What Your QSA Should be Clarifying About Version 3.0

November 19, 2014

Presenters/Speakers:
Craig Sullivan, CPA, CISA, QSA
Angie Hipsher, CISA, QSA

Agenda

What Your QSA Should be Clarifying About Version 3.0

- **Areas of Focus – e.g. the biggest impact on you!**
  - ***Scoping***: Effective and adequate segmentation
    - Impact of changes on Requirements 1, 2 & 11
  - ***Threat and Vulnerability Management***: Going Beyond patch management
    - Impact of changes to Requirements 5, 6, and 11
    - Difference between vulnerability scanning and penetration testing
    - Impact of changes to Requirement 11
- **Overview of Additional Changes in PCI DSS Version 3.0**
- **Conclusion**

Important Dates

- January 1, 2015 - PCI DSS Version 3.0 is Required

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	ROC Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.							
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	• Testing and approval of all network connections.	*<Report Findings Here>*					
	• Testing and approval of all changes to firewall and router configurations.	*<Report Findings Here>*					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	• **Identify** the sample of records for network connections that were examined.	*<Report Findings Here>*					
	• **Identify** the responsible personnel interviewed who confirm that network connections were approved and tested.	*<Report Findings Here>*					
	Describe how the sampled records were examined to verify that network connections were:						
	• Approved	*<Report Findings Here>*					
	• Tested	*<Report Findings Here>*					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations.	• **Identify** the sample of records for firewall and router configuration changes that were examined.	*<Report Findings Here>*					

- December 31, 2014 - PCI DSS Version 2.0 expires

Source: PCI Data Security Standards Requirements and Security Assessment Procedures, Version 3.0

Polling Question

- If your organization has been through a PCI compliance review, does the organization have a formal methodology for determining scope?

a) Yes

b) No

c) Unsure/don't know

PCI Scoping – Defined by the Standards

- In the past, the guidance of the PCI Security Standards Council consistently stated that systems that store, process, or transmit cardholder data are subject to the requirements of the PCI DSS.

- What has changed?

  - PCI DSS version 3.0, now clearly states that “PCI DSS security requirements apply to all system components included in ***or connected to*** the cardholder data environment.”

  - Independent assessors must understand how the organization conducted the assessment to define the scope.

  - The assessor must validate the accuracy of management’s scope.

PCI Scoping – Defined by Experience

- Systems that attach to or support the infrastructure of the cardholder data environment (CDE) will be considered for inclusion in scope.
  - "Attached" systems communicate with CDE systems.
  - "Support" systems define and regulate the CDE secure environment.

- In addition to the systems, the people and processes that handle cardholder data should be considered for inclusion in scope.
  - Usage of card data for business processes may surprise you.
  - Don't forget the paper!

- Rule of thumb:

If a system can affect the security of cardholder data, it is in scope!

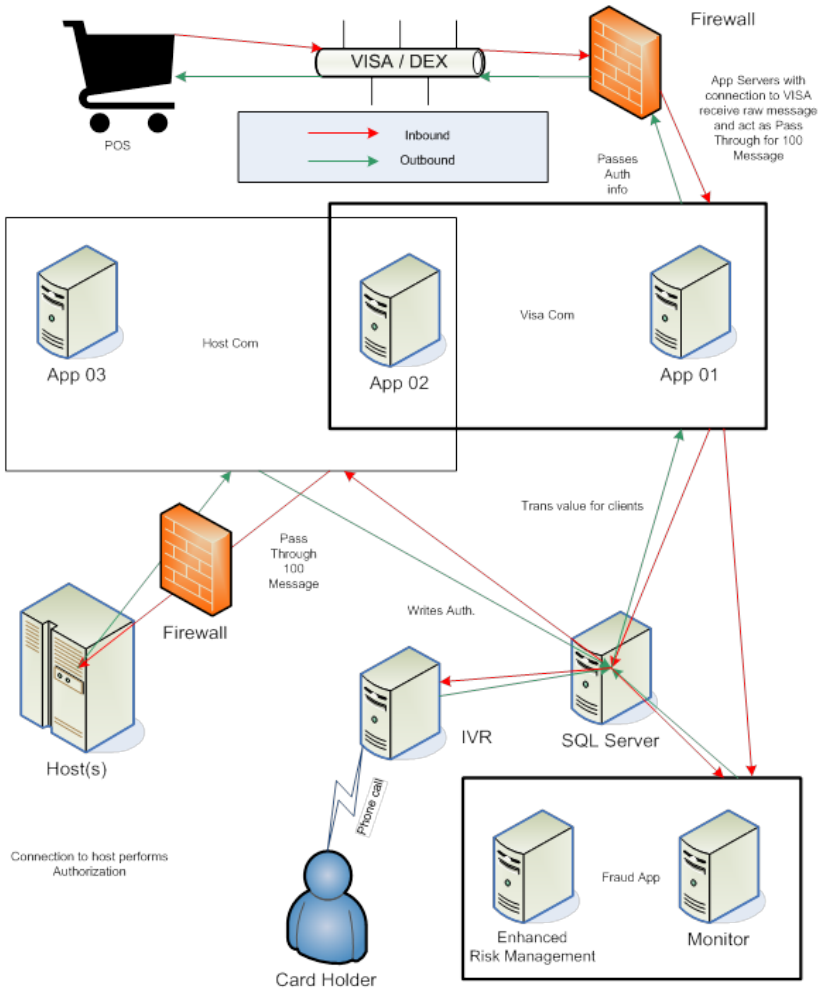
Defining your Cardholder Data Environment

