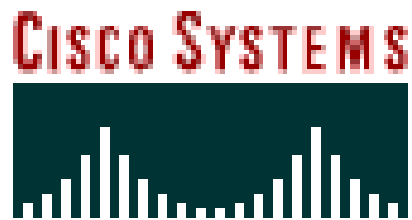


Welcome To

PCI Compliance: Debunking the Myths



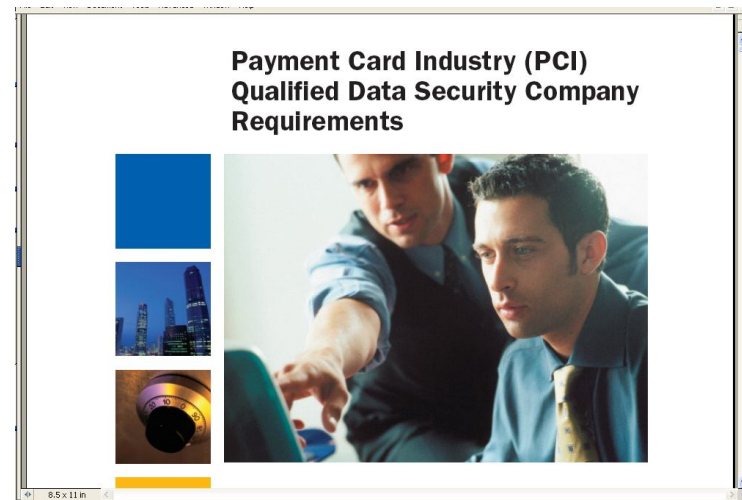
Introducing Your Sponsors



DRG PCI Expertise

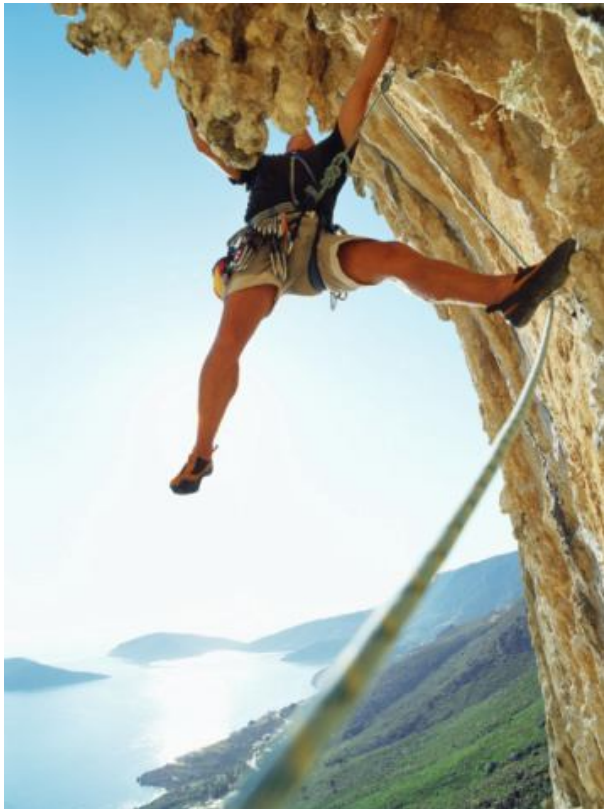
- ❖ Qualified Security Assessor (QSA)
- ❖ Qualified Payment Applications Security Company (QPASC)
- ❖ Approved Scan Vendor (ASV)

DRG performs PCI assessments and application reviews for industry-leading companies



Data Security Compliance

Are We There Yet?



January 2008, Visa Reports:
99% of Merchants (level 1 & 2)
attested to not storing
“Prohibited Data”

- ❖ Level 1: 77% compliant
- ❖ Level 2: 62% compliant
- ❖ Level 3: 54% compliant

New version 1.1 SAQs

- ❖ Four versions address various business scenarios

SAQ A

Merchants with all outsourced cardholder data storage, processing and transmission.

SAQ B

Merchants who process cardholder data via imprint machines or standalone dial-up terminals only.

SAQ C


Merchants whose payment applications systems are connected to other systems internally or on the Internet.

SAQ D

Merchants who do not fall under the types addressed by SAQ A, B or C, and all service providers defined by a payment brand as eligible to complete an SAQ.

Current SAQ will sunset on April 30, 2008

Confirmation of Report Accuracy



Attestation of Compliance, SAQ A

Instructions for Submission
 The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

Part 1. Qualified Security Assessor Company Information (if applicable)

Company Name:	<input type="text"/>
Lead QSA Contact Name:	<input type="text"/>
Title:	<input type="text"/>

Requires
Executive
Sign Off



Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	Date ↑
<input type="text"/>	<input type="text"/>
Merchant Executive Officer Name ↑	Title ↑
<input type="text"/>	<input type="text"/>
Merchant Company Represented ↑	
<input type="text"/>	

PCI DSS SAQ A, v1.1, Attestation of Compliance
 Copyright 2008 PCI Security Standards Council LLC

February 2008
 Page 2

Requirement 6.6

- ❖ Protect *all* web-facing applications against known attacks

Custom application code review

- or -

Application layer firewall



Payment Application - DSS

PA-DSS Version 1.1 announced April 15, 2008

- ❖ Council will qualify companies to become Payment Application Qualified Security Assessors (PA-QSAs)
- ❖ Fall 2008: Council will roll out list of validated payment applications

Compliant app does not ensure
PCI DSS Compliance



Introducing Hans Van Tilburg



- ❖ Director Payment System Risk
- ❖ Leading service provider ROC reviews
- ❖ Extensive security and cryptographic expertise

Questions



Contact Information



James Cowing, CISSP, QSA, CISM, CPA, CITP

Managing Director, Digital Resources Group

Email: jim.cowing@drgsf.com

Web: www.drgsf.com

Phone: 650-638-3350



Hans Van Tilburg, Ph.D., CISSP

Director Payment System Risk, Visa Inc.

Email: hvantilb@visa.com

Web: www.visa.com

Phone: 650-432-3512