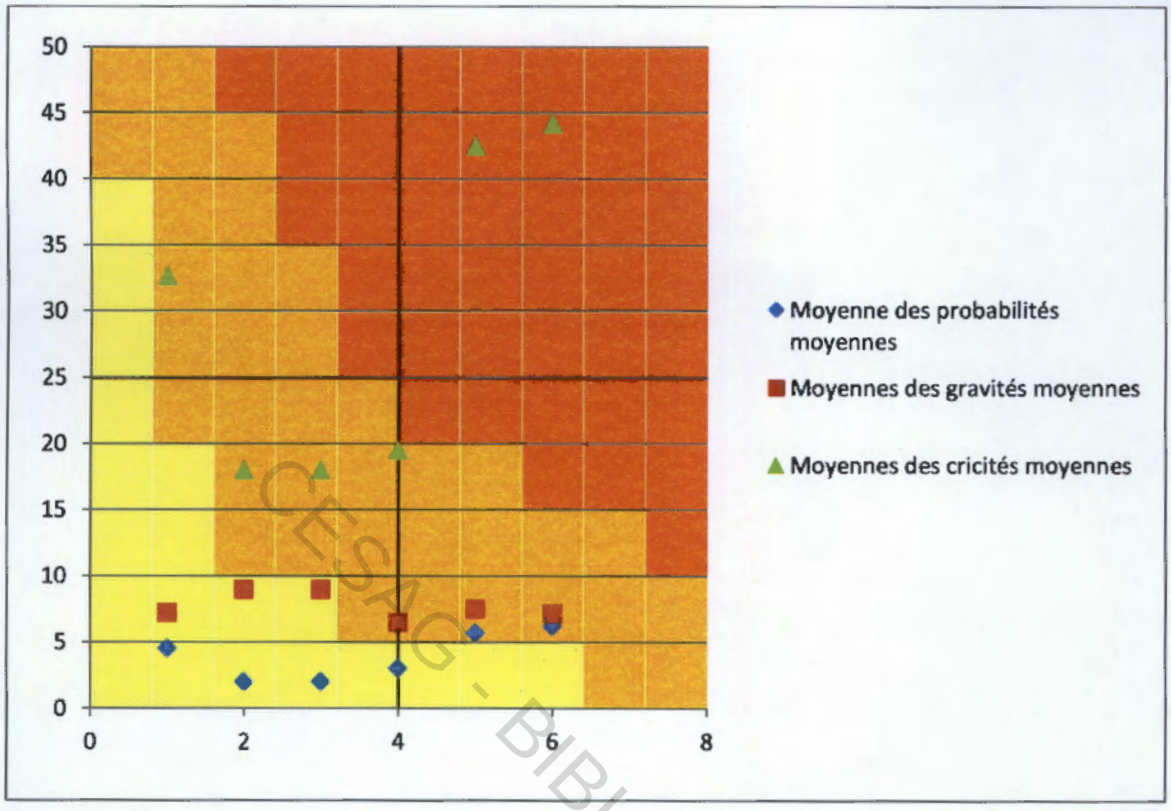
Tableau 12 : Résumé de l'évaluation des risques à la SCBC

EXIGENCES	Moyenne des probabilités moyennes	Moyennes des gravités moyennes	Moyennes des criticités moyennes
Création et gestion d'un réseau sécurisé	4,5	7,25	32,625
Protection des données des titulaires des cartes de crédit	2	9	18
Gestion d'un programme de vulnérabilités	2	9	18
Mise en œuvre de mesures de contrôle d'accès strictes	3	6,5	19,5
Surveillance de tests réguliers des réseaux	5,67	7,5	42,5
Gestion d'une politique de sécurité des informations	6,17	7,17	44,194

Source : nous -même

De ce résumé de l'évaluation des risques, la matrice de criticité suivante est déduite.

Figure 9 : Matrice de criticité.



Source : nous-même à partir d'AUTISSIER & al. (2007 : 227)

Interprétation :

- la zone dont la criticité est comprise entre 0 et 7,5 : les risques situés dans cette zone sont peu critiques. Il conviendrait d'énumérer et mettre en place des dispositifs de contrôle interne de manière spécifique à chaque risque et en fonction de leur coût ;
- la zone dont la criticité est comprise entre 7,5 et 10 : les risques situés dans cette zone ont une criticité moyenne. Une nouvelle politique de sécurité des cartes à la SCBC doit être intégrée dans le processus de décision pour leur traitement ;
- la zone dont la criticité est comprise entre 10 et 45 : les risques situés dans cette zone sont extrêmement critiques. L'absence de leur traitement peut remettre en cause la sécurité des cartes bancaires. Les mesures PCI DSS dans ce cas seraient une contrainte à intégrer impérativement.

En vu d'améliorer, la sécurité sur les cartes bancaires à la SCBC, il est opportun de définir un plan d'action.

6.4 Plan d'action vers la conformité à la norme PCI DSS

A l'origine, le domaine Emetteur était peu concerné par les mesures PCI qui se sont historiquement concentrées sur le domaine acquéreur et accepteur. Depuis peu, il est demandé aux Emetteurs de se mettre en conformité PCI-DSS pour protéger leurs données. Le PCI-DSS concerne essentiellement les systèmes bancaires à travers la protection des réseaux d'autorisation, la protection du système d'autorisation et la protection du système Back Office de création, fabrication et gestion de la carte. De manière générale, les Emetteurs se doivent de bâtir un plan d'actions qui portera sur :

- **les réseaux**
- sécurisation des liens ;
- création de LAN virtuels étanches ;
- cryptage des données sur les liens (messages temps réel et fichiers).

- **systèmes**
- mise à jour périodique et systématique des Systèmes d'exploitation, des middlewares et outils standards ;
- configuration et maintien opérationnel des anti-virus et pare-feu.

- **applications**
- faire appliquer la certification PA-DSS aux éditeurs de logiciels ;
- demander aux sous-traitants leurs certifications ;
- faire passer les certifications aux systèmes internes.

En particulier, l'ensemble des recommandations formulées à l'endroit de la Standard Chartered Bank Cameroon en vue d'améliorer la sécurité sur les cartes bancaires et par ricochet de tendre vers une conformité aux exigences du standard PCI DSS sont les suivantes :

- **création et gestion d'un réseau sécurise**

A ce niveau, la recommandation portera sur la condition 1 à savoir installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes. Spécifiquement, il

s'agira d'interdire l'accès public direct entre internet et tout composant du système dans l'environnement des données des titulaires de cartes.

En ce qui concerne la condition 2 relative aux mots de passe, il sera question de modifier les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur. En particulier, modifier les clés de cryptage à l'installation, modifier les chaines de communauté SNMP par défaut sur les périphériques. Par ailleurs, crypter tous les accès administratifs non-console à l'aide d'une cryptographie robuste. Utiliser des technologies pour la gestion sur le Web et autres accès.

- **surveillance de tests réguliers des réseaux**

Les recommandations formulées ici sont :

- synchroniser tous les systèmes d'horloge et temporels critiques ;
- s'assurer que les éléments suivants sont mis en œuvre pour l'acquisition, la distribution et l'enregistrement du temps, il s'agit de : la technologie de synchronisation temporelle, l'examen des processus d'acquisition, de distribution, d'enregistrement, les serveurs temporels ;
- examiner les configurations du système et des paramètres de synchronisation temporelle ;
- restreindre au seul personnel l'accès des données temporelles justifié par un besoin professionnel ;
- consigner tout changement aux paramètres temporels sur des systèmes critiques ;
- prévenir toute tentative malveillante de changer l'horloge ;
- empêcher toute utilisation non autorisée des serveurs d'horloge interne ;
- protéger les vérifications à rebours pour empêcher leur modification ;
- sauvegarder rapidement sur un serveur centralisé réservé à la journalisation les fichiers de vérification à rebours ;
- tester la présence de point d'accès sans fil ;
- détecter les points d'accès sans fil non autorisés tous les trimestres ;
- prévoir un plan de réponse aux incidents de l'entreprise en cas de détection de périphériques sans fil non autorisés ;
- analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par mois après tout changement significatifs des réseaux ;

- effectuer des tests de pénétration externe et internes au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications ;
- utiliser des systèmes de détection d'intrusion et/des systèmes de prévention d'intrusions pour contrôler l'intégrité du trafic ;
- déployer des logiciels de contrôle de l'intégrité des fichiers.

➢ **protection des données des titulaires de carte de crédit**

Il s'agira de :

- garder le stockage de données de titulaires de cartes à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données ;
- empêcher le stockage des données d'authentification sensibles après autorisation même cryptées ;
- masquer le PAN lorsqu'il s'affiche ;
- rendre le PAN illisible où qu'il soit stocké ;
- protéger les clés utilisées pour les données des titulaires de cartes de la divulgation et de l'utilisation illicites ;
- documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données des titulaires de cartes ;
- crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.

➢ **mise en œuvre de mesures de contrôle d'accès strictes**

L'essentiel des recommandations se résume ici à :

- suivre les processus et procédures de contrôle des changements pour toutes les modifications apportées à des composants du système ;
- développer des applications basées sur les directives de codage sécurisé ;
- prévenir les vulnérabilités de codage courantes dans les processus de développement de logiciel ;
- traiter les nouvelles menaces et vulnérabilités de manière régulière ;
- veiller à ce que les applications soient protégées contre les attaques connues.

- **gestion d'une politique de sécurité des informations**

Cette exigence étant presque parfaitement couverte par la banque, il s'agira simplement de rendre tous les mots de passe illisibles pendant la transmission et le stockage sur tous les composants du système à l'aide d'une méthode de cryptographie robuste telle que le hachage.

- **gestion d'un programme de vulnérabilités**

Aucune recommandation à faire ici, car le domaine de la norme assure une excellente couverture. Cependant, sensibiliser et former l'ensemble du personnel ainsi que les clients au tant que faire ce peut sur les mesures sécuritaires liés l'utilisation de la carte serait un atout. Par ailleurs, la SCBC gagnerait à installer sur place un service technique.

L'ensemble de ces recommandations est adressé au sein de la Banque au Département des Opérations et en particulier aux unités Information et technologie et Contrôle et Support.

Au terme de notre chapitre, il en résulte que la Banque comme toute structure présente aussi bien des forces et des faiblesses. Etant donné que le risque est inhérent à l'activité bancaire et qu'il n'y a point de risque zéro, la Banque doit mettre en œuvre des dispositifs de contrôle actuels pour garantir le minimum de sécurité. D'après notre évaluation, il en ressort que les dispositifs en cours répondent aux exigences de sécurité pour lesquelles ils ont été implémentés. Par ailleurs, dans l'optique de se conformer aux standards internationaux de l'heure, il serait aisé au regard de l'écart observé entre dispositif EMV de la SCBC et PCIDSS d'envisager mettre en avant PCI DSS.

CONCLUSION GENERALE

La modernisation des systèmes de payement a conduit les banques à émettre diverses cartes bancaires pour satisfaire à une demande de plus en plus accrue et répondre à un besoin précis des consommateurs et par là se démarquer de la concurrence. Malheureusement, l'effort de recherche de la qualité est entaché par l'émergence de nouveaux risques sur les cartes bancaires dans les pays développés simultanément. Ces menaces ont poussé les grands réseaux de fabricant de cartes à mettre en œuvre divers moyens et dispositifs de contrôle interne pour les contrer, c'est ainsi que le PCI DSS entre dans ce canevas.

L'efficacité de la norme EMV n'est plus à démontrer de nos jours. Dans le cadre de la bande magnétique, elle a considérablement réduit la fraude surtout avec l'introduction de la carte à puce EMV. Cependant, de nos jours, avec l'émergence de nouvelles technologies et les modifications de l'environnement, le système d'acception peut traiter des transactions en marge d'EMV. Dans ce cas, l'intégrité des données des titulaires de carte n'est plus garantie. Ainsi donc, une protection supplémentaire ou une nouvelle solution est requise.

Les douze conditions du PCI DSS de par leurs objectifs de garantir l'intégrité des composants du système et la protection de la confidentialité des données du titulaires de carte et d'identification quelque soit l'environnement, viennent pallier les insuffisances de EMV.

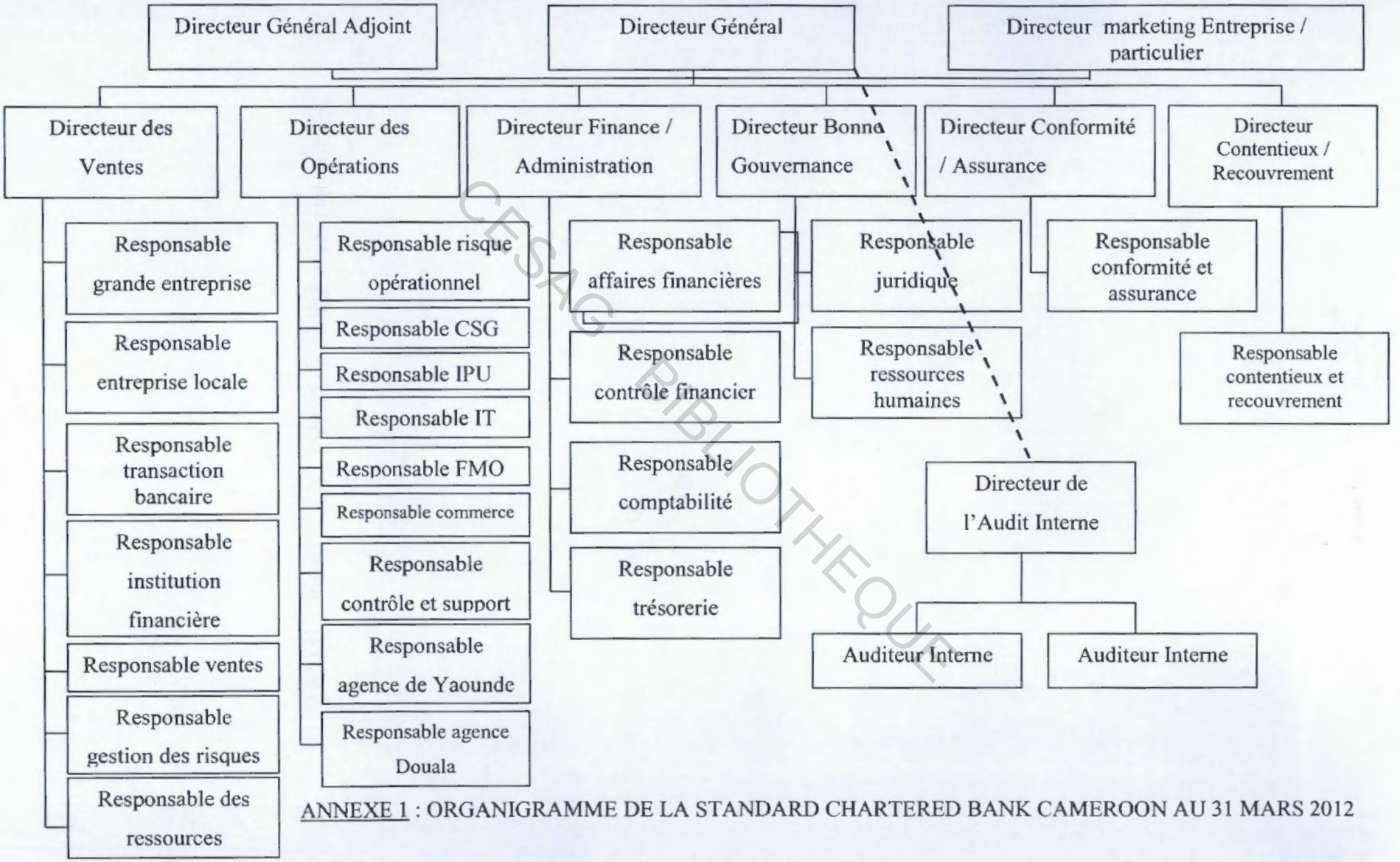
Le PCI DSS par son développement et son implémentation ne distingue pas les transactions à sécuriser, mais s'inscrit dans la globalité en cherchant à plutôt à protéger les données sensibles.

