

Approach to **A**ttain, **M**aintain and **R**etain **PCI DSS and PA DSS**

Presenter – Erik Winkler, SVP – ControlCase



Agenda

- History of PCI DSS
- Evolution of Standard
- Advantages
- Challenges
- Solutions
- PCI DSS v3.1 and PA DSS
- Takeway

Acronyms

- Payment Card Industry (PCI) Data Security Standard (DSS) is family of data security standards
- PCI as a term is generally never used alone. The key standard in PCI is PCI Data Security Standard, or PCI DSS.
- Payment Card Industry (PCI) Security Standard Council (SSC)

PCI DSS – Historical Perspective

- Different Card Brands (Visa, MasterCard, Amex, Discover, JCB)
- Different Compliance Requirements
- Year 2006 – Formation PCI SSC



Evolution of Standard

- Encourage and enhance cardholder data security
- Adoption of consistent data security standard globally
- Current Standard Version is 3.1
- Considers market implementation of standard
- To protect service providers and merchants



What is PCI DSS Standard

- ❑ Data Security Standard adopted by major card processing networks (Visa, MasterCard, etc.) to combat fraud and promote secure processing of payment card transactions
- ❑ Unified standard for security associated with card data storage, transmission, and processing
- ❑ PCI DSS Compliance is recommended / mandatory as per the organizations levels that deals with card data.

PCI Family of Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users



Applicability

Systems which **STORE**, **PROCESS**, **TRANSMIT** Cardholder Data



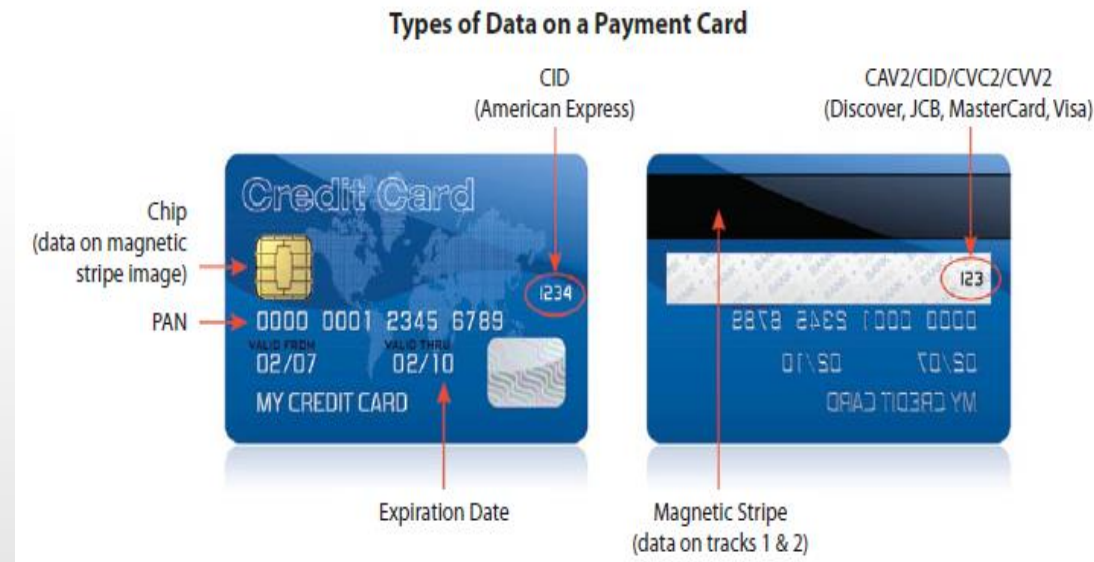
Advantages

- Assurance that payment system is protected
- Possibly Avoid/Reduce penalties in case of fraud
- Increases the confidence of users for their data
- Helps meet regulatory compliance requirements
- Improves overall Information Security Posture
- Makes aware employees about protecting data



Data in Question (Credit & Debit Card)

- Cardholder number (Called PAN)
- Cardholder Name
- Expiration Date
- Service Code
- CVV/CVV2/CVC2
- Track Data
- PIN