- New Requirement 2.4 - Will require organizations to maintain an inventory of system components in scope for PCI DSS to support effective scoping practices.
- New Requirement 9.9.1 - Maintain an up-to-date list of devices.
- New Requirement 11.1.1- Requires inventory of all authorized wireless access points (justification will have to be part of the inventory).

Description	IP Address	Hostname	Location	Application	Card Data Present	Length of Storage	Method of Protection
Mainframe #1	xxx.xx.xx.x	Host1	CITY, State	Application 1	Full PAN	8 days	AES 256
System #1	xx.xx.xx.x	Host2	CITY, State	Application 2	Truncated PAN	90 days	n/a – Truncated
System #2	xxx.xx.xx.x	Host3	CITY, State	Application 3	Full PAN and transaction data	8 days	Proprietary Encryption

Defining your Cardholder Data Environment

- If your organization has upcoming plans to increase system scalability & utilization levels, it will be increasingly important to document the added systems as well update the new requirement for maintaining a current diagram that shows cardholder data flows (**New Requirement 1.1.3**) as well as network diagrams.



Polling Question

- Has your organization employed segmentation to reduce the scope and complexity of the PCI review process?

a) The full network is within scope.
b) Segmentation has been used to reduce the scope.
c) Unsure/don't know

Impact on Scope – Network Architecture

- A simple or flat network does not provide adequate segmentation between the cardholder data repositories and unrelated systems.
  - Communication is unconstrained between systems, which allows for the spread of malware and targeted attacks from these otherwise unrelated systems.
  - The scope and corresponding cost of compliance for a flat network would extend to all systems.
  - It might be extremely difficult to enforce more stringent requirements to all users of a flat network.
  - Some segmentation between cardholder systems and public networks (e.g., the Internet) are always required, as described in Requirement 1 of the PCI DSS.

Impact on Scope – Network Architecture

- Internally segmented networks may be used to compartmentalize the scope of compliance cost to only the CDE.
  - Effective segmentation must go beyond zone definition. Interzone traffic to unrelated systems and zones should be blocked or restricted to less interactive protocols required for business purposes.
  - Segmented support systems should still be considered in scope where the support systems have a direct impact on the security and compliance of the primary systems in the CDE (e.g., the logging system).
  - Some small environments might not be able to effectively segment the network for scope reduction.

Defining your Cardholder Data Environment

Validating Segmentation:

- A new requirement 11.3.4, if segmentation is used to isolate the cardholder data environment (CDE) from other networks, the penetration test will need to verify that the segmentation methods are operational and effective.

Polling Question

- Has vulnerability scanning been completed within the last quarter at your organization?
  a) Yes – Internal vulnerability scanning has been completed
  b) Yes – External vulnerability scanning has been completed
  c) Yes – Both an internal and external vulnerability scans have been completed
  d) No
  e) Unsure/don't know

Threat and Vulnerability Management:

To cope with the growing numbers of threats to the customer data maintained by organizations that store, process, or transmit payment card data, these organizations need to have a rigorous process to:

- Identify and rank vulnerabilities according to the level of risk they pose to their IT environments
- Develop procedures for installing corrective patches on a timely basis
- Conduct internal and external network scans at least quarterly to identify new vulnerabilities
- Develop configuration standards for all system components to help prevent future vulnerabilities

Threat and Vulnerability Management

There are many requirements that help to address the concept of vulnerability management and include the following:

- Employ appropriate Anti-Virus (Requirement 5)
- Identify and Rank Vulnerabilities (Requirement 6)
- Install Corrective Patches (Requirement 6)
- Conduct Vulnerability Scans and Penetration Tests (Requirement 11)
- Develop Configuration Standards (Requirement 2)

So, what is new?