Au terme de notre étude, en guise de résumé, notre objectif principal face au problème de la recrudescence de la fraude sur les cartes bancaires, était de poser le diagnostic de la sécurité des cartes bancaires de la SCBC conformément au standard PCI DSS et par là même de l'améliorer. Pour ce faire, nous avons entrepris de :

- évaluer la sécurité sur les cartes bancaires ;
- identifier les forces et les faiblesses ;
- faire un test de conformité et permanence ;
- établir un programme de travail basé sur les faiblesses ;
- et enfin faire des recommandations.

Dans un contexte africain en général et en particulier au Cameroun, l'introduction de la carte bancaire dans le système de payement est dans sa phase de développement. S'il est vrai que la carte bancaire est en plein essor dans les grandes villes africaines, il n'en demeure pas moins qu'elle est mal connue dans les milieux ruraux. Ce retard peut se justifier entre autres par le degré de croissance de ces zones peu attractives pour les investisseurs, le niveau de formation très bas de la population ainsi que l'absence de sensibilisation à l'utilisation de ce moyen de payement. Plusieurs causes peuvent être énumérées ici, mais la préoccupation de l'heure serait de chercher à rattraper ce retard en se servant d'expériences antérieures externes. L'expansion de la carte bancaire en Afrique, tout comme en Occident nécessite la prise en compte des risques et menaces que rencontrent les pays développés aujourd'hui. C'est également dans une logique de prévention que se situe ce travail. Nous espérons donc que ce mémoire a atteint les objectifs visés et contribuera à améliorer la sécurité non seulement de la SCBC mais également d'autres structures au niveau national et international.

ANNEXES



ANNEXE 1 : ORGANIGRAMME DE LA STANDARD CHARTERED BANK CAMEROON AU 31 MARS 2012

ANNEXE 2 : DESCRIPTION D'UNE CARTE BANCAIRE

Source : Google image (2012)

ANNEXE 3 : PRESENTATION DES CARTES BANCAIRES D'OMAC ET GIM EUMOA

OMAC

CB OMAC

DESCRIPTION

La carte CB OMAC régionale se présente comme une carte ayant les dernières technologies : masque CB, technologie puce DDA, possibilité de mettre plusieurs applications (AID) sur la puce.

AVANTAGES

Plus sûre que l'argent liquide, plus pratique que le chèque, la carte CB OMAC régionale vous permet de retirer de l'argent dans tous les distributeurs automatiques de billets et dans toutes les banques de la zone CEMAC.

Source : Site de l'OMAC (2012)

CARTE OMAC VISA

DESCRIPTION

Protégée par un code confidentiel à plusieurs chiffes, la carte OMAC VISA est une carte à puce garantissant au client une sécurité optimale par signature électronique.

AVANTAGES

La Carte OMAC VISA vous permet de régler vos achats (billets d'avoir, différents factures, magazins,..) et d'effectuer vos opérations bancaires dans la zone CEMAC et partout dans le monde, grâce au premier réseau mondial, le réseau VISA.

Source : Site de l'OMAC (2012)

GIM UEMOA

CARTE BANCAIRE GIM UEMOA

CARACTERISTIQUES

- Norme ISO 7810 : Caractéristiques physiques (1ère partie)
- Norme ISO 7816-1 : Caractéristiques physiques (2ème partie)
- Norme ISO 7816-2 : Caractéristiques électriques
- Longueur : 85,6 mm +/- 0,12 , Epaisseur : 0,75 mm +/- 0,028
- Hauteur : 53,98 mm +/- 0,05
- Le GIM-UEMOA s'oriente naturellement vers la carte à puce.

Source : Site du GIM UEMOA (2012)

ANNEXE 4 : QUESTIONNAIRE DE PRISE DE CONNAISSANCE DE LA BANQUE

1. Quel est votre statut actuel au sein de la Banque :.....

Historique et évolution

2. Pouvez-vous nous donner la dénomination de l'entité :

.....

3. Quel en est le sigle : .....

4. Date de création : .....

5. Vous appartenez à un groupe d'origine :

☐ Américaine ☐ Anglaise ☐ Française ☐ Africaine

☐ Mixte

6. Lequel ?.....

7. Forme juridique de l'entité :

☐ SA ☐ SARL ☐ SNC ☐ SCS

8. Vos actionnaires sont-ils des :

☐ Etrangers ☐ Nationaux ☐ Mixte

9. Le capital social à la création était de :

☐ 500.000.000 ☐ Entre 500.000.000 et 1.000.000.000 ☐ >1.000.000.000

10. De nos jours, ce capital s'élève à :

☐ < 1.000.000.000 ☐ Entre 1.000.000.000 et 5.000.000.000

☐ Entre 5.000.000.000 et 10.000.000.000 ☐ < 10.000.000.000

11. Quels sont vos principaux actionnaires et leurs parts respectives de capital ?.....

.....

12. Au cours de ces dix (10) dernières années, le bilan de votre présence au Cameroun peut être jugé ?

☐ Médiocre ☐ Passable ☐ Peut mieux faire ☐ Satisfaisant

☐ Très satisfaisant ☐ Autres

Autres à préciser.....

Structure et fonctionnement

13. L'organe qui définit la politique générale de la Banque c'est :

☐ Le Conseil d'Administration ☐ l'Assemblée Générale

☐ Le Comité d'audit ☐ La Direction Générale

☐ Autre

14. Son mandat est compris entre :

☐ 1 – 3 ans ☐ 3 – 5 ans ☐ 5 – 7 ans ☐ Autres

Autres à préciser.....

15. De combien de membres dispose-t-il ?

☐ 3 à 5 ☐ 5 à 8 ☐ 8 à 12 ☐ Autres

Autres à préciser.....

16. D'après l'organigramme, on peut dire que la structure de la banque est :

☐ Centralisée ☐ Décentralisée ☐ Mixte

17. Disposer-vous d'une entité responsable du volet monétique au sein de la Banque ?

☐ Oui ☐ Non

18. Cette entité est-elle érigée en :

☐ Direction ☐ Service ☐ Département ☐ Autres

Autres à préciser .....

19. Quelle est la date de création de cette entité monétique ?

☐ < 5 ans ☐ entre 5 et 10 ans ☐ >10ans

☐ A la création de la Banque

Activités et réseau d'agences

20. Emettez-vous des cartes bancaires pour le compte de vos clients ?

☐ Oui ☐ Non

21. Quels types de cartes bancaires offrez-vous à vos clients ?

☐ Carte de garantie de chèques ☐ Cartes bancaires de retrait de billets

☐ Cartes à débit immédiat ☐ Cartes à débit différé

☐ Cartes de crédit ☐ Cartes à usage restreint

☐ Cartes accréditives ☐ Cartes privatives

☐ Cartes orientées entreprise

22. D'après les spécifications techniques la Banque utilise :

☐ Les cartes à puce ☐ les cartes à bande magnétique ☐ Autres

Autres à préciser.....

23. En quelle année avez-vous mis à la disposition de vos clients les premières cartes bancaires ?

☐ 1986 ☐ 1987 ☐ 1988 ☐ 1989 ☐ 1990 ☐ 1991
☐ 2000 ☐ 2001 ☐ 2002 ☐ 2003 ☐ 2004 ☐ 2005

☐ 2006 ☐ 2007 ☐ 2008 ☐ 2009 ☐ 2010 2☐

Autres à préciser.....

24. Combien de cartes bancaires aviez-vous en circulation à la première émission ?

☐ <1 000 ☐ Entre 1 000 et 5 000 ☐ Entre 5 000 et 10 000

☐ Entre 10 000 et 15 000 ☐ Entre 15 000 et 20 000 ☐ Entre 20 000 et 25 000

☐ >25 000 ☐ Autres

Autres à préciser.....

25. Combien de cartes bancaires aviez-vous en circulation à la fin de l'année 2011 ?

☐ <10 000 ☐ Entre 10 000 et 15 000 ☐ Entre 15 000 et 20 000

☐ Entre 20 000 et 25 000 ☐ Entre 25 000 et 30 000 ☐ Entre 30 000 et 35 000

☐ Entre 35 000 et 40 000 ☐ Entre 40 000 et 45 000 ☐ Entre 45 000 et 50 000

☐ > 50 000 ☐ Autres

Autres à préciser.....

26. Combien de cartes bancaires avez-vous en circulation cette année ?

☐ <10 000 ☐ Entre 10 000 et 15 000 ☐ Entre 15 000 et 20 000
☐ Entre 20 000 et 25 000 ☐ Entre 25 000 et 30 000 ☐ Entre 30 000 et 35 000

☐ Entre 35 000 et 40 000 ☐ Entre 40 000 et 45 000 ☐ Entre 45 000 et 50 000

☐ >25 000 ☐ Autres

Autres à préciser .....

27. Dans combien de régions la Banque est-elle présente au Cameroun ?

☐1 ☐2 ☐3 ☐4 ☐ ☐ ☐ 8☐ 9☐ 10☐

28. Comment qualifiez-vous la fréquence de survenance des incidents sur les cartes bancaires au sein de la banque ou dans les agences ?

☐ Jamais ☐ Rarement ☐ Souvent ☐ Fréquemment
☐ Autres

Autres à préciser.....

29. Comment qualifiez-vous la fréquence de survenance des fraudes sur les cartes bancaires au sein de la banque ou dans les agences ?

☐ Jamais ☐ Rarement ☐ Souvent ☐ Fréquemment

☐ Autres

Autres à préciser.....

30. Quels sont les risques liés aux cartes que vous connaissez ?

31. Quels sont les risques liées au porteur de la carte que vous connaissez ?

32. Quels sont les risques liés aux banques que vous connaissez ?

33. Quels sont les risques liés aux marchands que vous connaissez ?

34. En matière de sécurité sur les cartes bancaires, utilisez-vous l'une des normes suivantes ?

☐ La norme EMV (Europay Mastercard et Visa) ☐ La norme PCI DSS

☐ Les normes de la famille ISO 27 000 ☐ Autres

Autres à préciser.....

35. De combien d'agences disposez-vous sur l'ensemble du territoire ?

☐ 5 -15 ☐ 16 – 25 ☐ >25 ☐ Autres

Autres à préciser.....

36. Quelles sont vos activités principales ?

☐ Collecte des fonds uniquement ☐ Distribution du crédit uniquement

☐ Les deux à la fois ☐ Autres

Autres à préciser.....

37. Comment appréciez-vous la contribution des revenus issus des cartes bancaires à la rentabilité de la Banque ?

☐ Faible ☐ Insuffisante ☐ Moyenne ☐ Supérieure à la moyenne

☐ Forte ☐ Elevée ☐ Excellente ☐ Autres

Autres à préciser.....

La dynamique concurrentielle

38. Quels sont vos 5 principaux concurrents actuels en termes de cartes bancaires émises ?

☐ AFRILAND FIRST BANK ☐ ECOBANK CAMEROON

☐ CREDIT FONCIER DU CAMEROUN ☐ UNITED BANK FOR AFRICA

☐ UNION BANK OF CAMEROON ☐ SGBC

☐ SCB CREDIT LYONNAIS BICEC

Autres.....

39. Quelle position la Banque occupe-t-elle en termes de cartes bancaires émises et en circulation ?

1ière ☐ 2e ☐ 3e ☐ 4e ☐ 5e ☐ 6è ☐

7ière ☐ 8e ☐ 9e ☐ 10e ☐ 11e ☐ 12è ☐

13ière ☐ 14e ☐ 15e ☐ 16e ☐ 17e ☐ 18è ☐

Autres.....

40. Quelle position la Banque occupe-t-elle en termes de GAB ou DAB et de couverture du territoire?

1ière ☐ 2e ☐ 3e ☐ 4e ☐ 5e ☐ 6è ☐

7ière ☐ 8e ☐ 9e ☐ 10e ☐ 11e ☐ 12è ☐

13ière ☐ 14e ☐ 15e ☐ 16e ☐ 17e ☐ 18è ☐

Autres.....

MERCI DE VOTRE AIMABLE PARTICIPATION

ANNEXE 5 : QUESTIONNAIRE D'EVALUATION PCI DSS

CREATION ET GESTION D'UN RESEAU SECURISE

1) Installation et gestion d'une configuration de pare-feu pour protéger les données des titulaires de cartes

1.1	Définition des normes de configuration des pare-feu et des routeurs	Oui	Non
A	Existe-t-il 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 ?		
B	Existe-t-il un schéma de réseau actuel indiquant toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil ?		
C	Existe-t-il un schéma de réseau actuel indiquant toutes les connexions aux données des titulaires de cartes, notamment tous les réseaux sans fil régulièrement mis à jour ?		
D	les normes de configuration des pare-feu comprennent-elles l'exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée et la zone de réseau Internet ?		
E	le schéma de réseau actuel est-il conforme aux normes de configuration des pare-feu ?		
F	les normes de configuration des pare-feu et des routeurs comprennent-elles la description des groupes, des rôles et des responsabilités pour la gestion logique des composants réseau ?		
G	les normes de configuration des pare-feu et des routeurs comprennent-ils la liste documentée des services, protocoles et ports nécessaires à la conduite des activités de l'entreprise ?		
H	Existent-ils des services, des protocoles et des ports non sécurisés autorisés ?		
I	Les services, les protocoles et les ports non sécurisés autorisés sont-ils nécessaires ?		
J	Les fonctions de sécurité sont-elles documentées et mises en œuvre en		

	examinant les normes de configuration des pare-feu et des routeurs ainsi que les paramètres de chaque service ?		
K	les normes de configuration des pare-feu et des routeurs exigent-elles l'examen des règles des pare-feu et des routeurs au moins tous les six mois ?		
L	Peut-on obtenir et examiner la documentation pour vérifier que les règles sont passées en revue au moins tous les six mois ?		
M	Créer une configuration de pare-feu qui limite les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données des titulaires de cartes		

1.2	**Création d'une configuration de pare-feu limitant les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données des titulaires de cartes**	**Oui**	**Non**
A	Le trafic entrant et sortant est-il limité au trafic nécessaire à l'environnement des données des titulaires de cartes ?		
B	Les restrictions sont-elles documentées ?		
C	Tous les autres trafics entrants et sortants sont-ils explicitement refusés ?		
D	Les fichiers de configuration des routeurs sont-ils sécurisés et synchronisés ?		
E	Des pare-feu de périmètre sont-ils installés entre tous les réseaux sans fil et les systèmes stockant les données des titulaires de cartes ?		
F	Des pare-feu refusent t'ils ou contrôlent t'ils le trafic (si celui-ci est nécessaire à des fins professionnelles) de l'environnement sans fil vers l'environnement des données des titulaires de cartes ?		

