

# PCI DSS – Achieving and Maintaining Compliance

---

## INTRODUCTION AND RECAP



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire



# Overview



What the journey looks like

The key terms

You can be a PCIP

Core PCI DSS concepts (revision)



# Your Authors



# The Compliance Journey

**Prepare**

**Understand Scope**

**Scope Reduction**

**Remediate**

**Assessment**

**BAU Maintenance**





# PCI DSS: The Big Picture

★★★★★ By John Elliott

The Payment Card Industry (PCI) Data Security Standard (DSS) affects every organization that stores, processes, or transmits credit or debit cards. In this course, you'll learn about the standard and how it is used in card scheme compliance programs.

This course really is a prerequisite

Course Overview



Course Overview

2m

Introduction



🔒 What Is PCI DSS?

8m

🔒 What Is Compliance?

5m

Inside the Standard



What Is PCI DSS  
Compliance?



Ten PCI DSS Common  
Myths



# Participants



The Entity (you): Merchant, Service Provider, Financial Services Company



Card Brands: American Express, Discover, JCB, Mastercard, Visa



Payment Card Industry (PCI) Security Standards Council (SSC)



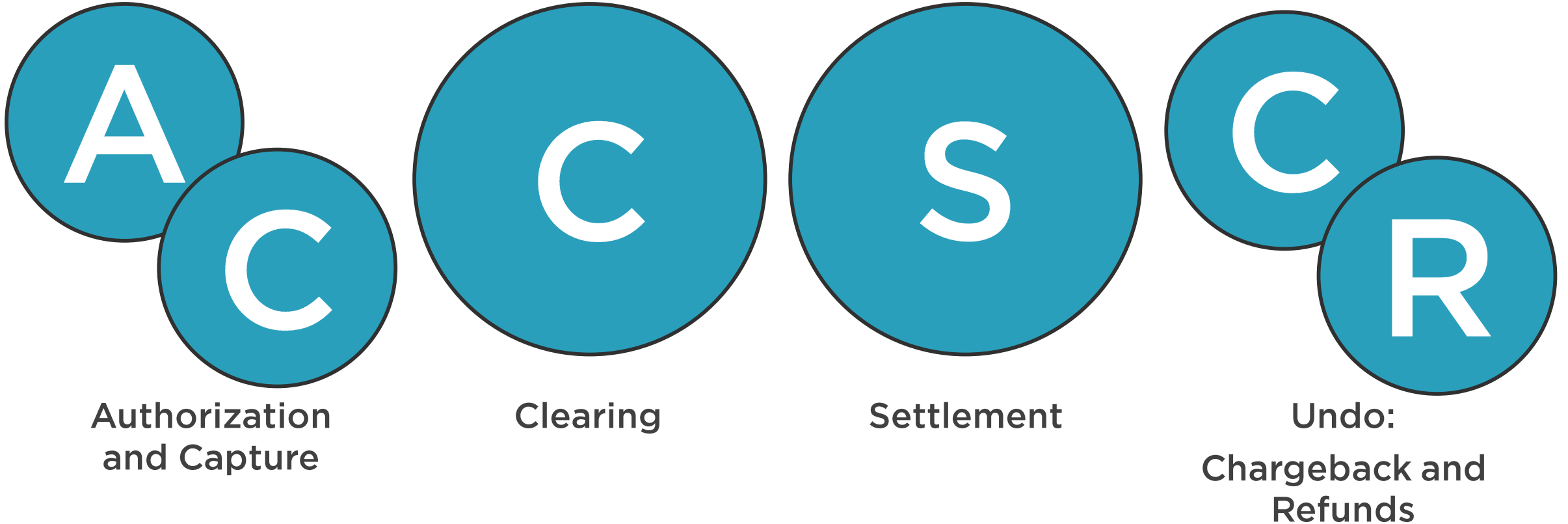
Acquirers & Issuers



Service Providers (third parties)



# Card Processing



# PCI Roles (Qualifications)



**Qualified Security  
Assessor (QSA)**



**Internal Security  
Assessor (ISA)**



**PCI Professional  
(PCIP)**





# PCI Professional



**Cements your knowledge**

**Get a direct relationship with the PCI SSC**

- Newsletters
- Community meeting

**Recognized qualification**

**Easier to work with QSAs and ISAs**

**Something to show for this ....**



# How to Become a PCI Professional

---





Payment Card Industry (PCI)  
**Qualification Requirements**

---

**For Payment Card Industry  
Professionals (PCIP)™**  
Version 2.0  
July 2014

**Qualification requirements**  
**Application form**  
**Code of professional conduct**

[https://www.pcisecuritystandards.org/documents/pcip\\_qualification\\_requirements\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pcip_qualification_requirements_v2.pdf)





**Qualification is yours**

- Not tied to the organization

**Valid for three years**



# Candidates Must Possess a Base Level of Knowledge and Awareness of ...



Information Technology



Network Security



Network Architecture



Payment Industry Participants



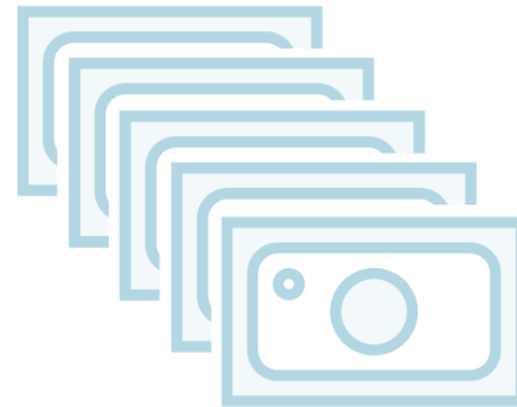
# PCI Application



Web application  
form



Resume /  
Curriculum  
Vitae



Fee



Training?