PCI Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors

Challenges

Firewall,
IDS/IPS,
NTP

Antivirus,
FIM

SDLC, Code
Review

Identity
Control,
Training

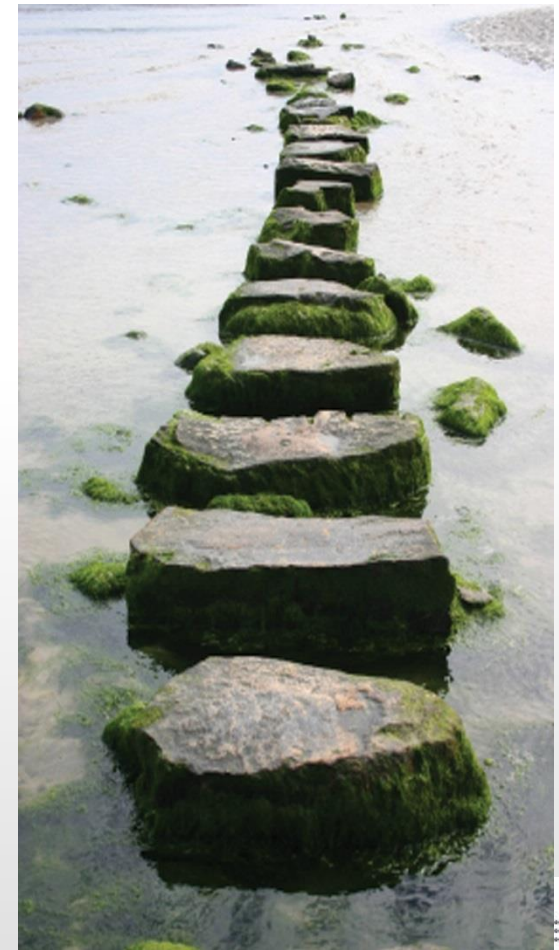
Creating
Policies &
Procedures

Scoping,
Service
providers

Centralized
Logging
Monitoring

Roadmap to PCI DSS

- Engage Qualified Security Assessor (QSA)
- Scoping (Card data discovery)
- Gap Assessment (Preparation)
- Remediation
- Certification Audit (Validation)
- Maintain PCI DSS Certification
- Recertification



Compliance as a Service

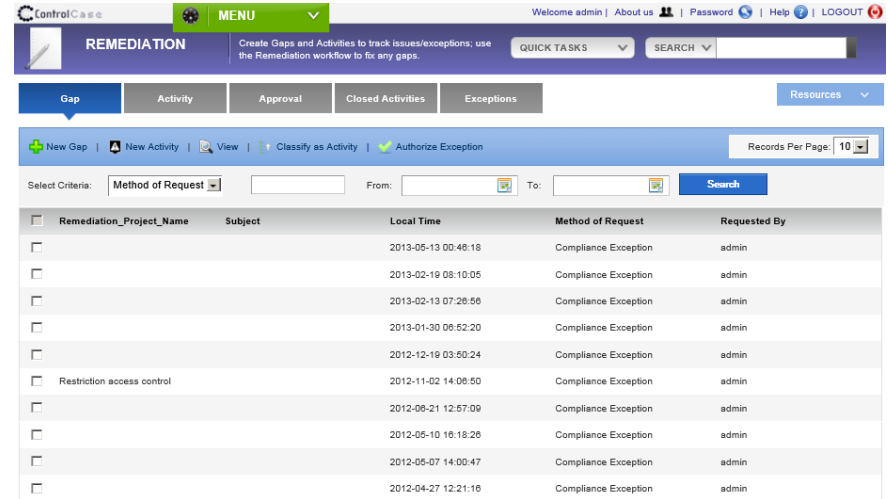
Gap Assessment

- Identify assets which store, process, transmit account data
- Perform Card Data Discovery
- Define the scope
- Assessment by Qualified Security Assessor (QSA)
- Identify what is affected
- Identify what are the big issues



Remediation

- Implement changes
- Implementation queries
- Identify solutions/products
- Contain cost
- Purchase Solutions
- Take expert advise from experienced QSA partner
- Ask question “Am I ready for Final Audit?”