1.3	**Interdiction d'accès public direct entre Internet et tout composant du système dans l'environnement des données des titulaires de cartes.**	**Oui**	**Non**
A	Une zone démilitarisée est-elle déployée pour limiter le trafic entrant aux seuls composants du système fournissant des services, protocoles et ports autorisés, accessibles au public ?		
B	Le trafic Internet entrant est-il limité aux adresses IP dans la zone démilitarisée ?		
C	connexion directe entrante ou sortante est-elle autorisée pour le trafic entre Internet et l'environnement des données des titulaires de cartes ?		
D	Les adresses internes peuvent-elles passer d'Internet dans la zone démilitarisée ?		
E	Le trafic sortant de l'environnement des données des titulaires de cartes vers Internet est-il expressément autorisé ?		
F	Le pare-feu effectue-t-il un contrôle avec état ?		
G	Les composants du système qui stockent les données de titulaires de cartes se trouvent-ils dans une zone de réseau interne isolée de la zone démilitarisée et des autres réseaux non approuvés ?		
H	Existe-t-il des moyens en place pour prévenir la divulgation d'adresses IP et d'informations d'acheminement confidentielles des réseaux internes sur Internet ?		
I	Un logiciel pare-feu personnel est-il installé et activé sur les ordinateurs portables et/ou les ordinateurs appartenant aux employés équipés d'une connexion directe à Internet (par exemple, ordinateurs portables utilisés par les employés), qui sont utilisés pour accéder au réseau de l'entreprise ?		
J	Le logiciel pare-feu personnel est-il configuré par l'entreprise selon des normes spécifiques ?		
K	La configuration du logiciel pare-feu peut-il être modifiée par les utilisateurs d'ordinateurs portables ?		

2) Mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

2.1	**Les mots de passe, les chaînes de communauté SNMP et les clés de cryptage sans fil par défaut**	**Oui**	**Non**
A	Les clés de cryptage par défaut ont-elles été modifiées à l'installation ?		
B	Les clés de cryptage sont-elles changées à chaque fois qu'un employé qui les connaît quitte l'entreprise ou change de poste ?		
C	Les chaînes de communauté SNMP par défaut sur les périphériques sans fil ont-elles été modifiées ?		
D	Les mots de passe/locutions de passage par défaut des points d'accès ont-ils été modifiés ?		
E	Le firmware des périphériques sans fil est-il mis à jour de manière à prendre en charge un cryptage robuste pour l'authentification et la transmission sur les réseaux sans fil ?		
F	Les autres paramètres par défaut liés à la sécurité, définis par le fournisseur des équipements sans fil, ont-ils été changés, le cas échéant.		

2.2	**Élaborer des normes de configuration pour tous les composants du système. S'assurer que ces normes couvrent toutes les vulnérabilités de la sécurité et sont compatibles avec toutes les normes renforçant les systèmes en vigueur dans le secteur.**	**Oui**	**Non**
A	Les normes de configuration du système de l'organisation pour tous les types de composants du système sont-elles examinées ?		
B	Ces normes sont-elles compatibles avec les normes de renforcement en vigueur dans le secteur ?		
C	Les normes de configuration du système sont-elles mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités ?		
D	Les normes de configuration du système sont-elles appliquées lorsque de nouveaux systèmes sont configurés ?		
E	Sur un échantillon de composants du système, une seule fonction principale par serveur est-elle implémentée ?		
F	Si des technologies de virtualisation sont utilisées, seule une fonction		

	principale est-elle déployée par composant de système ou dispositif virtuels ?		
G	Sur un échantillon de composants du système, les démons, les protocoles et les services activés du système sont-ils examinés ?		
H	Seuls les services ou protocoles nécessaires sont-ils activés ?		
I	Tous services, démons ou protocoles activés et non sécurisés sont-ils identifiés ?		
J	Leur utilisation est-elle justifiée ?		
K	Des fonctions de sécurité sont-elles documentées et déployées ?		
L	Les administrateurs système et/ou les responsables de la sécurité connaissent-ils les paramètres de sécurité courants des composants du système ?		
M	Les paramètres de sécurité courants sont-ils inclus dans les normes de configuration du système ?		
N	Sur un échantillon de composants du système, les paramètres de sécurité courants sont-ils correctement définis ?		
O	Sur un échantillon de composants du système, toutes les fonctionnalités qui ne sont pas nécessaires (scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers, etc.) sont-elles supprimées ?		
P	Les fonctions activées sont-elles documentées ?		
Q	et prennent-elles en charge une configuration sécurisée ?		
R	La fonctionnalité documentée est-elle présente sur les composants de système échantillonnés ?		

2.3	**Crypter tous les accès administratifs non-console, à l'aide d'une cryptographie robuste. Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion sur le Web et autres accès administratifs non-console.**	**Oui**	**Non**
A	Une méthode de cryptage robuste est-elle appelée avant que l'administrateur ne soit invité à taper son mot de passe ?		
B	En passant en revue les services et les fichiers de paramètres sur les		

	systèmes peut-on déterminer que Telnet et d'autres commandes de connexion à distance ne sont pas disponibles pour un usage interne ?		
C	L'accès administrateur aux interfaces de gestion Web est-il crypté au moyen d'une méthode de cryptage robuste ?		

PROTECTION DES DONNEES DES TITULAIRES DE CARTE DE CREDIT

1) protéger les données de titulaire de carte stockées

3.1	**Garder le stockage de données de titulaires de cartes à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données**	**Oui**	**Non**
A	Les politiques et les procédures comprennent-elles des dispositions légales, réglementaires et professionnelles sur la conservation des données, notamment des conditions spécifiques sur la conservation des données des titulaires de cartes ?		
B	Les politiques et les procédures comprennent-elles des dispositions sur l'élimination des données qui ne sont plus requises à des fins légales, réglementaires ou professionnelles, notamment la suppression des données des titulaires de cartes ?		
C	Les politiques et procédures couvrent-elles l'ensemble du stockage de données de titulaires de cartes ?		
D	Toutes les politiques et procédures Comprennent-elles au moins un des éléments suivants :		
	Un processus programmé (automatique ou manuel) pour supprimer, au moins une fois par trimestre, les données de titulaires de cartes stockées, excédant les conditions définies dans la politique de conservation des données.		
	L'obligation d'une vérification, au moins trimestrielle, afin de contrôler que les données de titulaires de cartes stockées n'excèdent pas les conditions définies dans la politique de conservation des données.		
E	Sur un échantillon de composants de système stockant des données de titulaires de cartes, les données stockées excèdent-elles les conditions définies dans la politique de conservation des données ?		

3.2	**Ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée)**	**Oui**	**Non**
A	Dans le cas des émetteurs et des sociétés qui prennent en charge les services d'émission et stockent des données d'authentification sensibles, ce stockage est-il justifié du point de vue professionnel ?		
B	Ces données sont-elles protégées ?		
C	Pour toutes les autres entités, si des données d'authentification sensibles sont reçues et supprimées, peut-on obtenir et passer en revue les processus de suppression des données pour vérifier que ces dernières sont irrécupérables ?		
D	Sur un échantillon de composants du système, peut-on examiner les sources de données, y compris sans s'y limiter les éléments suivants :		
	les données de transaction entrantes		
	tous les journaux (par exemple, transactions, historique, débogage, erreur)		
	les fichiers d'historique		
	les fichiers trace		
	plusieurs schémas de bases de données		
	le contenu des bases de données		
E	La totalité du contenu d'une quelconque piste de la bande magnétique au verso d'une carte ou sur une puce, est-elle stockée ?		
F	Sur un échantillon de composants du système, peut-on examiner les sources de données, y compris sans s'y limiter les éléments suivants :		
	les données de transaction entrantes ;		
	tous les journaux (par exemple, transactions, historique, débogage, erreur) ;		
	les fichiers d'historique ;		
	les fichiers trace ;		
	plusieurs schémas de bases de données ;		
G	le code ou la valeur de vérification de carte à trois ou quatre chiffres figurant au recto de la carte de paiement, ou dans l'espace réservé à la		

	signature, (données CVV2, CVC2, CID, CAV2) est-il stocké ?		
H	Sur un échantillon de composants du système, peut-on examiner les sources de données, y compris sans s'y limiter les éléments suivants :		
	les données de transaction entrantes ;		
	tous les journaux (par exemple, transactions, historique, débogage, erreur) ;		
	les fichiers d'historique ;		
	les fichiers trace ;		
	plusieurs schémas de bases de données ;		
	le contenu des bases de données.		
I	les codes et blocs PIN cryptés sont-ils stockés ?		

3.3	**Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés).**	**Oui**	**Non**
A	Peut-on obtenir et examiner les politiques écrites ?		
B	Peut-on passer en revue l'affichage des PAN (par exemple, à l'écran, sur les reçus papier) afin de vérifier que les numéros de comptes principaux (PAN) sont masqués lors de l'affichage des données des titulaires de cartes ?		
C	Les utilisateurs qui ont un besoin professionnel légitime de voir l'intégralité du PAN le peuvent-ils ?		
D	Peut-on obtenir et passer en revue la documentation relative au système utilisé pour protéger le PAN ? (le fournisseur, le type de système/processus et les algorithmes de cryptage)		
E	le PAN est-il rendu illisible à l'aide de l'une des méthodes suivantes :		
	hachage unilatéral s'appuyant sur une méthode cryptographique robuste		
	une troncature		
	tokens et pads d'index, les pads devant être stockés de manière sécurisée		
	cryptographie robuste associée à des processus et des procédures de gestion des clés.		

3.4	**Rendre le PAN illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux)**	**Oui**	**Non**
A	Peut-on obtenir et passer en revue la documentation relative au système utilisé pour protéger le PAN ? (le fournisseur, le type de système/processus et les algorithmes de cryptage)		
B	Vérifier que le PAN est rendu illisible à l'aide de l'une des méthodes suivantes :		
	hachage unilatéral s'appuyant sur une méthode cryptographique robuste		
	une troncature		
	tokens et pads d'index, les pads devant être stockés de manière sécurisée		
	cryptographie robuste associée à des processus et des procédures de gestion des clés		
C	Peut-on examiner plusieurs tables ou fichiers d'un échantillon de référentiels de données afin de vérifier que le PAN est rendu illisible ?		
D	Peut6on examiner un échantillon de support amovible (par exemple bandes de sauvegarde) pour s'assurer que le PAN est rendu illisible ?		
E	Peut-on examiner un échantillon des journaux d'audit pour confirmer que le PAN est bien illisible ou supprimé des journaux ?		
F	un cryptage par disque est-il utilisé ?		
	L'accès logique aux systèmes de fichiers cryptés est-il implémenté par le biais d'un mécanisme indépendant des mécanismes des systèmes d'exploitation natifs (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales) ?		
G	Les clés cryptographiques sont-elles stockées de manière sécurisée (par exemple, sur des supports amovibles correctement protégés avec des contrôles d'accès stricts) ?		
H	Vérifier que les données des titulaires de cartes sur les supports amovibles sont cryptées où qu'elles soient stockées ?		

3.5	**Protéger les clés utilisées pour protéger les données de titulaires de cartes de la divulgation et de l'utilisation illicites**	**Oui**	**Non**
A	Peut-on passer en revue les listes d'accès utilisateur afin de vérifier que l'accès aux clés est restreint aux opérateurs strictement nécessaires ?		
B	Peut-on passer en revue les fichiers de configuration des systèmes pour vérifier que les clés sont stockées dans un format crypté et que les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données ?		
C	Peut-on Identifier les emplacements de stockage des clés pour vérifier que celles-ci sont stockées dans aussi peu d'endroits et sous aussi peu de formes que possible ?		

3.6	**Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données des titulaires de cartes**	**Oui**	**Non**
A	Peut-on vérifier l'existence de procédures de gestion des clés pour les clés de cryptage des données de titulaires de cartes ?		
B	Pour les prestataires de services seulement : si le prestataire de services partage des clés avec ses clients pour la transmission de données de titulaires de cartes. Il leur fournit-il la documentation nécessaire avec les instructions sur la manière de sécuriser la transmission, le stockage et la mise à jour des clés ?		
C	Peut-on passer en revue les procédures de gestion des clés et procéder comme suit :		
	des procédures de gestion des clés sont mises en œuvre pour la production de clés robustes		
	des procédures de gestion des clés sont mises en œuvre pour une distribution de clés sécurisée.		
	des procédures de gestion des clés sont mises en œuvre pour le stockage de clés sécurisé.		
	des procédures de gestion de clés sont mises en œuvre pour appliquer		

	les changements de clés périodiques à la fin de la crypto période définie.		
	des procédures de gestion des clés sont mises en œuvre pour supprimer les clés lorsque leur intégrité a été affaiblie.		
	des procédures de gestion des clés sont mises en œuvre pour requérir le remplacement des clés soupçonnées d'avoir été compromises, ou si ce fait est avéré.		
	Si des clés cryptographiques retirées ou remplacées sont conservées, vérifier qu'elles ne sont pas utilisées pour des opérations de cryptage.		
	des procédures de gestion manuelle de clés en texte clair exigent un fractionnement des connaissances et un double contrôle.		
	des procédures de gestion des clés sont mises en œuvre pour empêcher la substitution non autorisée des clés		
	des procédures de gestion des clés sont mises en œuvre pour exiger des opérateurs chargés de la gestion de clés cryptographiques qu'ils reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités.		

2) crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts

4.1	**Utiliser des protocoles de sécurité et de cryptographie robustes (par exemple, SSL/TLS, IPSEC, SSH, etc.) afin de protéger les données sensibles des titulaires de cartes durant la transmission sur des réseaux publics ouverts.**	**Oui**	**Non**
A	L'utilisation de protocoles sécurisés chaque fois que les données des titulaires de cartes sont transmises ou reçues sur des réseaux publics ouverts. Un cryptage robuste est-il utilisé pendant la transmission des données, comme suit :		
	à la réception de transactions, choisir un échantillon et examiner les transactions pendant qu'elles s'exécutent afin de vérifier que les données des titulaires de cartes sont cryptées pendant le transfert.		
	seuls des clés/certificats approuvés sont acceptés.		
	le protocole est déployé de manière à n'utiliser que des configurations		

	sécurisées et qu'il ne prend en charge aucune version ni configuration non sécurisées		
	le niveau de cryptage approprié est mis en œuvre pour la méthodologie de cryptage employée (Vérifier les recommandations/meilleures pratiques du fournisseur).		
B	Pour les implémentations SSL/TLS, la mention HTTPS apparaît-elle dans l'adresse URL (Universal Record Locator) dans le navigateur ?		
	une donnée de titulaires de cartes est-elle requise lorsque la mention HTTPS n'apparaît pas dans l'URL ?		
C	Pour les réseaux sans fil sur lesquels sont transmises les données des titulaires de cartes ou qui sont connectés à l'environnement des données des titulaires de cartes. Les meilleures pratiques du secteur sont-elles mises en œuvre pour appliquer un cryptage robuste pour l'authentification et la transmission ?		
D	Le PAN est-il rendu illisible ou protégé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie pour les utilisateurs finaux ?		
E	Existe-t-il une politique interdisant la transmission de PAN non protégés à l'aide de technologies de messagerie pour les utilisateurs finaux ?		

