



# *Comment se conformer à la norme PCI DSS V3.0*

## *Démarche et Méthodologie*

**Du 29 Septembre au 1er Octobre 2014  
Hôtel NOVOTEL Mohamed V - Tunis**

## **Introduction**

La formation sur l'implémentation de la norme PCI DSS est conçu pour les professionnels des cartes de paiements et des systèmes d'informations qui ont la responsabilité de gérer et de mettre en œuvre tous les aspects des contrôles de la conformité PCI au sein de leurs organisations.

La formation porte sur la norme PCI DSS en terme de sa mise en œuvre, mais aborde également les lignes directrices des normes PA DSS, et PTS ainsi que d'autres pratiques telles que les bonnes pratiques concernant les Guichets Automatiques Bancaires.

Les participants à ce cours trouveront de nombreuses réponses qui les aideront à résoudre certaines problématiques exigées et seront dotés d'orientations claires et pratiques leur permettant d'économiser des efforts, du temps et de l'argent.

Cette formation s'adresse donc à l'ensemble des entités qui traitent, stockent ou transportent des données « Cartes » soit les banques, acquéreurs, émetteurs, commerçants, sociétés informatiques.

Le second volet de cette formation inclut la présentation d'un outil et d'une démarche afin de mesurer l'écart par rapport aux exigences et de gérer le projet de mise en conformité.

## **Pourquoi participer à cette formation**

Une occasion unique de comprendre l'ensemble des éléments à prendre en compte au cours de l'analyse des écarts de conformité, des améliorations à apporter et des points déterminants de validation, grâce à un consultant certifié QSA (Qualified Security Auditor) ayant plus de 20 ans d'expérience dans la monétique.

L'approche n'est pas uniquement théorique mais interactive et permet d'approcher la réalité de la fraude et des moyens de protection au travers de démonstrations pratiques et de conseils sur l'applicabilité et l'importance des contrôles résultant des normes PCI DSS.

Partager les expériences des autres organisations et leurs progrès dans le cheminement de la conformité et acquérir de précieuses connaissances à travers des échanges d'information avec vos pairs est aussi un objectif de cette formation

## **Cadre de cette formation**

La formation sera dispensée en français. Toutefois la version 3 de la norme n'existant pas en langue française la seconde journée de cours sera prodiguée dans les deux langues.

La formation est réalisée sous un format interactif permettant à chaque intervenant de poser des questions.

La formation inclut des exercices permettant au formateur de s'assurer de la bonne compréhension des sujets abordés.

Chaque participant se verra remettre un support de cours et un certificat de participation à la formation PCI DSS.

## **Public visé**

Cette formation s'adresse à l'ensemble des entités qui traitent, stockent ou transportent des données « Cartes » soit les banques, acquéreurs, émetteurs, commerçants, sociétés informatiques.

## **Formateur**

Mr Charles Delbrassine, QSA et expert belge de la société ITWORKS ayant plus de 20 ans d'expérience dans la monétique. Voir <http://www.linkedin.com/in/delbrassinecharles>

## **Contenu de la formation**

### **Programme de la journée 1 (de 09:00 à 17:00) « Introduction PCI »**

- Introduction aux acteurs de la monétique.
- Vue d'ensemble de la fraude monétique.
- Présentation du « council » PCI.
  - Origines
  - Organisation
  - Domaines de responsabilité
- Présentation des normes éditées par le council.
  - PCI DSS
  - PCI PA DSS
  - PCI P2P
  - PCI PTS
  - Autres publications
- Relation avec le standard EMV.
- Relation avec le standard ISO27001.
- Présentation des exigences de conformité.
  - PCI DSS Scan
  - Self Assessment Questionnaire (SAQ)
  - Report of Compliance (ROC)
- Présentation des programmes de preuve de conformité et rôles des auditeurs certifiés (QSA, ASV).
- Cycle d'évolution des standards.

### **Programme de la journée 2 (de 09:00 à 17:00) « Présentation du standard PCI DSS V3.0 »**

- Mise en place et maintenance d'un réseau sécurisé
  - Exigence 1: Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de cartes

- Exigence 2: Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
- Protection des données de titulaire de carte
  - Exigence 3: Protéger les données de titulaire de carte stockées
  - Exigence 4: Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts
- Maintenance d'un programme de gestion 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 aux données de titulaire de carte aux seuls individus qui doivent les connaître
  - Exigence 8: Attribuer un ID unique à chaque utilisateur d'ordinateur
  - Exigence 9: Restreindre l'accès physique aux données de titulaire de carte
- Surveillance et test 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: Respecter les lignes directrices concernant la sécurité de l'information pour les employés et sous-traitants
- Introduction aux contrôles compensatoires.

### **Programme de la journée 3 (de 09:00 à 17:00) « Implémenter et maintenir la conformité »**

- Présentation d'une démarche type
- Analyse d'écart.
- Réalisation de fiches « NCR » (Non Conformity Report)
- Réalisation des diagrammes de flux
- Réalisation des diagrammes réseaux
- Présentation d'outils et solutions permettant d'atteindre et maintenir la conformité
- Présentation de l'outil de suivi de la conformité PCI DSS
- Relevé des éléments posant habituellement des problèmes et solutions potentielles.
- Question / Réponses.

# Demande d'inscription

## à la formation *Comment se conformer à la norme PCI DSS V3.0* *Démarche et Méthodologie*

du 29/09 au 1<sup>er</sup>/10 2014

Inscrivez-vous dès maintenant en complétant ce bulletin d'inscription – L'envoyer  
Par Fax + 216 71 89 23 48 ou Par mail : [contact@bit.tn](mailto:contact@bit.tn)

M./ Mme	Prénom Nom	Fonction	E-mail / GSM

Entreprise :

Adresse :

Code postal :

Ville :

Téléphone :

Fax :

Email :

Site Web :

Les frais d'inscription sont à **2000 DT\* (1000 Euros)** HT par personne

**NB : Les places sont limitées**

### **\*Conditions Générales d'inscription**

Votre inscription sera définitive après réception de ce formulaire dûment rempli. Elle sera prise en compte dans la limite des places disponibles.

#### **10% de remise si inscription 3 semaines avant la formation**

Pour discuter d'une offre de groupe ou pour plus d'amples détails sur la formation, merci de nous consulter par:

Email : [contact@bit.tn](mailto:contact@bit.tn)

Phone # : +216 71 892 348 / 71 892 352 / 94 70 77 37

**Lieu de formation :** Hôtel NOVOTEL à Mohamed V - Tunis

#### **Etrangers intéressés par la formation :**

- Nous pouvons vous conseiller pour votre hébergement. Merci de nous contacter.
- Le paiement des frais de participation se fait au plus tard une semaine avant le démarrage de la session par virement bancaire.

#### **Calcul des coûts:**

Le prix inclus :

- La participation à la formation.
- Les supports de cours
- Pausas café et déjeuner

#### **Mode de paiement :**

- Par chèque au nom de Business and Information Technology
- Par virement bancaire au compte :
  - RIB : 010901251107003039-49
  - IBAN : TN59 010901251107003039-49

Cette Formation est éligible à la ristourne de la TFP. Numéro d'enregistrement MFPE : 11116912

#### **Annulation de session:**

Nous nous réservons le droit d'annuler une session lorsque le nombre de participants est insuffisant.

#### **Annulation d'inscription:**

Tout désistement devra nous être notifié au moins une semaine avant le début de la session (annulation avec remboursement sans frais). Au-delà de ce délai, le montant prévu pour la session vous sera intégralement facturé.