The screenshot displays the ControlCase Remediation interface. The header includes the ControlCase logo, a MENU dropdown, and user information (Welcome admin | About us | Password | Help | LOGOUT). The main navigation bar features tabs for Gap, Activity, Approval, Closed Activities, and Exceptions, with a Resources dropdown. Below the navigation, there are buttons for New Gap, New Activity, View, Classify as Activity, and Authorize Exception, along with a Records Per Page selector set to 10. A search bar is present with a dropdown for 'Method of Request' and fields for 'From' and 'To'. The main content area is a table with the following columns: Remediation_Project_Name, Subject, Local Time, Method of Request, and Requested By. The table contains 10 rows of data, all with 'Compliance Exception' as the Method of Request and 'admin' as the Requested By.

Remediation_Project_Name	Subject	Local Time	Method of Request	Requested By
<input type="checkbox"/>		2013-05-13 00:46:18	Compliance Exception	admin
<input type="checkbox"/>		2013-02-19 08:10:05	Compliance Exception	admin
<input type="checkbox"/>		2013-02-13 07:26:56	Compliance Exception	admin
<input type="checkbox"/>		2013-01-30 08:52:20	Compliance Exception	admin
<input type="checkbox"/>		2012-12-19 03:50:24	Compliance Exception	admin
<input type="checkbox"/>	Restriction access control	2012-11-02 14:08:50	Compliance Exception	admin
<input type="checkbox"/>		2012-08-21 12:57:09	Compliance Exception	admin
<input type="checkbox"/>		2012-05-10 16:18:26	Compliance Exception	admin
<input type="checkbox"/>		2012-05-07 14:00:47	Compliance Exception	admin
<input type="checkbox"/>		2012-04-27 12:21:16	Compliance Exception	admin

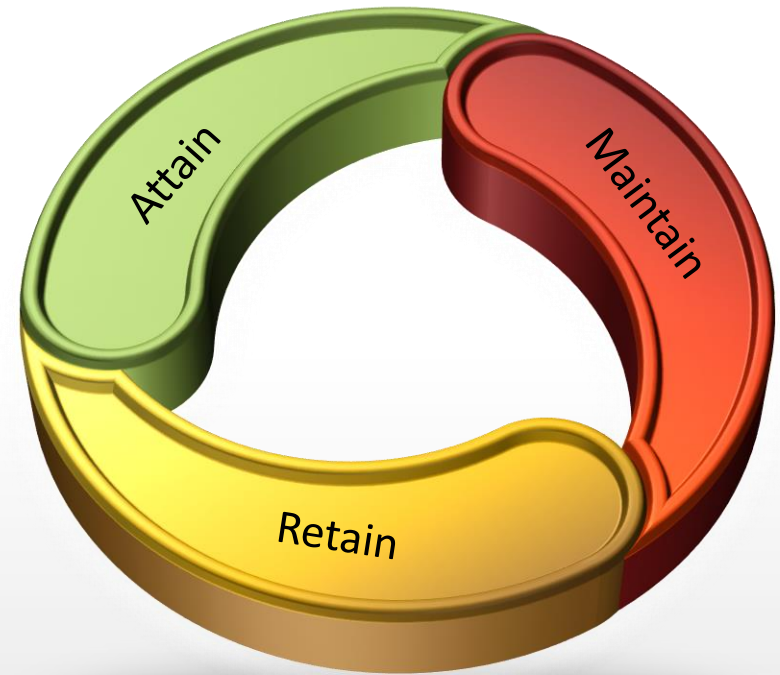
Certification Audit (Validation)

- Demonstrate Compliance
- Provide necessary evidences to QSA
- Justify compensating controls
- Achieve certification



Continual Compliance

- Maintain your certification to achieve recertification
- Follow procedures set by PCI DSS
- Perform periodic activities
- Retain PCI DSS certification



A faint, dotted world map is visible in the background of the slide. In the bottom right corner, there is a logo consisting of a circle of grey dots of varying sizes, with the text 'Control Case' and 'Compliance as a Service' below it.