GESTION D'UN PROGRAMME DE GESTION DES VULNERABILITES

1) utiliser des logiciels antivirus et les mettre à jour régulièrement

5.1	**Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).**	**Oui**	**Non**
A	Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants. Des logiciels antivirus sont-ils déployés et, le cas échéant, qu'une technologie de protection antivirus est en place ?		
B	Sur un échantillon de composants du système. Tous les programmes antivirus détectent-ils et éliminent-ils tous les types de logiciels malveillants connus ?		

	et constituent-ils une protection efficace contre ces fléaux ?		

5.2	**Vérifier que tous les logiciels antivirus sont à jour, en cours d'exécution et génèrent des journaux**	**Oui**	**Non**
A	Peut-on obtenir et passer en revue la politique, et vérifier qu'elle stipule la mise à jour des logiciels antivirus et des définitions de virus ?		
B	l'installation principale du logiciel est-elle configurée pour la mise à jour automatique et l'exécution d'analyses à intervalles réguliers ?		
C	Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants. Les mises à jour automatiques et les analyses à intervalles réguliers sont-elles activées ?		
D	Sur un échantillon de composants du système. La génération des journaux des logiciels antivirus est-elle activée ?		
	ceux-ci sont-ils conservés ?		

2) développer et gérer des systèmes et des applications sécurisés

6.1	**S'assurer que tous les logiciels et les composants du système sont dotés des derniers correctifs de sécurité développés par le fournisseur, afin de les protéger des vulnérabilités connues. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.**	**Oui**	**Non**
A	Sur un échantillon de composants du système et de logiciels associés, compare-t-on la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur ?		
	les correctifs les plus récents disponibles sont-ils installés.		
B	Passe-t-on en revue les politiques relatives à l'installation des correctifs de sécurité afin de s'assurer qu'elles stipulent l'installation de tous les nouveaux correctifs de sécurité stratégiques dans un délai d'un mois ?		

6.2	**Établir un processus pour identifier et assigner une catégorie de risque aux nouvelles vulnérabilités de sécurité découvertes.**	**Oui**	**Non**
A	les processus d'identification des nouvelles vulnérabilités de la sécurité sont-ils mis en œuvre ?		
B	ces dernières (vulnérabilités) reçoivent-elles un classement de risque ?		
C	les processus pour identifier les nouvelles vulnérabilités de sécurité comprennent-ils l'utilisation de sources externes d'information sur la vulnérabilité de sécurité ?		

6.3	**Développer des applications logicielles (internes et externes, y compris l'accès administratif aux applications par le Web). Intégrer la sécurité des informations à tout le cycle de vie du développement de logiciel**	**Oui**	**Non**
A	Peut-on se procurer les processus écrits de développement de logiciel ?		
	les examine-t-on pour vérifier que les processus respectent les normes du secteur et/ou les meilleures pratiques ?		
B	Examine-t-on les processus écrits de développement de logiciel pour vérifier que la sécurité des informations est intégrée à tout le cycle de vie ?		
C	Examine-t-on les processus écrits de développement de logiciel pour vérifier que les applications logicielles sont développées conformément à la norme PCI DSS ?		
D	En examinant les processus écrits de développement de logiciel et les entretiens des développeurs de logiciels, peut-on vérifier que : les comptes d'application personnalisés, les noms d'utilisateur et les mots de passe sont supprimés avant la mise en production du système ou sa mise à la disposition des clients ?		
E	Peut-on obtenir et passer en revue les politiques afin de vérifier que toutes les modifications apportées au code personnalisé d'application sont examinées (manuellement ou automatiquement), comme suit :		
	Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et		

	maîtriser les pratiques de codage sécurisées.		
	Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé (voir la condition 6.5 de la norme PCI DSS).		
	Les corrections appropriées sont implémentées avant la publication.		
	Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant la publication.		
F	Peut-on sélectionner un échantillon de modifications apportées récemment à une application personnalisée et vérifier que le code correspondant est examiné conformément aux instructions décrites au point ci-dessus.		

6.4	**Suivre les processus et procédures de contrôle des changements pour toutes les modifications apportées à des composants du système.**	**Oui**	**Non**
A	Les environnements de test/développement sont-ils distincts de l'environnement de production ?		
	Existe-t-il un contrôle d'accès pour garantir la séparation ?		
B	Existe-t-il une séparation entre les missions des collaborateurs affectés aux environnements de développement/test et celles des personnels affectés à l'environnement de production ?		
C	Les données de production (PAN actifs) ne sont-elles pas utilisées à des fins de test ou de développement ?		
D	Les données de test et les comptes sont-ils supprimés avant que le système de production ne devienne actif ?		
E	Les procédures de contrôle des modifications liées à la mise en œuvre des correctifs de sécurité et des modifications logicielles sont-elles documentées ?		
F	La documentation de l'impact est-elle comprise dans la documentation de contrôle des changements, et ce pour chaque changement inclus dans l'échantillon ?		
G	Une approbation documentée par les responsables existe-t-elle pour		

	chaque modification échantillonnée ?		
H	Pour chaque changement échantillonné, le test de fonctionnalité a-t-il été exécuté pour vérifier que le changement ne compromet pas la sécurité du système ?		
I	Pour les modifications de code personnalisé, toutes les mises à jour avant leur mise en production sont-elles conformes à la condition 6.5 de la norme PCI DSS ?		
J	Des procédures de suppression sont-elles préparées pour chaque changement inclus dans l'échantillon ?		

6.5	**Développer des applications basées sur les directives de codage sécurisé. Prévenir les vulnérabilités de codage courantes dans les processus de développement de logiciel**	**Oui**	**Non**
A	Peut-on se procurer et examiner les processus de développement de logiciel ?		
	le processus exige-t-il la formation aux techniques de codage sécurisé pour les développeurs, selon les directives et les meilleures pratiques du secteur ?		
B	Interroge-t-on un panel de développeurs afin d'obtenir la preuve qu'ils disposent des connaissances nécessaires en techniques de codage sécurisé ?		
C	Existe-t-il un processus garantissant, au minimum, la non-vulnérabilité des applications aux éléments suivants :		
	Attaques par injection, notamment les injections de commandes SQL (valider l'entrée pour vérifier que les données utilisateur ne peuvent pas modifier le sens des commandes et des requêtes, utiliser des requêtes paramétrées, etc.).		
	Saturation de la mémoire tampon (valider les limites de la mémoire tampon et tronquer les chaînes d'entrée).		
	Stockage cryptographique non sécurisé (prévient les défauts cryptographiques).		
	Communications non sécurisées (crypter correctement toutes les		

	communications authentifiées et sensibles).		
	Traitement inapproprié des erreurs (ne pas laisser échapper d'informations par les messages d'erreurs)		
	Toutes les vulnérabilités de niveau « élevé », identifiées par la condition 6.2 de la norme PCI DSS.		
	Attaques par script intersite (XSS) (valider tous les paramètres avant l'inclusion, utiliser un mécanisme d'échappement sensible au contexte, etc.).		
	Contrôle d'accès inapproprié comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, et survol de répertoire (authentifier correctement les utilisateurs et nettoyer les entrées. Ne soumettre en aucun cas les références à des objets internes aux utilisateurs).		
	Attaques CSRF (Cross-site request forgery) (ne pas se fier aux éléments d'authentification et tokens automatiquement soumis par les navigateurs)		

6.6	**Pour les applications Web orientées public, traiter les nouvelles menaces et vulnérabilités de manière régulière et veiller à ce que ces applications soient protégées contre les attaques connues**	**Oui**	**Non**
A	Pour les applications Web orientées public, l'une des méthodes ci-dessous est-elle en place comme suit :		
B	les applications Web orientées public sont examinées (à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité automatiques ou manuels) de la manière suivante :		
	- au moins une fois par an ;		
	- après toute modification ;		
	- par une société spécialisée dans la sécurité des applications ;		
	- toutes les vulnérabilités sont corrigées ;		
	- l'application est réévaluée après les corrections		
C	un pare-feu pour applications Web est en place devant les applications Web orientées public et les attaques via Internet.		

MISE EN ŒUVRE DE MESURES DE CONTROLE D'ACCES STRICTES

1) restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître

7.1	**Restreindre l'accès aux composants du système et aux données des titulaires de cartes aux seuls individus qui doivent y accéder pour mener à bien leur travail**	**Oui**	**Non**
A	S'assure-t-on que les droits d'accès accordés aux ID d'utilisateur privilégiés sont les plus faibles nécessaires à la réalisation des obligations professionnelles ?		
B	S'assure-t-on que les privilèges sont octroyés aux individus sur la base de leur classification et de leur fonction professionnelles ?		
C	Peut-on obtenir une confirmation que l'approbation documentée par les responsables est requise (par écrit ou par voie électronique) pour tout accès, et qu'elle spécifie les privilèges requis ?		
D	Peut-on obtenir une confirmation que les contrôles d'accès sont mis en œuvre par le biais d'un système de contrôle d'accès automatisé ?		

7.2	**Définir un système de contrôle d'accès pour les composants de systèmes comptant plusieurs utilisateurs, qui limite l'accès aux seuls utilisateurs qui doivent accéder aux données et qui est configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés.**	**Oui**	**Non**
A	les systèmes de contrôle d'accès sont-ils en place sur tous les composants du système ?		
B	les systèmes de contrôle d'accès sont-ils configurés pour octroyer les privilèges aux individus en fonction de leur classification et fonction professionnelles ?		
C	les systèmes de contrôle d'accès intègrent-ils un paramètre par défaut « Refuser tout » ?		

2) affecter un ID unique à chaque utilisateur d'ordinateur

8.1	**Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants du système ou aux données de titulaires de cartes.**	**Oui**	**Non**
A	Tous les utilisateurs ont-ils un ID unique pour accéder aux composants du système ou aux données de titulaires de cartes ?		

8.2	**Outre l'affectation d'un ID unique, employer au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs : quelque chose de connu, comme un mot de passe ou une locution de passage ; quelque chose de détenu, comme un dispositif token ou une carte à puce ; quelque chose concernant l'utilisateur, comme une mesure biométrique.**	**Oui**	**Non**
A	Pour vérifier que les utilisateurs sont authentifiés à l'aide d'un ID unique et une autre méthode d'authentification (par exemple, un mot de passe) afin d'accéder à l'environnement des données de titulaires de cartes. Peut-on :		
	obtenir et examiner la documentation qui décrit les méthodes d'authentification utilisées ?		
	pour chaque type de méthode d'authentification employée et pour chaque type de composant du système, observer une authentification pour vérifier qu'elle se déroule conformément aux méthodes d'authentification décrites ?		

8.3	**Intégrer l'authentification à deux facteurs pour l'accès à distance (accès au niveau du réseau depuis l'extérieur du réseau) des employés, des administrateurs et de tiers au réseau (par exemple, authentification à distance et service de renseignements par téléphone (RADIUS) avec tokens ; système de contrôle d'accès au contrôleur d'accès du terminal (TACACS) avec tokens ; ou autres technologies permettant une authentification à deux facteurs).**	**Oui**	**Non**
A	Pour vérifier qu'une authentification à deux facteurs est utilisée pour tout accès réseau à distance. Peut-on observer un employé (par exemple un administrateur) se connectant à distance au réseau ?		
B	Peut-on vérifier que deux des trois méthodes d'authentification sont utilisées ?		

8.4	**Rendre tous les mots de passe illisibles pendant la transmission et le stockage sur tous les composants du système à l'aide d'une méthode de cryptographie robuste.**	**Oui**	**Non**
A	Sur un échantillon de composants du système, peut-on passer en revue les fichiers de mots de passe pour vérifier que les mots de passe sont illisibles pendant la transmission et le stockage ?		
B	Pour les prestataires de services seulement, peut-on passer en revue les fichiers de mots de passe pour vérifier que les mots de passe des clients sont cryptés ?		

8.5	**S'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants du système**	**Oui**	**Non**
A	Peut-on examiner les procédures et interroger le personnel pour vérifier que des procédures sont mises en œuvre pour l'identification des utilisateurs et la gestion de l'authentification, en procédant comme suit :		

B	Sélectionner un échantillon d'ID d'utilisateur, qui comprend aussi bien des administrateurs que des utilisateurs ordinaires. Vérifier que chaque utilisateur est autorisé à utiliser le système conformément à la politique en procédant comme suit :		
C	obtenir et examiner un formulaire d'autorisation pour chaque ID.		
	vérifier que les ID d'utilisateur inclus dans l'échantillon sont implémentés conformément au formulaire d'autorisation (notamment les privilèges spécifiés et obtention de toutes les signatures exigées), en suivant les informations du formulaire d'autorisation vers le système.		
D	Peut-on examiner les procédures relatives aux mots de passe ?		
E	Peut-on observer le personnel en charge de la sécurité afin de s'assurer, lorsqu'un utilisateur demande la réinitialisation de son mot de passe par téléphone, par e-mail, via Internet ou toute autre méthode n'impliquant pas un face-à-face, que son identité est vérifiée au préalable ?		
F	Peut-on observer le personnel en charge de la sécurité pour vérifier que les mots de passe initiaux de chaque nouvel utilisateur, et les mots de passe réinitialisés des utilisateurs existants sont uniques pour chaque utilisateur et qu'ils sont modifiés après leur première utilisation ?		
G	Peut-on sélectionner un échantillon d'employés qui ont quitté la société au cours des six derniers mois, et passer en revue les listes d'accès utilisateur actuelles pour vérifier que leurs ID ont été désactivés ou supprimés ?		
H	Les comptes inactifs depuis plus de 90 jours sont-ils supprimés ou désactivés ?		
I	Les comptes utilisés par les fournisseurs pour l'accès, la maintenance et l'entretien des composants du système sont-ils désactivés ?		
	ne sont-ils activés que lorsqu'une intervention du fournisseur est nécessaire ?		
J	Les comptes d'accès à distance du fournisseur sont-ils surveillés pendant leur utilisation ?		
K	Les politiques et les procédures d'authentification sont-elles connues des les utilisateurs ?		
L	Sur un échantillon de composants du système, après avoir passé en		