Pay by fax, telephone  
or bank transfer



Schedule your exam  
at a testing center







Multiple choice

A case study



# PCI Security Standards Council, LLC

acknowledges that

**John Elliott**

has successfully fulfilled the requirements for

---

**Payment Card Industry Professional (PCIP)<sup>™</sup>**

---

as defined in the Payment Card Industry (PCI) Qualification Requirements  
for Payment Card Industry Professionals (PCIP)<sup>™</sup>.

Certificate Number: 1000-267

Expiration Date: 14 December 2021



A handwritten signature in black ink, appearing to read "Lance J. Johnson".

---

Lance J. Johnson,  
Executive Director, PCI SSC





**Valid for three years**

**Fee payable for re-certification**

**Continuing Professional Education (CPE)**

- 10 hours per year
- 30 hours in three years

**Requalification exam**



# A Quick Recap of the Standard

---



# Quick Look at All Twelve



**Payment Card Industry (PCI)  
Data Security Standard**

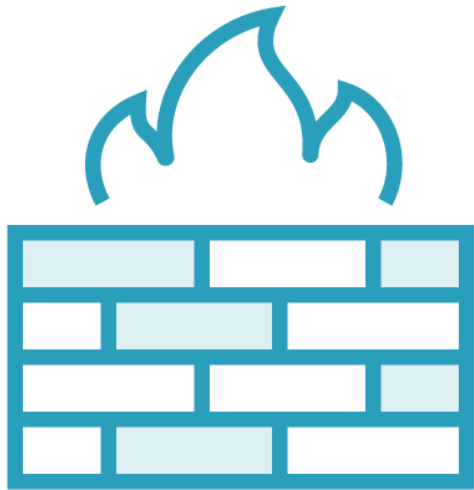
**Requirements and Security Assessment Procedures**

**Version 3.2**  
April 2016

1. Have firewalls
2. No defaults
3. Protect stored data
4. Encrypt transmissions
5. Use anti-virus
6. Secure apps and OSES
7. Restrict access
8. Identify and authenticate
9. Physical protection
10. Log and monitor
11. Test security
12. Have policies



# 1. Install and Maintain a Firewall Configuration to Protect Cardholder Data



**Have configuration standards for firewalls**

**Build and configure firewalls properly**

**Make all traffic go through a firewall (ie not a direct connection to the internet)**

**Put personal firewalls on devices**

**Have written policies for this**

## 2. Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters



admin

**Change default credentials**

**Have secure (hardened) builds that only enable what's needed**

**Encrypt non-console access**

**Keep an inventory**

**Have policies for this**

### 3. Protect Stored Cardholder Data



**Retain only minimal cardholder data**

**Don't store plaintext cardholder data**

**Never store track data, CVV2 or PINs**

**Do encryption properly**





## 4. Encrypt Transmission of Cardholder Data Across Open, Public Networks



Accept and send cardholder data using strong cryptography

Move away from SSL and TLS 1.0

Don't send cardholder data via email, IM, and other messaging channels

Have policies for all of this

## 5. Protect All Systems Against Malware and Regularly Update Anti-virus Software or Programs



**Have operational anti-virus software  
(please use anti-malware)**

**Keep the AV logs**

**Don't let people disable AV**

**Have policies for all of this**

## 6. Develop and Maintain Secure Systems and Applications



Track published vulnerabilities for all your software: applications and OS

Patch regularly

Have a secure SDLC

Have proper change control

Test the security of web-facing apps or use a Web Application Firewall

Have policies for all of this

## 7. Restrict Access to Cardholder Data by Business Need to Know



Only give people access to systems and cardholder data when they really need it

Use an access control system  
(eg AD, LDAP)

Have policies for all of this

## 8. Identify and Authenticate Access to System Components



**Manage unique user IDs**

**Have strong(ish) passwords**

**Use MFA for admin and all remote access**

**Don't allow direct query access to databases containing cardholder data**

**Have policies for all of this**

## 9. Restrict Physical Access to Cardholder Data



**Control and log physical access to the CDE**

**Secure physical media (paper and electronic) containing cardholder data.  
Dispose of media securely**

**Protect card-reading devices (e.g. chip and PIN / EMV readers)**

**Have policies for all of this**

## 10. Track and Monitor All Access to Network Resources and Cardholder Data



- Create audit logs, retain them for a year
- Secure the logs against tampering
- Make sure everything is time synchronized
- Review logs daily :-o
- Have polices for all of this

# 11. Regularly Test Security Systems and Processes



**Check for rogue wireless access points**

**Do internal and external vulnerability scans**

**Do internal and external penetration tests**

**Have IDS and/or IPS**

**Use change detection software (FIM)**

**Have policies for all of this**



## 12. Maintain a Policy That Addresses Information Security for All Personnel



**Have an information security policy**

**Do risk assessments**

**Assign key security tasks to individuals**

**Have a security awareness program**

**Screen employees**

**Manage third party service providers**

**Have & practice an incident response plan**

# Next: What Is Compliance?

---