Threat and Vulnerability Management

Changes to Requirement 5 will include…

- **New requirement 5.1.2** – requires the evaluation of evolving malware threats for systems not to be commonly affected by malicious software.
  - This requirement will introduce the increased need for your organization to stay up to date with the industry trends in emerging malicious software and how this can affect your systems.

- **Requirement 5.3** updates involve ensuring that your organization's anti-virus solutions are actively running (formerly noted in 5.2) and cannot be *disabled or altered by users unless specifically authorized by management on a per-case basis*.
  - Your organization will want to update IT security policies & procedures to include procedures for enhanced security controls surrounding anti-virus solutions. Consult your anti-virus solution vendor for assistance.
  - Cloud-based anti-virus solutions have emerged and most include these controls.

Threat and Vulnerability Management

Changes to patching in Requirement 6:

- **Requirement 6.2** – Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
  - Installation of "Non-Critical" vendor-supplied security patches must have a defined time they will be installed in and policy followed accordingly.

Threat and Vulnerability Management: Vulnerability Scans

Vulnerability Assessment Pros

- Thousands of security checks can be performed in automated fashion.
- The entire network can be assessed relatively quickly.
- Vulnerability assessments typically can be integrated into the organization's threat and vulnerability management program.
- Vulnerability assessments are useful for layer-one remediation testing.
- Vulnerability assessments identify easy targets.

Vulnerability Assessment Cons

- Vulnerability assessments can provide an overwhelming, incoherent amount of data.
- They typically contain numerous false positives, especially for areas such as patch management and secure application development.
- Due to lack of impact analysis, they have inadequate risk rankings often based on tool suggestions.
- They are unable to chain together vulnerabilities to determine overall impact to the business.
- They fail to identify logical attack vectors such as password reuse and application logic flaws.
- Recommendations for remediation are often generic and based on tool output.

Threat and Vulnerability Management: Penetration Testing

- Mimic a real-world attacker attempting to access systems and data by identifying vulnerabilities and combining (chaining) them to get unauthorized access to information or gain administrative control of the environment.
- Can take into account mitigating controls and issue's impact by evaluating the confidentiality, integrity, and availability of the supporting environment.
- Involves the human factor, which is required to required to chain vulnerabilities and understand the organizational impact of issues.
- False positives are removed from all layers of the security model.
- Logical, realistic recommendations that fit the organization are provided.

Threat and Vulnerability Management: Vulnerability Scans vs. Penetration Testing

- Vulnerability Scanning and Penetration Testing are similar services in that they are both necessary tools in threat and vulnerability management programs. However, they differ greatly with regard to providing value in their analysis.

	Vulnerability Assessment	Penetration Test
Target identification	X	X
Layer one vulnerability identification	X	X
Removal of false positives		X
Vulnerability exploitation and compromise		X
Password strength analysis		X
File-share authorization analysis		X
User-rights examination		X
Egress traffic analysis		X
Password reuse analysis		X
Voice and data traffic segmentation		X
Service or application account privilege analysis		X

Penetration Testing Changes….

- Requirement 11.3 - New requirement to develop and implement a methodology for penetration testing (effective July 1, 2015). Pen testing requirements from PCI DSS v2.0 must be followed until the new requirement takes effect.

MORE ON CHANGES….

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 1:
  - Requirement 1.1.3 - Network Diagram must include a current diagram that shows cardholder data flows.

- Requirement 2:
  - Requirement 2.4 - New requirement to maintain an inventory of all system components in scope for PCI DSS to support effective scoping practices.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 4:
  - Requirement 4.1.a - *All locations where CHD is transmitted/received over open/public networks must be identified* and system settings for corresponding protocols and cryptography reviewed.

- Requirement 5:
  - Requirement 5.1.2 - New requirement to evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.
  - Requirement 5.3 - New requirement to implement controls to make sure anti-virus cannot be disabled or altered by users unless specifically authorized by management on a per-case basis.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 6:
  - Requirement 6.5 – Provides *clarification* for coding practices to document how Primary Account Numbers (PAN) and Sensitive Authentication Data (SAD) is stored in memory.