	revue les listes d'ID d'utilisateur :		
	les ID d'utilisateur et les comptes génériques sont-ils désactivés ou supprimés ?		
	n'existe-t-il pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ?		
	aucun ID d'utilisateur partagé ou générique n'est-il pas utilisé pour l'administration d'aucun composant du système ?		
M	Peut-on passer en revue les politiques/procédures d'authentification ?		
	les mots de passe ou autres méthodes d'authentification collectives et partagés sont-ils interdits de façon explicite ?		
N	Les administrateurs système distribuent-ils des mots de passe ni autre méthode d'authentification, collectifs ou partagés, même si on le leur demande ?		
O	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	les mots de passe utilisateur sont-ils configurés de manière à demander aux utilisateurs de modifier leur mot de passe au moins tous les 90 jours ?		
P	Pour les prestataires de services seulement, peut-on examiner les processus internes et la documentation des clients/utilisateurs ?		
	les mots de passe utilisateur non client sont-ils changés régulièrement ?		
	est-il demandé aux utilisateurs non clients de changer régulièrement leurs mots de passe, avec indication de la fréquence et des circonstances de ce changement ?		
Q	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	les mots de passe utilisateur sont-ils configurés pour comporter au moins sept caractères ?		
R	Pour les prestataires de services seulement, peut-on examiner les processus internes et la documentation des clients/utilisateurs ?		
	Est-il demandé aux utilisateurs non clients de définir des mots de passe		

	comportant un nombre de caractères ?		
S	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	les mots de passe sont-ils configurés pour comporter des caractères alphanumériques ?		
T	Pour les prestataires de services seulement, peut-on examiner les processus internes et la documentation des clients/utilisateurs ?		
	Est-il demandé aux utilisateurs non clients de définir des mots de passe comportant des caractères alphanumériques ?		
U	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	Exigent-on que les nouveaux mots de passe ne puissent pas être identiques aux quatre derniers mots de passe utilisés ?		
V	Pour les prestataires de services seulement, peut-on examiner les processus internes et la documentation des clients/utilisateurs ?		
	les nouveaux mots de passe des utilisateurs non clients sont-ils identiques aux quatre derniers utilisés ?		
W	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	les paramètres d'authentification sont-ils configurés pour exiger le verrouillage d'un compte d'utilisateur après six tentatives de connexion non valides au maximum ?		
X	Pour les prestataires de services seulement, peut-on examiner les processus internes et la documentation des clients/utilisateurs ?		
	les comptes des utilisateurs non clients sont provisoirement-ils verrouillés après six tentatives d'accès non valides au maximum ?		
Y	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		
	les mots de passe sont-ils configurés pour exiger qu'un compte d'utilisateur, une fois verrouillé, reste à cet état 30 minutes au moins ou jusqu'à ce qu'un administrateur système réinitialise le compte ?		
Z	Sur un échantillon de composants du système, peut-on obtenir et contrôler les paramètres de configuration du système ?		

	les fonctions d'expiration du système/de la session sont-elles réglées sur 15 minutes ou moins ?		
A	Peut-on examiner les paramètres de configuration de la base de données et de l'application ?		
	tous les utilisateurs s'authentifient-ils avant d'y accéder ?		
B	Les paramètres de configuration de la base de données et de l'application garantissent-ils que tous les accès d'utilisateurs aux bases de données, toutes les consultations et toutes les actions exécutées dans celles-ci (par exemple, déplacement, copie, suppression d'informations) s'effectuent exclusivement au moyen de méthodes programmées (par exemple, par le biais de procédures stockées) ?		
C	Les paramètres de configuration de la base de données et de l'application restreignent-ils l'accès direct des utilisateurs ou les requêtes aux bases de données aux seuls administrateurs de bases de données ?		
D	Peut-on examiner les applications de base de données et les ID d'application associés ?		
	ces derniers ne peuvent-ils pas être utilisés que par les applications (et non par des utilisateurs individuels ou d'autres processus) ?		

3) restreindre l'accès physique aux données des titulaires de cartes

9.1	**Utiliser des contrôles d'accès aux installations appropriés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de cartes.**	**Oui**	**Non**
A	Des contrôles de sécurité physiques sont-ils en place dans chaque salle informatique, centre de données et autres zones physiques qui abritent des systèmes appartenant à l'environnement des données de titulaires de cartes ?		
	L'accès est-il contrôlé par des lecteurs de badge et autres dispositifs tels que des badges autorisés, des clés et des cadenas ?		
	Peut-on observer un administrateur système pendant qu'il tente de se connecter sur les consoles de systèmes choisis de façon aléatoire dans l'environnement des données de titulaires de cartes ?		

	ces consoles sont-elles « verrouillées » pour empêcher toute utilisation non autorisée ?		
B	Des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès sont-ils en place pour surveiller les points d'entrée/de sortie des zones sensibles ?		
C	Les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont-ils protégés contre la falsification ou la désactivation ?		
D	les caméras vidéo et/ou autres mécanismes de contrôle d'accès sont-ils sous surveillance ?		
	les données enregistrées sont-elles conservées pendant trois mois au moins ?		
E	Peut-on interroger les administrateurs réseau ?		
	peut-on observer si les prises réseau ne sont activées que lorsque le personnel autorisé sur place a besoin de les utiliser ?		
	les visiteurs sont-ils accompagnés à tout moment dans les zones contenant des prises réseau actives ?		
F	l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans fil est-il restreint de la manière appropriée ?		

9.2	**Élaborer des procédures qui aident à faire facilement la distinction entre le personnel du site et les visiteurs, en particulier dans les zones où sont accessibles les données de titulaires de cartes.**	**Oui**	**Non**
A	Peut-on passer en revue les processus et les procédures d'attribution de badges au personnel du site et aux visiteurs ?		
	Ces processus et procédures incluent-ils la remise de nouveaux badges ?		
	Ces processus et procédures incluent-ils le changement des conditions d'accès ?		
	Ces processus et procédures incluent-ils la révocation des badges des personnels ne travaillant plus sur le site et des badges visiteurs		

	périmés ?		
B	L'accès au système de badges est-il restreint au seul personnel autorisé ?		
C	les badges en cours d'utilisation identifient-ils clairement les visiteurs ?		
	est-il facile de distinguer les visiteurs du personnel du site ?		

9.3	**S'assurer que tous les visiteurs sont traités de la manière suivante**	**Oui**	**Non**
A	Vérifier que des contrôles des visiteurs sont en place comme suit :		
	Observer l'utilisation des badges d'ID des visiteurs afin de vérifier qu'un tel badge ne permet pas d'accéder aux zones physiques où sont stockées les données des titulaires de carte sans être accompagné.		
	Observer les gens au sein de l'établissement afin de vérifier l'utilisation des badges d'ID visiteur et de s'assurer qu'ils permettent de clairement distinguer les visiteurs du personnel du site.		
	Vérifier que les badges des visiteurs portent une date d'expiration.		
	Observer les visiteurs qui quittent les locaux pour vérifier qu'on leur demande bien de remettre leur badge d'identification à la sortie ou à l'expiration du badge		

9.4	**Utiliser un registre des visites pour tenir un contrôle physique de la circulation des visiteurs. Y consigner le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son accès physique. Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi**	**Oui**	**Non**
A	un registre des visites est-il utilisé pour consigner l'accès physique aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de cartes ?		
	ce registre comporte-t-il le nom du visiteur, l'entreprise qu'il représente et le personnel du site qui autorise son accès physique ?		
	ce document est-il conservé pendant au moins trois mois ?		

9.5	**Ranger les sauvegardes sur support en lieu sûr, de préférence hors de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an.**	**Oui**	**Non**
A	Peut observer la sécurité physique du site de stockage ?		
	le stockage des supports de sauvegarde est-il sécurisé ?		
B	La sécurité physique du site de stockage est-elle passée en revue au moins une fois par an ?		

9.6	**Assurer la sécurité physique de tous les supports.**	**Oui**	**Non**
A	Les procédures de protection des données de titulaires de cartes comprennent-elles le contrôle de la sécurité physique de tous les supports (entre autres, ordinateurs, supports électroniques amovibles, réseaux, reçus et rapports sur papier, et fax)		

9.7	**Assurer un contrôle strict de la distribution interne ou externe de tout type de support**	**Oui**	**Non**
A	Une politique est-elle en place pour le contrôle de la distribution des supports ?		
	celle-ci couvre-t-elle tous les supports distribués, y compris ceux qui sont remis aux individus ?		
B	Tous les supports sont-ils classés afin de déterminer la sensibilité des données qu'ils contiennent ?		
C	Tous les supports expédiés à l'extérieur sont-ils consignés et autorisés par les responsables ?		
	sont-ils envoyés par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis ?		

9.8	**S'assurer que les responsables approuvent tous les supports déplacés d'une zone sécurisée (en particulier s'ils sont distribués à des individus).**	**Oui**	**Non**
A	Peut-on choisir un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports ?		
	les informations de suivi et les autorisations appropriées des responsables y sont-ils consignées ?		

9.9	**Assurer un contrôle strict du stockage et de l'accessibilité des supports.**	**Oui**	**Non**
A	Peut-on obtenir et examiner la politique de contrôle du stockage et de la gestion des supports ?		
	Stipule-t-elle l'inventaire des supports à intervalles réguliers ?		
B	Peut-on obtenir et passer en revue le journal d'inventaire des supports ?		
	un inventaire des supports est-il réalisé au moins une fois par an ?		

9.10	**Détruire les supports lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou légales comme suit :**	**Oui**	**Non**
A	Peut-on obtenir et examiner la politique de destruction périodique des supports ?		
	couvre-t-elle tous les supports ?		
	les points suivants sont respectés :		
B	les documents papier sont déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être reconstitués.		
	examiner les conteneurs dans lesquels sont stockées les informations à détruire afin de vérifier qu'ils sont bien protégés. Par exemple, s'assurer que le conteneur portant la mention « À déchiqueter » est doté d'un dispositif de verrouillage empêchant d'accéder à son contenu		

C	Les données de titulaires de cartes sur support électronique sont-elles rendues irrécupérables à l'aide d'un programme de nettoyage sécurisé, conformément aux normes du secteur en matière d'élimination sécurisée des informations, ou à l'aide de tout autre procédé de destruction physique des supports (par exemple, par démagnétisation) ?		

SURVEILLANCE DE TESTS REGULIERS DES RESEAUX

1) effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes

10.1	**Définir un processus pour associer chaque accès aux composants du système (en particulier les accès avec des droits administrateur, tels que root) à chaque utilisateur individuel.**	**Oui**	**Non**
A	Peut-on observer les activités et interroger l'administrateur système ?		
B	les vérifications à rebours des composants du système sont-ils activés et actifs ?		

10.2	**Mettre en œuvre des vérifications à rebours automatisées pour tous les composants du système afin de reconstituer les événements suivants :**	**Oui**	**Non**
A	Tous les accès des utilisateurs aux données de titulaires de cartes sont-ils consignés ?		
B	Les actions exécutées par tout utilisateur avec des droits root ou administrateur sont-elles consignées ?		
C	Les accès à toutes les vérifications à rebours sont-ils consignés ?		
D	Les tentatives d'accès logique non valides sont-elles consignées ?		
E	L'utilisation des mécanismes d'identification et d'authentification est-elle consignée ?		
F	L'initialisation des journaux d'audit est-elle consignée ?		
G	La création et la suppression d'objets au niveau système sont-elles consignées ?		

10.3	**Consigner dans les vérifications à rebours au moins les entrées suivantes pour chaque événement :**	**Oui**	**Non**
A	Les ID d'utilisateur sont-ils inclus dans les entrées des journaux ?		
B	Le type d'événement est-il inclus dans les entrées des journaux ?		
C	L'horodatage est-il inclus dans les entrées des journaux ?		
D	L'indication de succès ou d'échec est-elle incluse dans les entrées des journaux ?		
E	L'origine de l'événement est-elle incluse dans les entrées des journaux ?		
F	L'identité ou le nom des données, du composant du système ou de la ressource affectés est-l inclus dans les entrées des journaux ?		

10.4	**À l'aide d'une technologie de synchronisation temporelle, synchroniser tous les systèmes d'horloge et temporels critiques et s'assurer que les éléments suivants sont mis en œuvre pour l'acquisition, la distribution et l'enregistrement du temps.**	**Oui**	**Non**
A	Une technologie de synchronisation temporelle est-elle mise en œuvre et active selon les conditions 6.1 et 6.2 de la norme PCI DSS ?		
B	Peut-on obtenir et examiner le processus d'acquisition et de distribution et d'enregistrement de l'heure correcte au sein de l'entreprise ainsi que les paramètres systèmes d'horloge sur un échantillon de composants du système ?		
	seuls des serveurs temporels reçoivent-ils des signaux temporels de sources externes et que ces demiers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné) ?		
	les serveurs temporels centraux désignés se consultent-ils mutuellement pour maintenir l'exactitude de l'heure ?		
	les autres serveurs internes ne reçoivent-ils l'heure que de ces serveurs temporels centraux ?		
C	Peut-on examiner les configurations du système et des paramètres de synchronisation temporelle ?		

	l'accès aux données temporelles est-il restreint au seul personnel dont l'accès à ces données est justifié par un besoin professionnel ?		
D	Peut-on examiner les processus et configurations du système et des paramètres de synchronisation temporelle ?		
	tout changement aux paramètres temporels sur des systèmes critiques est-il consigné, surveillé et vérifié ?		
E	Les serveurs temporels acceptent-ils des mises à jour temporelles de sources externes spécifiques, reconnues par le secteur (afin de prévenir toute tentative malveillante de changer l'horloge) ?		
	est-il également possible de crypter ces mises à jour avec une clé symétrique, et de créer des listes de contrôle d'accès qui indiquent les adresses IP des machines clientes qui recevront les mises à jour temporelles (afin d'empêcher toute utilisation non autorisée des serveurs d'horloge internes) ?		

10.5	**Protéger les vérifications à rebours de sorte qu'elles ne puissent pas être modifiées.**	**Oui**	**Non**
A	En interrogeant l'administrateur système peut-on passer en revue les autorisations ?		
	les vérifications à rebours sont-ils uniquement accessibles aux individus qui en ont besoin pour mener à bien leur travail ?		
	les fichiers de vérifications à rebours existants sont-ils protégés contre toute modification non autorisée par des mécanismes de contrôle d'accès, leur isolation physique et/ou l'isolation du réseau ?		
	les fichiers de vérifications à rebours sont-ils rapidement sauvegardés sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer ?		
	les journaux des technologies orientées vers l'extérieur (par exemple, sans fil, pare-feu, DNS, messagerie) sont-ils déchargés ou copiés sur un support ou sur un serveur centralisé interne réservé à la journalisation sécurisée ?		
	les journaux sont-ils analysés à l'aide d'un logiciel de contrôle de		

	l'intégrité des fichiers ou de détection des modifications en passant en revue les paramètres système ainsi que les fichiers contrôlés et les résultats des activités de contrôle ?		

10.6	**Passer en revue les journaux relatifs à tous les composants du système au moins une fois par jour. L'examen des journaux doit inclure les serveurs exécutant des fonctions des sécurité, tels que les serveurs IDS (système de détection d'intrusion) et AAA (Authentication, Authorization, and Accounting) (par exemple, RADIUS).**	**Oui**	**Non**
A	Peut-on obtenir et examiner les politiques et les procédures de sécurité ?		
	comprennent-elles des procédures d'analyse des journaux de sécurité au moins une fois par jour ?		
	et exigent-elles le suivi des anomalies ?		
B	En observant et en interrogeant les utilisateurs, les journaux relatifs à tous les composants du système sont-ils régulièrement vérifiés ?		