PCI DSS v3.0 – v3.1 Highlights

Quick Glance - “0” to “12”

Req. #	Topic
Scoping	Web redirection server in scope
1.1.3	Separated network diagram and data flow diagram requirements
2.4	Maintain an inventory of system components
5.1.2	Evaluate evolving malware threats for systems not commonly affected by malware
8	Re-organized to provide a more holistic approach to authentication
9.3	Physical access to sensitive areas must be authorized and terminated when no longer needed
12.2	Risk assessments after significant changes to the environment
12.8	Information about responsibility for PCI DSS requirements

Req. which are best practices until June 30, 2015

Req. #	Topic
6.5.10	Broken authentication and session management
8.5.1	Service providers to use a unique authentication credential for each customer
9.9	Protect POS terminals and devices from tampering or modification
11.3	Develop and implement a methodology for penetration testing
12.9	For service providers – acknowledgement of responsibility

Highlights of PCI DSS 3.1

- Removed SSL as an example of a secure technology. Added note that SSL and early TLS are no longer considered to be strong cryptography and cannot be used as a security control after June 30, 2016.
- Req 11.2 - vulnerability scan could be a combination of automated and manual tools, techniques, or other methods.

Highlights of PCI DSS 3.1

- Changed reference from “protecting cardholder data” to “protecting account data”.
- Clarified that PCI DSS applies to any entity that stores, processes or transmits account data.
- Changed reference from “financial institutions” to “acquirers, issuers”.
- Clarified that validation processes for service providers include undergoing their own annual assessments or undergoing multiple on demand assessments.
- Clarified in requirements that storage of sensitive authentication data is not permitted “after authorization”.
- additional controls are required if hashed and truncated versions of the same PAN are present in an environment.



PA DSS Introduction

PA DSS Scope

- PA DSS applies to software development organizations who develop payment applications that store, process or transmit cardholder data as part of authorization or settlement.

Applicability of PA DSS

- Applies to payment applications that are sold ‘off the shelf’ without much customization
- Does not applies to:
 - › Payment applications offered as a service i.e. customers would not be having ability to manage, install or control the application
 - › Payment Applications developed for and sold to single customer for sole use i.e. ‘Bespoke’ application
 - › Payment applications developed by merchants or service provider for their own usage i.e. in-house applications.

