



---

## WELCOME AND AGENDA

### PCI-DSS 3.0

- Review the high-level areas that have changed
- Review specific requirement changes
- Clarify **why** the changes happened

### Defining and Reducing Scope

- Review how to accurately determine scope
- Identify ways to reduce scope thus reducing risk

### Question and Answer



## PCI LIFECYCLE – ITERATIVE THREE-YEAR PROCESS

Eight steps in process to adopting new standard

- **Year 1**
  - November: Standards Published **(Done)**
  - January: Standards Effective **(Done)**
  - All year: Market Implementation
- **Year 2**
  - November: Feedback Begins
  - December 31: Older Standards Retired
  - April – August: Feedback Review
- **Year 3**
  - November – April: Draft Revisions
  - May – July: Final Review



## PCI 3.0 HIGH-LEVEL ADJUSTMENTS

- 1 Compliance as “Business as Usual”
- 2 Segmentation Clarifications
- 3 Risk Assessment Clarifications





# COMPLIANCE AS “BUSINESS AS USUAL”

 Trustwave®

## COMPLIANCE AS “BUSINESS AS USUAL”

**Compliance point of view**

- Duty of care.
- Move toward compliance as “business as usual” and a reminder of ongoing responsibility.
- Businesses are also expected to stay aware of the changes to the standard.

 Trustwave®



# RISK ASSESSMENT CLARIFICATION



## RISK ASSESSMENT

Compliance point of view

- Clarified that the risk assessment should be performed at least annually ***and after significant changes to the environment.***



---



# SEGMENTATION CLARIFICATIONS



---

---

## SEGMENTATION

Compliance point of view

“Segmentation equals isolation”

- Clarification as to the level of separation required
- SSC will be creating a white paper
- Segmentation boundary now a part of pen testing requirement



---

## SPECIFIC REQUIREMENT UPDATES

- 1 Penetration Testing rigidity
- 2 Scope change for e-commerce redirect merchants
- 3 Adjustment to AV requirement
- 4 Service Provider requirements
- 5 POS physical protection
- 6 Log review specifications
- 7 Assess data in memory



## PEN TEST REQUIREMENT RIGIDITY

### Compliance point of view

- New requirement to implement a methodology for penetration testing.
- *Effective July 1, 2015*
  - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
  - Includes testing from both inside and outside the network
  - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- New requirement, if segmentation is used to isolate the CDE from other networks, to perform penetration tests to verify that the segmentation methods are operational and effective



---

## E-COMMERCE REDIRECT MERCHANTS

### Compliance point of view

- Clarification of what is in scope:
  - Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or **web redirection servers**) the CDE.
- Affects e-commerce redirect merchants
- SSC will be providing clarification to the PCI community
  - FAQ
  - New SAQ and scanning requirements (include iframes, pure redirects, HOPs).
- These websites are a key security control for the flow of CHD into the CDE. They therefore are required to apply PCI security controls.



---

## ADJUSTMENT TO AV REQUIREMENT

### Compliance point of view

- New requirement to evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.
- New requirement to ensure that anti-virus solutions cannot be disabled or altered by users unless specifically authorized by management on a per-case basis
- Configured to perform automatic updates.
- Configured to perform regular scans.



---

## SERVICE PROVIDER REQUIREMENTS

### Compliance point of view

- Auth Credentials
  - New requirement for service providers with remote access to customer premises, to use unique authentication credentials for each customer.
  - *Effective July 1, 2015*
- New Agreements
  - Service Provider Agreements MUST articulate what they're responsible for



---

## POS PHYSICAL PROTECTION

### Compliance point of view

- New requirement to protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
- *Effective July 1, 2015*
- Essential Requirement:
  - Maintain a list of devices
  - Periodically inspect devices to look for tampering or substitution
  - Train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.



## IMPROVING LOG REVIEWS

### Compliance point of view

- Requirement change clarified that the intent of log reviews is to identify anomalies or suspicious activity
- Specifies what needs to be reviewed daily
  - All security events
  - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
  - Logs of all critical system components
  - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)



## Reducing Cardholder Data Environment Scope



---

## Identifying Scope

### Get an Executive Sponsor!

- Not a trivial exercise
- Follow the card data
  - Point of entry
  - Card data manipulation
  - Settlement processes
- Identify non-standard processes
  - Departmental databases
  - Spreadsheets
  - Hard copy data
- Identify service providers
- Map out dependent systems
  - Management systems
  - Security systems
  - Monitoring systems



---

## Reducing Scope

### Get rid of the data! Less CHD = Less Risk!

- Consolidate card data
- Implement segmentation
- Outsource
- Tokenization
- End-to-end encryption/P2PE



QUESTIONS?