10.7	**Conserver l'historique des vérifications à rebours pendant une aunée au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, pour analyse (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde).**	**Oui**	**Non**
A	Peut-on obtenir et examiner les politiques et les procédures de sécurité ?		
	Comprennent-elles des dispositions pour la conservation des journaux, dont elles fixent la période à un an au moins ?		
B	Les journaux d'audit sont-ils disponibles pendant un an au moins ?		
	des processus sont-ils en place pour restaurer immédiatement les journaux des trois derniers mois au moins, pour analyse ?		

2) tester régulièrement les processus et les systèmes de sécurité

11.1	**Tester la présence de points d'accès sans fil et détecter les points d'accès sans fil non autorisés tous les trimestres.**	**Oui**	**Non**
A	L'entreprise possède-t-elle un processus documenté pour détecter et identifier les points d'accès sans fil, tous les trimestres ?		
B	La méthodologie est-elle appropriée ?		
C	Permet-elle de détecter et d'identifier tout point d'accès sans fil non autorisé, notamment au moins ce qui suit :		
	cartes WLAN insérées dans les composants du système ;		
	dispositifs sans fil portatifs connectés aux composants du système (par exemple, par USB, etc.) ;		
	dispositifs sans fil branchés sur un port réseau ou à périphérique réseau		
D	Le processus documenté pour identifier les points d'accès sans fil non autorisés est-il exécuté au moins chaque trimestre pour tous les composants du système et toutes les Installations ?		
E	Si l'on utilise une surveillance automatisée (par exemple systèmes de détection et/ou de prévention d'intrusions sans fil, NAC, etc.), la configuration déclenchera-t-elle des alertes pour le personnel ?		
F	Le plan de réponse aux incidents de l'entreprise (condition 12.9) prévoit-il une réaction en cas de détection de périphériques sans fil non autorisés ?		

11.2	**Analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux (par exemple, installation de nouveaux composants du système, modification de la topologie du réseau ou des règles des pare-feu, mise à niveau de produits).**	**Oui**	**Non**
A	Les analyses de vulnérabilité interne et externe sont-elles exécutées comme suit :		
	Examiner les rapports d'analyse et vérifier que quatre analyses trimestrielles internes ont eu lieu au cours de la période de 12 mois la		

	plus récente.		
	Examiner les rapports d'analyse et vérifier que le processus d'analyse comprenne de nouvelles analyses jusqu'à obtenir un résultat satisfaisant ou jusqu'à ce que toutes les vulnérabilités à « haut risque », définies à la condition 6.2 de la norme PCI DSS, aient été résolues		
	Vérifier que l'analyse a été effectuée par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).		
B	Peut-on examiner les résultats des quatre analyses trimestrielles de vulnérabilité externe les plus récentes ?		
	ont-elles toutes eu lieu au cours de la période de 12 mois la plus récente ?		
C	Peut-on examiner les résultats de chacune des quatre analyses trimestrielles ?		
	satisfont-elles aux conditions du guide de programme ASV (par exemple, pas de vulnérabilité supérieure à la note 4.0 du CVSS et aucune défaillance automatique) ?		
D	Peut-on examiner les rapports d'analyse ?		
	les analyses ont-elles été réalisées par un prestataire de services d'analyse agréé (ASV) par le PCI SSC ?		
E	Peut-on inspecter la documentation de contrôle des changements et analyser les rapports ?		
	les composants du système assujettis à un changement d'importance ont-ils été analysés ?		
F	Peut-on examiner les rapports d'analyse et vérifier que le processus d'analyse stipule de nouvelles analyses jusqu'à ce que :		
	aucune vulnérabilité supérieure à la note 4.0 du CVSS ne soit détectée pour les analyses externes ;		
	un résultat satisfaisant soit obtenu ou jusqu'à ce que toutes les vulnérabilités à « haut risque », définies dans la condition 6.2 de la norme PCI DSS, aient été résolues, pour les analyses internes.		

G	l'analyse a-t-elle été effectuée par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV) ?		

11.3	**Effectuer des tests de pénétration externe et interne au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement)**	**Oui**	**Non**
A	Peut-on obtenir et passer en revue les résultats du dernier test de pénétration ?		
	un tel test est-il effectué au moins une fois par an et après tout changement signifieatif de l'environnement. ?		
B	Les vulnérabilités relevées et exploitables ont-elles été corrigées et que les tests ont été réexécutés ?		
C	le test a-t-il été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV) ?		
D	les tests de pénétration comprennent-ils des tests de pénétration de la couche réseau ?		
	Ces tests incluent-ils les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation ?		
E	les tests de pénétration comprennent-ils des tests de pénétration de la couche application ?		
	les tests comprennent-ils au minimum les vulnérabilités répertoriées dans la condition 6.5 ?		

11.4	**Utiliser des systèmes de détection d'intrusions et/ou des systèmes de prévention d'intrusions pour contrôler l'intégralité du trafic, ainsi que les points critiques, dans l'environnement des données de titulaires de cartes et signaler au personnel tous les soupçons portant sur des altérations potentielles. Tenir à jour tous les moteurs de détection et de prévention des intrusions, les références et les signatures.**	**Oui**	**Non**
A	Utilise-t-on des systèmes de détection d'intrusions et/ou de systèmes de prévention d'intrusions pour contrôler l'intégralité du trafic, ainsi que les points critiques, dans l'environnement des données de titulaires de cartes ?		
B	Les systèmes de détection et/ou de prévention d'intrusions sont-ils configurés pour alerter le personnel sur des altérations potentielles ?		
C	Peut-on examiner les configurations des systèmes de détection et/ou de prévention d'intrusions ?		
	le matériel correspondant est-il configuré, géré et mis à jour conformément aux instructions des fournisseurs pour garantir une protection optimale ?		

11.5	**Déployer des logiciels de contrôle de l'intégrité des fichiers pour alerter le personnel de toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques, et configurer ces logiciels pour effectuer des comparaisons entre les fichiers stratégiques au moins une fois par semaine.**	**Oui**	**Non**
A	Utilise-t-on des outils de contrôle de l'intégrité des fichiers dans l'environnement des données de titulaires de cartes en examinant les paramètres système et les fichiers contrôlés, ainsi que les résultats des activités de contrôle ?		
B	Contrôle-t-on les fichiers suivants :		
	exécutables du système ;		

	exécutables des applications ;		
	fichiers de configuration et de paramètres ;		
	fichiers d'historique, d'archive, de journaux et d'audit stockés à un emplacement centralisé.		
C	les outils sont-ils configurés de manière à alerter le personnel de toute modification non autorisée des fichiers stratégiques et à procéder à de comparaisons de fichiers stratégiques au moins une fois par semaine ?		

GESTION D'UNE POLITIQUE DE SECURITE DES INFORMATIONS

1) gérer une politique de sécurité es informations pour l'ensemble du personnel

12.1	**Définir, publier, gérer et diffuser une politique de sécurité qui remplit les fonctions suivantes :**	**Oui**	**Non**
A	Peut-on passer en revue la politique de sécurité des informations ?		
	est-elle publiée et diffusée à tout le personnel concerné (mais aussi aux fournisseurs et partenaires commerciaux) ?		
B	la politique satisfait-elle à toutes les conditions de la norme PCI DSS ?		
C	Le processus annuel d'évaluation des risques qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques est-t-il documenté ?		
D	Peut-on examiner la documentation d'évaluation des risques ?		
E	le processus d'évaluation est-t-il exécuté au moins une fois par an ?		
F	la politique de sécurité des informations est-elle passée en revue au moins une fois par an et mise à jour le cas échéant, pour tenir compte des modifications apportées aux objectifs de l'entreprise ou à l'environnement de risque ?		

12.2	**Élaborer des procédures de sécurité opérationnelles quotidiennes conformes aux exigences de cette spécification (par exemple, des procédures de gestion des comptes d'utilisateur et des procédures d'examen des journaux)**	**Oui**	**Non**

A	Peut-on examiner les procédures de sécurité opérationnelles quotidiennes ?		
	sont-elles conformes à cette spécification		
	comprennent-elles des procédures administratives et techniques pour chaque condition ?		

12.3	**Élaborer les politiques d'utilisation des technologies stratégiques (par exemple, technologies d'accès à distance, technologies sans fil, supports électroniques amovibles, ordinateurs portables, assistants numériques personnels (PDA), utilisation du courrier électronique et d'Internet) et définir l'usage approprié de ces technologies. S'assurer que ces politiques d'utilisation exigent ce qui suit :**	**Oui**	**Non**
A	Peut-on obtenir et examiner la politique d'utilisation des technologies stratégiques ?		
B	Les politiques d'utilisation exigent-elles l'approbation explicite des responsables pour l'utilisation des technologies ?		
C	Les politiques d'utilisation exigent-elles que l'utilisation de toute technologie soit authentifiée à l'aide d'un ID d'utilisateur et d'un mot de passe, ou toute autre méthode d'authentification (par exemple, token) ?		
D	Les politiques d'utilisation exigent-elles une liste de tous les périphériques et personnel autorisé à utiliser ce matériel ?		
E	Les politiques d'utilisation exigent-elles que soient indiqués sur les périphériques le nom de leur propriétaire, ses coordonnées et leur usage ?		
F	Les politiques d'utilisation exigent-elles un usage acceptable de la technologie ?		
G	Les politiques d'utilisation exigent-elles des emplacements acceptables des technologies sur le réseau ?		
H	Les politiques d'utilisation exigent-elles une liste des produits approuvés par la société ?		
I	Les politiques d'utilisation exigent-elles la déconnexion automatique des sessions des technologies d'accès à distance après une période		

	d'inactivité spécifique ?		
J	Les politiques d'utilisation exigent-elles l'activation des technologies d'accès à distance utilisées par les fournisseurs et partenaires commerciaux, uniquement lorsque c'est nécessaire, avec désactivation immédiate après usage ?		
K	Les politiques d'utilisation interdisent-elles la copie, le déplacement ou le stockage des données de titulaires de cartes sur des disques durs locaux et des supports électroniques amovibles lors de l'accès à ces informations au moyen de technologies d'accès à distance ?		
L	Pour le personnel dûment autorisé, les politiques d'utilisation exigent-elles la protection des données des titulaires de cartes conformément aux conditions de la norme PCI DSS ?		

12.4	**S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tout le personnel en la matière.**	**Oui**	**Non**
A	Les politiques de sécurité des informations définissent-elles clairement les responsabilités de tout le personnel en la matière ?		

12.5	**Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations :**	**Oui**	**Non**
A	la sécurité des informations a-t-elle été assignée formellement à un chef de la sécurité ou tout autre responsable compétent ?		
	Peut-on obtenir et examiner les politiques et les procédures de sécurité des informations ?		
B	les responsabilités suivantes en matière de sécurité des données sont-elles assignées de manière spécifique et formelle :		
	Vérifier que la responsabilité de l'établissement et de la distribution des procédures et politiques de sécurité est formellement attribuée au personnel compétent.		
	Vérifier que la responsabilité du contrôle, de l'analyse des alertes de sécurité, et de la diffusion des informations aux chefs de divisions		

	appropriés et au personnel chargé de la sécurité est formellement assignée au personnel compétent.		
	Vérifier que la responsabilité de l'établissement et de la diffusion des politiques et des procédures de remontée et de réponse aux incidents liés à la sécurité est formellement assignée au personnel compétent.		
	Vérifier que la responsabilité de l'administration des comptes d'utilisateur et de la gestion des authentifications est formellement assignée au personnel compétent.		
	Vérifier que la responsabilité de la surveillance et du contrôle de tous les accès aux données est formellement assignée au personnel compétent		

12.6	**Mettre en œuvre un programme formel de sensibilisation à la sécurité pour sensibiliser les employés à l'importance de la sécurité des données de titulaires de cartes.**	**Oui**	**Non**
A	un programme formel de sensibilisation à la sécurité de tout le personnel est-il en place ?		
B	Peut-on obtenir et examiner les procédures et la documentation du programme de sensibilisation à la sécurité, et procéder comme suit :		
	Vérifier que le programme de sensibilisation à la sécurité comprend plusieurs méthodes de sensibilisation et de formation du personnel (par exemple, affiches, lettres, mémos, formations sur le Web, réunions et promotions).		
	Vérifier que le personnel participe à des formations de sensibilisation au moment de son recrutement et au moins une fois par an.		
	Vérifier que le programme de sensibilisation à la sécurité exige que le personnel reconnaisse, par écrit ou par voie électronique, au moins une fois par an, avoir lu et compris la politique de sécurité des informations.		

12.7	**Effectuer une sélection préalable à l'embauche du personnel pour minimiser les risques d'attaques par des sources internes (Ces**	**Oui**	**Non**

	contrôles devraient inclure, par exemple, les antécédents professionnels, le casier judiciaire, les renseignements de solvabilité et la vérification des références).		
A	En interrogeant le responsable des ressources humaines, existent-t-il, avant toute embauche, des contrôles des antécédents professionnels (dans les restrictions imposées par la loi) pour le personnel qui aura accès aux données des titulaires de cartes ou à l'environnement de ces données ?		

12.8	**Si les données de titulaires de cartes sont partagées avec des prestataires de services, gérer et mettre en œuvre des politiques et des procédures de gestion de ces derniers, de manière à inclure :**	**Oui**	**Non**
A	Si l'entité partage des données de titulaires de cartes avec des prestataires de services (par exemple, sites de stockage sur bandes de sauvegarde, prestataires de services gérés tels que les prestataires de services d'hébergement sur le Web ou les prestataires de services de sécurité, ou encore les prestataires qui reçoivent des données en vue de la modélisation des fraudes). Peut-on observer les intervenants, examiner les politiques et les procédures ainsi que les documents justificatifs pour :		
	une liste des prestataires de services est-elle tenue ?		
	l'accord écrit stipule-t-il la reconnaissance par les prestataires de services de leur responsabilité en matière de protection des données de titulaires de cartes ?		
	les politiques et les procédures sont-elles décrites et respectées, notamment le contrôle préalable à l'engagement de tout prestataire de services ?		
	l'entité a-t-elle mise en place un programme qui contrôle la conformité de ses prestataires de services à la norme PCI DSS au moins une fois par an ?		