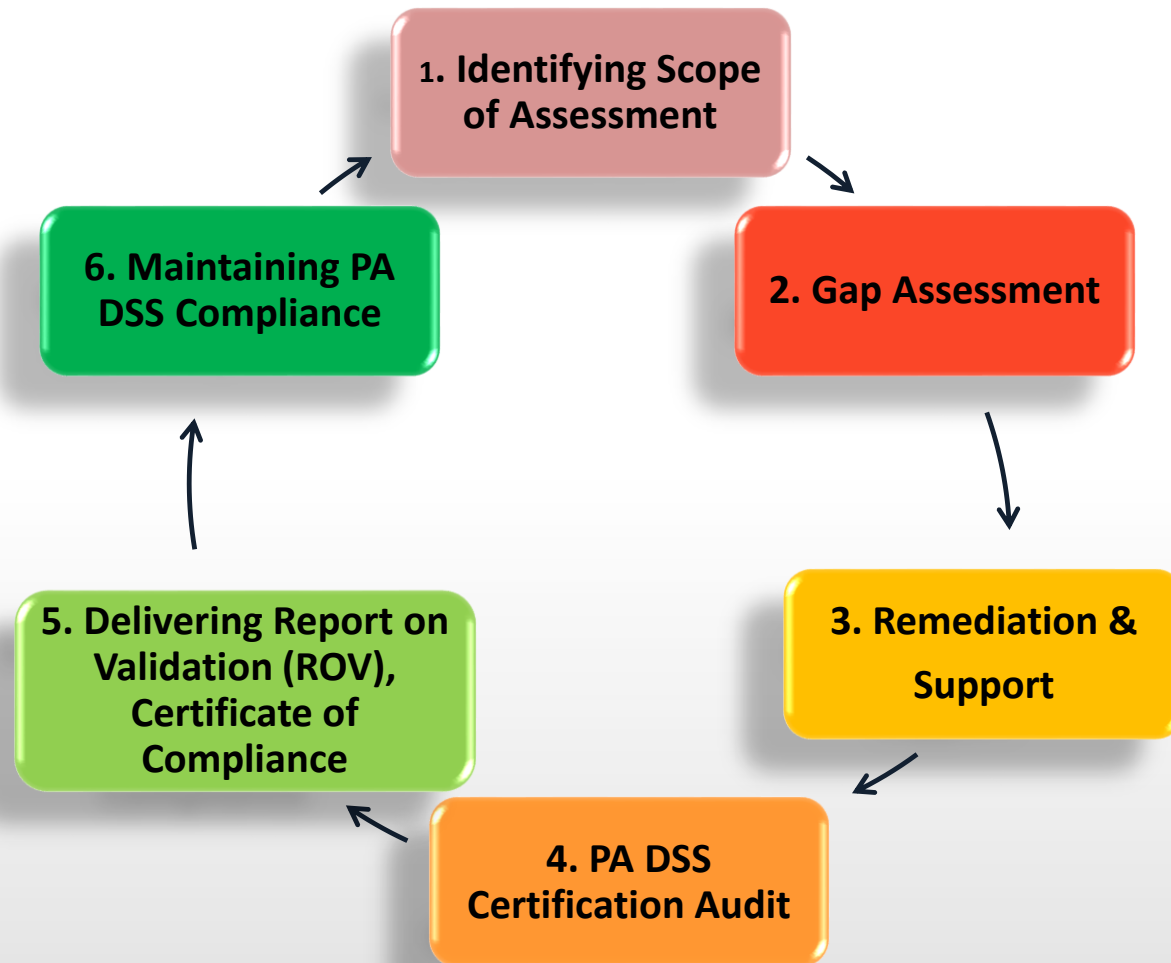
Exempted from PA DSS

- Operating Systems
- Database systems
- Back Office Systems

Responsibilities

- Payment Brands: Responsible for developing and enforcing PA DSS compliance programs
- PCI SSC:
 - › Central repository for PA DSS RoV
 - › Perform QA for PA DSS review reports
 - › List PA DSS validated application on the website
 - › Qualifies and train PA QSAs
 - › Maintain and update PA DSS
- Software Vendors:
 - › Develop Secure applications as per PA DSS guidelines
 - › Prepare PA DSS implementation guide

PA DSS Certification Life Cycle



PA DSS - Top 5 Gaps

- Clear text storage of Account Data (Card No., Track Data, CVV etc.)
- Insufficient Cryptographic Key Management
- Absence of complete Password Policy
- Inadequate audit logging and no support for sending logs to centralized log server
- Absence of Threat Modeling, Code Review, Application Pen Test, OWASP Training

Compliance as a Service for PA DSS

Component	PA DSS Requirement Met
PA DSS Gap analysis	Overall PA DSS Certification
PA DSS Remediation support	Overall PA DSS Certification
PA DSS Final Audit and Report on Validation (ROV)	Overall PA DSS Certification
Continual compliance including annual minor updates (For year 2 onwards)	Overall PA DSS Certification
Card data discovery (twice for year 1)	1, 2
Application security scanning (For year 1 only)	5
Code Review Service (For year 1 only)	5
Application Threat Modeling (For year 1 only)	5
Creation of implementation guide (For year 1 only)	13
Training in secure coding techniques for developers (For year 1 only)	5

Takeaway

Payment Card Info is sensitive data for sure, here are 12 requirements to make it more secure

PCI Data Security Standards Secure Your Data

Erik Winkler

Senior Vice President - ControlCase

PCI QSA, PA QSA, P2PE QSA/PA QSA, ASV, CISSP

✉ ewinkler@controlcase.com

✉ US +1-703-431-4517

🖱 www.controlcase.com