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

  - Requirements 6.5.1 to 6.5.10 - Specifics on what developers must be doing to prevent common coding vulnerabilities are now included.
  - Requirement 6.5.10 - New requirement for coding practices to protect against broken authentication and session management (effective July 1, 2015).

Source: https://www.pcisecuritystandards.org

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 8:
  - Requirement 8.2.3 - Combined minimum password complexity and strength requirements into single requirement *and increased flexibility for alternatives that meet the equivalent complexity and strength.*
  - Requirement 8.5.1 - New requirement for service providers to use different credentials for access to different customer environments (effective July 1, 2015).
  - Requirement 8.6 - New requirement for security considerations for authentication mechanisms such as physical security tokens, smart cards and certificates, to address authentication methods other than passwords.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 9:
  - Requirement 9.3 - New requirement to control physical access to sensitive areas for onsite personnel, including a process to authorize access and *revoke access immediately upon termination.*
  - Requirement 9.9 - New requirements to protect point-of-sale devices that capture payment card data from tampering or unauthorized modification or substitution (effective July 1, 2015).
  - Requirement 9.9.1 - New requirement to maintain an up-to-date list of devices.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 10:
  - Requirement 10.2.5 - New requirements to provide more stringent controls over logging of changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
  - Requirement 10.2.6 – Requires logging to include initialization, stopping, or ***pausing*** of the audit logs.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 11:
  - Requirement 11.1.1 - Requires inventory of all authorized wireless access points. (justification will have to be part of the inventory).
  - Requirement 11.3 - New requirement to develop and implement a methodology for penetration testing (effective July 1, 2015). Pen testing requirements from PCI DSS v2.0 must be followed until the new requirement takes effect.
  - Requirement 11.3.4 - A new requirement, if segmentation is used, to isolate the cardholder data environment (CDE) from other networks, the penetration test will need to verify that the segmentation methods are operational and effective.
  - Requirement 11.5.1 - New requirement to implement a process to respond to any alerts generated by the change-detection mechanism.

Overview of Evolving Requirements - PCI DSS v3.0

- Requirement 12:
  - Requirement 12.2 - Clarification that the risk assessment should be performed ***at least*** annually **<u>and</u>** ***after*** significant changes to the environment.
  - Requirement 12.8.5 - New requirement to maintain information about which PCI DSS requirements are managed by the service provider, and which are managed by the entity.
  - Requirement 12.9 - New requirement for service providers to acknowledge, ***in writing*** to the customer, that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer (effective July 1, 2015).

Polling Question

- Which of the changes to PCI DSS v3.0 are you most concerned about?

a) Scoping requirements
b) Validation of segmentation/penetration testing
c) Monitoring of third-parties
d) POS security
e) Other
f) Unsure/don't know

In Summary:

- Don’t get caught unprepared in 2015 when validating compliance on version 3.0.
- Review new solutions and programs that may be significant to maintaining ongoing compliance.
  - New technologies and changes in architecture require planning from a scoping perspective and may affect your compliance
- Use your Vulnerability Management Program to not only maintain compliance, but to manage risks!
- Recognize new challenges that organizations may face in achieving compliance with the new version of the standard.
  - Incorporate aspects of the scoping process to fulfill new requirements for inventory and penetration testing

Crowe Horwath

Additional Resources:

Please visit: http://www.crowehorwath.com/pci to discover useful resources, including:

Previous webinar recordings related to:

- *PCI Scoping*
- *PCI for 2012: Past, Present and Future*

And, white papers, including:

- *The Pros and Cons of Vulnerability Assessments*
- *Preparing for Heightened Standards for PCI Compliance*
- *Managing PCI Compliance in the Age of Mobile Payments*
- *PCI Compliance: The Risks Banks Can Miss*
- *PCI DSS Vulnerability Assessments: Going Beyond Patch Management*

As well as, other useful links, FAQ and references for your PCI needs

Crowe Horwath

Questions?

For more information, contact:

Craig Sullivan
Direct 574.236.7618
Craig.Sullivan@crowehorwath.com

Angie Hipsher
Direct 317.208.2430
Angie.Hipsher@crowehorwath.com

Please visit http://www.crowehorwath.com/pci to discover useful PCI resources.