12.9	**Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système.**	**Oui**	**Non**
A	Peut-on obtenir et examiner le plan de réponse aux incidents et les procédures associées ?		
B	le plan de réponse aux incidents inclut-il :		
	les rôles, les responsabilités et les stratégies de communication en cas d'incident, notamment la notification des marques de cartes de paiement, au minimum		
	les procédures de réponse aux incidents spécifiques		
	les procédures de continuité et de reprise des affaires		
	le processus de sauvegarde des données		
	l'analyse des exigences légales en matière de signalement des incidents (par exemple, le California Bill 1386, qui exige la notification des consommateurs affectés en cas d'incident avéré ou soupçonné pour toute entreprise comptant des résidents en Californie dans sa base de données)		
	la couverture et les réponses de tous les composants stratégiques du système		
	la référence ou l'inclusion des procédures de réponse aux incidents des marques de cartes de paiement		
C	Peut-on examiner la documentation d'un incident ou d'une alerte signalés antérieurement ?		
	les procédures et le plan documenté de réponse aux incidents sont-ils suivis ?		
D	Le plan est-il testé au moins une fois par an ?		
E	À travers l'observation et l'examen des politiques ? des équipes de réponse aux incidents sont-elles disponibles 24 heures sur 24 et sept jours sur sept ?		
	toutes les activités non autorisées, la détection des points d'accès sans fil non autorisés, les alertes des systèmes de détection d'incidents et/ou le signalement de toute modification non autorisée du contenu des fichiers ou des systèmes stratégiques sont-ils sous surveillance ?		
F	le personnel chargé de la réponse aux violations de la sécurité reçoit-il		

	une formation périodique ?		
G	le contrôle et la réponse aux alertes émises par les systèmes de sécurité, y compris la détection des points d'accès sans fil non autorisés, sont-ils prévus dans le plan de réponse aux incidents ?		
H	un processus est-il en place pour la modification et le développement du plan de réponse aux incidents en fonction des leçons apprises, et la prise en compte de l'évolution du secteur ?		

ANNEXE 6 : SECURISATION D'UNE CARTE PENDANT LA FABRICATION

PHASES ET ACTEURS	**DEMARCHE DE SECURISATION DE LA CARTE**
Conception : Concepteur	Elle se traduit par la protection du cahier de charge du circuit intégré, des documents de conception, des logiciels, des procédures de pré personnalisation et le contrôle de l'environnement de production
Fabrication : Fabricant	Le fabricant procède au sondage des puces, au blocage par chiffrement symétrique des puces avec une clé de fabrication de 8 à 16 bits, à la gravure du numéro de lot de fabrication et numéro de fabricant
Pré personnalisation : fournisseur	Le fournisseur détache des puces individuelles. Il effectue des tests et moulage sous pression des puces dans les cartes en plastique fraisées. Après intervient : - la gravure du logo du fournisseur de l'application sur le dos de la carte, - la vérification du fonctionnement correct de l'ensemble, - le déblocage du microprocesseur à l'aide d'une clé de fabrication, - l'ajout du système d'exploitation et gravure du numéro de série de la carte, - le blocage de l'écriture par accès direct à la mémoire, - le dialogue avec la mémoire par adressage logique uniquement, le blocage par chiffrement à l'aide d'une clé de pré personnalisation ou de transport.
Personnalisation : l'éditeur d'application	L'éditeur d'application procède à l'enregistrement des fichiers de données et données d'application et au stockage de l'identité du porteur, son code confidentiel, les codes de déblocages

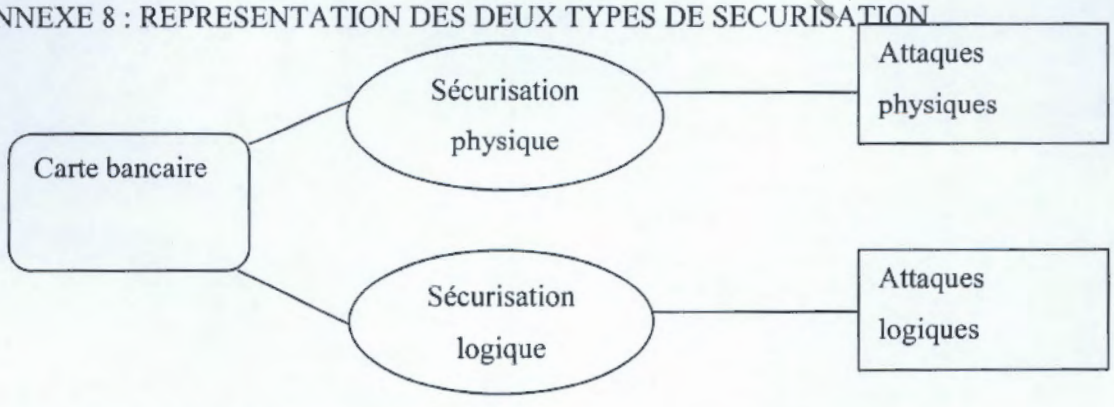
Source : nous-même d'après SHERIF et SERHROUCHNI (2000 : 402)

ANNEXE 7 : CYCLE DE VIE DU PCI DSS

CYCLE DE VIE DU PCI DSS	
Etape 1	Implémentation : C'est l'étape de la mise en place du standard. Elle va du 1er au 9ème mois et suit la dernière révision du standard.
Etape 2	Retour d'expérience : C'est l'étape à laquelle on prend en compte les observations et avis qui serviront à faire évoluer le standard à travers un processus formel. Elle va du 10ème au 12ème mois.
Etape 3	Revue des retours d'expérience : A ce niveau, une centralisation de tous les retours d'expérience est faite. Un groupe de travail technique du PCI SSC analyse ces retours et prend l'une des mesures suivantes : aucune action si le retour n'est pas jugé pertinent, la réalisation de documents complémentaires permettant de supporter la version actuelle et l'édition d'une nouvelle révision de PCI DSS le cas échéant. Cette étape dure 8 mois et va du 13ème au 20ème mois.
Etape 4	Elaboration et finalisation de la nouvelle version : Le PCI SSC finalise ici la nouvelle version ou révision du PCI DSS en vue de sa publication. Il fournit une liste des modifications et la date de publication. Elle dure 4 mois et s'étend du 21ème au 24ème mois.
Etape 5	Publication de la nouvelle version du standard : C'est l'étape qui marque la clôture du cycle par la publication de la nouvelle version. Elle intervient au 24ème mois. Le cycle peut reprendre pour une nouvelle version.

Source : nous-même d'après CHUVAKIN et WILLIAMS (2009 : 35)

ANNEXE 8 : REPRESENTATION DES DEUX TYPES DE SECURISATION



Source : nous-même à partir CARPETIER (2009 : 39)

ANNEXE 9 : ROLES ET RESPONSABILITES DES ACTEURS DU PCI DSS

Acteurs	Rôles / Responsabilités
PCI SSC	Il est chargé d'émettre de nouvelles normes, d'améliorer la sécurité des comptes de paiement, de sensibiliser et générer l'adoption du public, d'encourager la participation et obtenir du feedback, de gérer le processus de qualification et de test d'approbation pour les laboratoires ASV, QSA et PED et de maintenir leur liste à jour. Il est responsable du développement, de la gestion, de l'éducation et de la sensibilisation aux normes de sécurité PCI, dont : la norme de sécurité des données (DSS), la norme de sécurité des données d'application de paiement (PA-DSS) et les besoins liés au service de saisie du PIN (PED).
Les banques (Les Acquéreurs)	Elles sont en charge de l'émission des cartes bancaires pour ses clients en conformité avec le PCI DSS. Elles sont chargées de définir le niveau de conformité à PCI DSS des marchands et son maintien dans le temps, de définir le niveau du marchand en fonction du nombre consolidé de transactions par carte, de décider lequel des questionnaires d'auto-évaluation (SAQ-A, B, C ou D) le marchand doit remplir, d'accepter ou refuser un contrôle compensatoire ou simplement définir son interprétation d'une exigence, et enfin d'arbitrer les débats entre le marchand et le QSA.
Marchands	Ce sont des négociants agréés qui ont pour rôle d'accepter des cartes pour le paiement des marchandises et des services. Leur responsabilité est de démontrer leur niveau de conformité au standard PCI DSS
Acteurs	Rôles / Responsabilités
Fournisseurs des services de paiement (PSP)	Ce sont des organisations qui traitent, stockent, ou transmettent des données de titulaire de carte pour le compte des membres de carte, des négociants, ou d'autres fournisseurs de services. Leur responsabilité est d'être en conformité avec le PCI DSS
Hébergeur, fournisseurs d'application	Ils interviennent dans les paiements d'une manière directe ou indirecte. Leur responsabilité est de démontrer leur niveau de conformité au standard PCI DSS

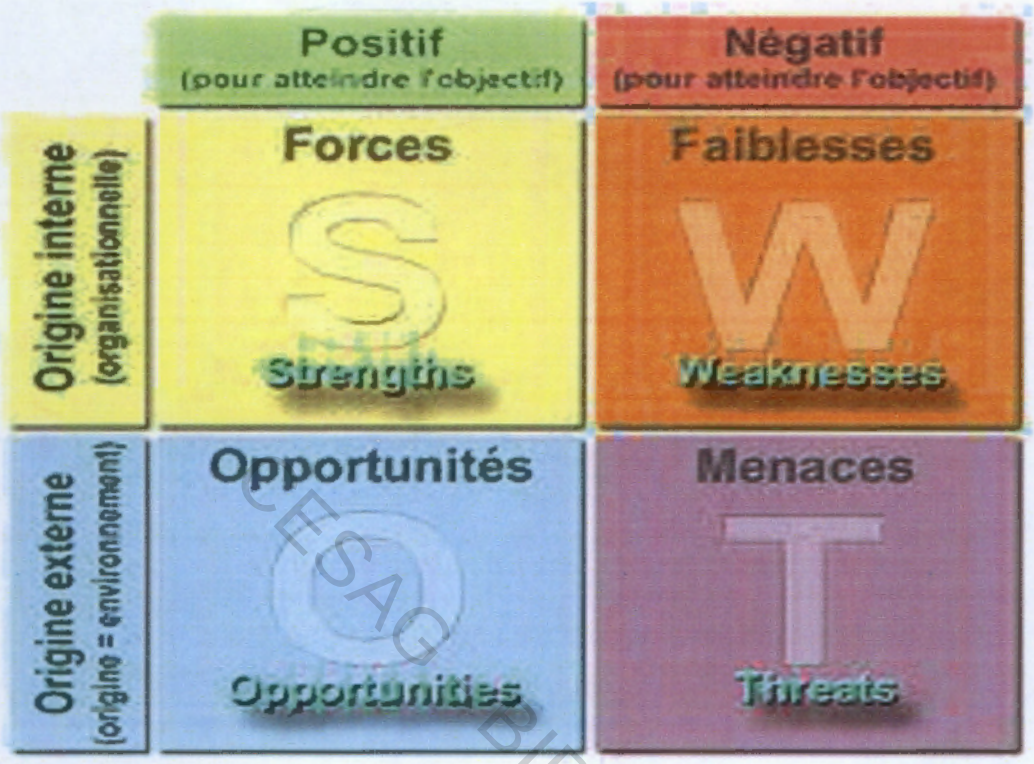
Source : nous-même d'après le glossaire dans site du PCI DSS (2012)

ANNEXE 10 : COMPARAISON DU PCI DSS ET LES AUTRES REFERENTIELS

Eléments comparatifs	**PCI DSS**	**ISO 27001/27002**	**COBIT**	**ITIL**
Elaboration	Emane des organismes de cartes eux-mêmes	Provient de l'organisation internationale de normalisation	Provient de l'ISACA (Information System Audit and Control Association)	Emane du code de bonne pratique des organisations
Périmètre	Toutes les organisations qui transmettent, traitent ou stockent des données de carte de paiement	Souple : entreprises à activités très différentes	Toutes les organisations qui utilisent les TIC (Technologies de l'Information et de la Communication)	Toute organisation de production informatique
Mesures de sécurité	Rigide : l'organisation de la sécurité liée à la carte bancaire	Souple : l'organisation de la sécurité dans sa globalité	Rigide : l'organisation de la sécurité liée au système d'information	Rigide : l'organisation de la sécurité de l'information
Conformité aux exigences et pré requis	Rigides : obligatoire	Souple : suggérée	Souple : suggérée	Souple : suggérée
Risques	Risques liés aux cartes bancaires	Risques variés	Risques liés au système d'information	Risques liés à l'informatique

Source : nous d'après VON SOLMS et VON SOLMS (2008 : 46), CALDER (2006 : 12), NOIRAULT (2008 : 7-8)

ANNEXE 11 : OUTIL SWOT



Source : Fernandez (2010 : 189)

ANNEXE 12 : LES CARTES BANCAIRES A LA SCB

1) Standard Chartered Priority Banking Credit Card

2) Standard Chartered Preferred Banking Credit Card

3) Standard Chartered executive platinum Credit Card

4) Standard Chartered executive Credit Card

5) Standard Chartered Platinum Credit Card

6) Standard Chartered Titanium Credit Card

7) MANHATTAN Platinum Credit Card

8) MANHATTAN Titanium Credit Card

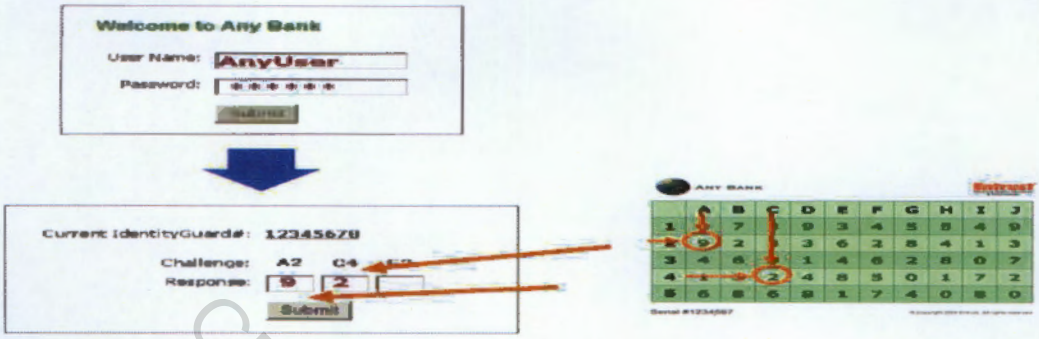
9) MANHATTAN id Platinum Credit Card

10) MANHATTAN id Credit Card

Source : Site de la SCB (2012)

ANNEXE 13 : FIGURES DES MODES DU PROCESSUS D'AUTHENTIFICATION FORTE

Figure 10 : Processus d'authentification forte par carte matricielle

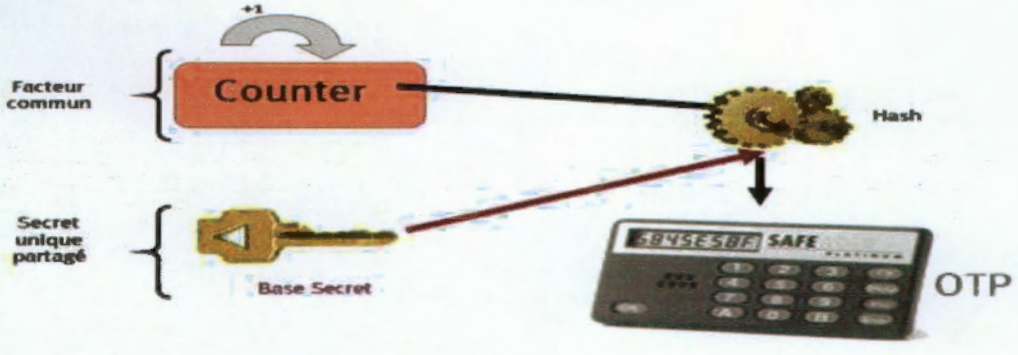


Source : MARET (2007 : 37)

Figure 11: Processus d'authentification forte par un token basé sur le temps

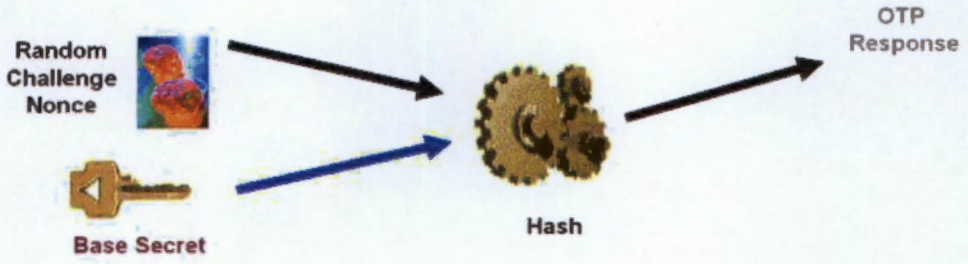
Source : MARET à partir de WIKIPEDIA (2012)

Figure 12 : Processus d'authentification forte basé sur un compteur



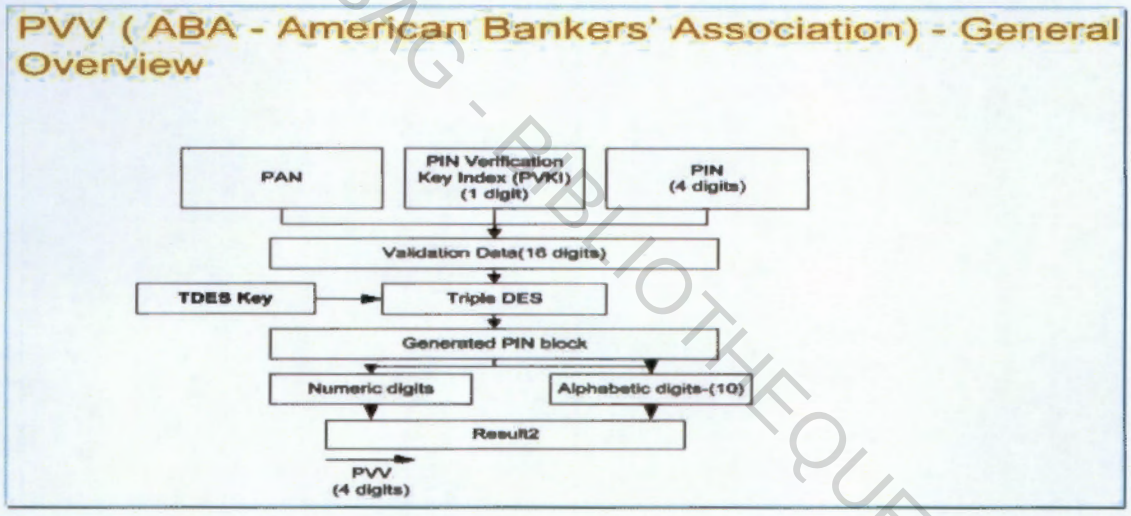
Source : MARET à partir de WIKIPEDIA (2012)

Figure 13 : Processus d'authentification forte par token basé sur un mécanisme de challenge/réponse



Souce : MARET à partir de WIKIPEDIA (2012)

ANNEXE 14 : PROCESSUS DE TRANSPORT DU CODE CONFIDENTIEL



Source : American Banker's Association (2010 : 53)

BIBLIOGRAPHIE

1) ALBARELLO (2004), Apprendre à chercher : l'acteur social et la recherche scientifique, Les Editions de Boeck, Belgique, 200 pages.
2) AMERICAN BAR ASSOCIATION (2008), Data security handbook, Section of Antitrust Law, ABA publishing, Etats Unis, 150 pages.
3) AMERICAN BAR ASSOCIATION (2010), ABA banking journal, Simmons-Boardman Pub. Co., Etats Unis, 98 pages.
4) AUTISSIER David, BOUDIER Fabienne, BENSEBAA Faouzi (2007), L'atlas du management : les meilleures pratiques et tendance pour actualiser vos compétences, Les Editions d'Organisation Eyrolles, France, 479 pages
5) AXELROD C. Warren, BAYUK L. Jennifer, SCHUTZER Daniel (2009), Enterprise Information Security and Privacy, Edition illustrée Artech House, U.S.A, 231 pages.
6) BERNET Luc-Rollande (2002), Principes de technique bancaire, 22è Edition Dunod, France, 432 pages.
7) BI TRA Doubi (2011), Banque, Finance & Bourse : Lexique des Termes Usuels, Les Editions Harmattan, France, 368 pages.
8) BOUTILLIER Sophie, D'ALLONDANS Alban Goguel, UZUNIDIS Dimitri (2005), Méthodologie de la thèse et du mémoire, Les Editions Studyrama, France, 239 pages.
9) BRADLEY Tony (2007), PCI Compliance : Implementing Effective PCI Data Security Standards, Edition illustrée Syngress, U.S.A, 352 pages.
10) CALDER Alan (2006), The Case for ISO 27001, Les Editions IT Governance publishing, Royaumes Unis, 120 pages.
11) CALDER Alan et CARTER Nicki (2008), PCIDSS : a pochet guide, Les Editions IT Governance publishing, Royaumes Unis, 42 pages.
12) CARPENTIER Jean-François (2009), La sécurité informatique dans la petite entreprise : Etat de l'art et bonnes pratiques, Editions ENI, France, 276 pages.
13) CENDROWSKI Harry, MAIR C. William (2009), Entreprise Risk Management and COSO : A Guide for Directors, Executives, and Practitioners, John Wiley & Sons, U.S.A, 335 pages.
14) CHAMP Clark (2007), InfoSecurity 2008 : Threat Analysis, Edition illustrée Syngress, U.S.A, 442 pages.

15) CHUVAKIN Anton, WILLIAMS R. Branden (2009), PCI Compliance : Understand and Implement Effective PCI Data Security Standard Compliance, Elsevier, Pays Bas, 380 pages.

16) COLOMBANI Pascal (2004), Fraudes à la carte bancaire, Les Editions Carnot, France, 185 pages.

17) DANCETTE Jeanne, WEGNEZ F. Léon, RETHORE Christophe (2000), Dictionnaire analytique de la distribution, Les Editions Presse Universitaire de Montréal, Canada, 347 pages.

18) DESMICHT François (2007), Pratique de l'activité bancaire, 2è Edition Dunod, France, 355 pages.

19) DRAGON Claude, GEIBEN Didier, NALLARD Gilbert (2002), La carte et ses atouts, Les Editions Revue Banque, France, 127 pages.

20) FERNANDEZ Alain (2010), Les nouveaux tableaux de bord des managers, Les Editions Eyrolles, France, 466 pages.

21) GAUFFRIAU Y. (1997), Gestion économique : modéliser, Les Editions Foucher, France, 192 pages.

22) GODART Didier (2002), Sécurité informatique : risques, stratégies et solutions, 2ème Editions EDIPRO, Belgique, 334 pages.

23) HARWOOD Mike (2010), Security Strategies in Web Applications and Social Networking, Jones & Bartlett Publishers, U.S.A, 406 pages.

24) HUET Franck, VERHILLE Christian (2007), GNU/Linux Fedora: Sécurité du système, sécurité des données, pare-feu, chiffrement, authentification, Les Editions ENI, France 342 pages.

25) KIM David et SOLOMON Adam (2010), Fundamentals of information systems security, Les Editions Jones and Bartlett Publishers, Etats Unis, 514 pages.

26) LESSARD-HERBERT et BOUTIN (1997), La recherche qualitative : fondement et pratique, Les Editions de Boeck, Belgique, 126 pages.

27) L'HEUREUX Nicole et LANGEVIN Louise (1991), Les cartes de paiement : aspects juridiques, Les Presses de l'Université Laval, France, 196 pages.

28) MADERS Henri-Pierre et MASSELIN Jean-Luc (2009), Piloter les risques d'un projet, Les Editions d'Organisation Groupe Eyrolles, France, 287 pages.

29) MELOUX Thierry (2008), Analyse 360° : pratique de l'analyse financière des entreprises, Les Editions Books on Demand, France, 156 pages.

30) MISHKIN Fréderic (2007), Monnaie, banque et marchés financiers, 8è éd. Pearson Education, France, 928 pages

31) OBSERVATOIRE DE LA SECURITE DES CARTES DE PAIEMENT (2008), Rapport annuel 2008 de l'observatoire de la sécurité des cartes de payement, Imprimerie Banque de France, France, 70 pages.

32) NOIRAULT Claire (2008 : 8), ITIL (version 3) : Les meilleures pratiques de gestion d'un service informatique, Les Editions ENI, France, 276 pages.

33) OBSERVATOIRE DE LA SECURITE DES CARTES DE PAIEMENT (2009), Rapport annuel 2009 de l'observatoire de la sécurité des cartes de payement, Imprimerie Banque de France, France, 78 pages.

34) OBSERVATOIRE DE LA SECURITE DES CARTES DE PAIEMENT (2010), Rapport annuel 2010 de l'observatoire de la sécurité des cartes de payement, Imprimerie Banque de France, France, 103 pages.

35) ORGANISATION POUR LA COOPERATION ECONOMIQUE ET LE DEVELOPPEMENT PERSONNEL (2000), Perspectives des technologies de l'information 2000 : TIC, Commerce électronique et Economie de l'information, OECD Publishing, France, 284 pages.

36) PCI SSC (2010), PCI (Payment Card Industry) Data Security Standard : Conditions et procédures d'évaluation de sécurité Version 2.0, PCI SSC, Etats Unis, 86 pages.

37) PCI SSC (Octobre 2008), Payment Card Industry (PCI) Data Security Standard Navigation dans les normes PCI DSS : Comprendre l'objectif des exigences, PCISSC Etats Unis, 60 pages.

38) PLAUCHU Vincent et TAÎROU Akim (2008), Méthodologie du diagnostic d'entreprise, Les Editions Harmattan, France, 300 pages

39) RAO H.Raghav, GUPTA Manish, UPADHYAYA Shambhu J. (2007), Managing Information Assurance in Financial Services, Idea Group Inc (IGI), Etats Unis, 331 Pages.

40) RENARD Jacques (2010), Théorie et pratique de l'audit interne, 7è Edition Eyrolles, France, 469 pages.

41) ROUNTREE Derrick (2010), Security for Microsoft Windows System Administrators : Introduction to Key Information Security Concepts, Edition Elsevier, Pays Bas, 216 pages

42) SHERIF Mostafa Hashem et SERHROUCHNI Ahmed (2000), La monnaie électronique système de paiement sécurisé, Eyrolles, France, 513 pages.

43) SHERIF Mostafa Hashem (2007), Paiements électroniques sécurisés, Les Editions PPUR Presses polytechniques, Suisse, 582 pages.

44) THOMAS M. Thomas II, THOMAS M. Thomas, STODDARD Donald (2011), Network security first step, Les Editions Cisco press, Etats Unis, 423 pages.

45) UNITED NATIONS (30 juin 2010), Etat de l'intégration régionale en Afrique IV: Développer le commerce intra-africain, United Nations Publications, Etats Unis, 563 pages.

46) VIRTUE M. Timothy (2008), Payment Card Industry Data Security Standard Handbook, John Wiley & Sons, U.S.A, 216 pages.

47) VON SOLMS S.H, VON SOLMS Rossouw (2008), Information Security Governance, Les Editions Springer, Afrique du sud, 138 pages.

48) WEISS Martin, SOLOMON G. Michael (2010), Auditing It Infrastructures for Compliance, Jones & Bartlett Publishers, U.S.A, 384 pages.

49) WRIGHT Steve (2011), PCI DSS : A practical guide to implementing and maintaining compliance, IT Governance publishing, Royaumes Unis, 253 pages.

WEBOGRAPHIE

1) Banque des Etats de l'Afrique Centrale (2003), Réforme des systèmes et moyens de paiement de la CEMAC, http://www.beac.int/index.php?option=com_content&view=article&id=168:projet-de-reforme-des-systemes-de-paiement-et-de-reglement&catid=50:systemes-de-paiement&Itemid=61.

2) Banque Centrale des Etats de l'Afrique de l'Ouest (09/07/2008), règlement N°15/2002/CM/UEMOA relatif aux systèmes de payement dans les Etats membre de l'UEMOA, http://www.bceao.int/internet/bcrsmp.nsf/zaffiche/e43d688aba773f1e00257481006c1da5.

3) GIM UEMOA (2012), les cartes, http://www.gim-uemoa.org/page_std.php?id=83.

4) Google images (2012), composition d'une carte bancaire, http://www.google.fr/imgres?q=carte+bancaire&um=1&hl=fr&sa=N&biw=1366&bih=651&tbm=isch&tbnid=627WxQ3MBo036M:&imgrefurl=http://cerig.efpg.inpg.fr/memoire/2010/carte-

bancaire.htm&docid=9CfA3lZY27a4FM&imgurl=http://cerig.efpg.inpg.fr/memoire/2010/images/carte-bancaire-composant.jpg&w=405&h=422&ei=MineT-7ZFYPMhAfZjcGGCg&zoom=1&iact=hc&vpx=171&vpy=305&dur=2023&hovh=229&hovw=220&tx=113&ty=82&sig=111803716096597354343&page=1&tbnh=131&tbnw=126&start=0&ndsp=21&ved=1t:429,r:7,s:0,i:159

5) KHELED Allab (2007), Sécurité des transactions dans le cadre de l'intégration maghrébine, http://www.google.fr/url?sa=t&rct=j&q=5)%09KHELED+Allab+(2007)%2C+S%C3%A9curit%C3%A9+des+transactions+dans+le+cadre+de+l%E2%80%99int%C3%A9gration+maghr%C3%A9bine&source=web&cd=1&ved=0CFMQFjAA&url=http%3A%2F%2Fwww.ubm.org.tn%2Fupload%2Fpdf%2Fs1%2FPresentation_Gemalto_UBM.pdf&ei=3VPeT_yrDYiHhQe1iPiwCg&usg=AFQjCNGHOYjfHpsq5eebjLAyDPuf3wvCtA.

6) MARET Sylvain (2007), Tutorial, Authentification forte, Technologie des identités http://www.google.fr/url?sa=t&rct=j&q=authentification+forte%2C+sylvain+maret%2C+pdf&source=web&cd=8&ved=0CHIQFjAH&url=http%3A%2F%2Fwww.rezonance.ch%2Ffs-search%2Fdownload%2FAuthentification-Forte-1.pdf%3Fversion_id%3D1805857&ei=jk7eT635A4-GhQeyoMCkCg&usg=AFQjCNG9W_H3oK04lrAMYbH0EmgHhaUuzQ

7) OMAC (2012), nos produits, http://www.omac-afr.org/pages/produits-et-services.php.

8) PCI SCC (2012), Glassary V2.0, https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_glossary#pci_dss_glossary

9) Standard Chartered bank (2012), personal banking : cards, http://www.standardchartered.com.hk/per.

10) WIKIPEDIA (2012), Authentification forte, http://fr.wikipedia.org/wiki/Authentification_forte.