



## A Note on Our New Name

*Secure Enterprise Computing was acquired as the Security Division of Agio LLC in March 2013. As part of our one-year anniversary with Agio (the superior provider of managed IT services for the world's premier alternative investment managers) we're fully adopting the Agio brand. We will continue serving our clients across the financial, government, healthcare, education, commercial, retail and hospitality markets, and now we have the capability to offer a rich portfolio of IT services solutions. As the market continues to seek integrated, single-point-of-contact providers, this augmentation to our business ensures our clients remain ahead of the curve.*

*Same great people, same great service, but now with so much more...*

AGIO

1

## Agio - What We Do



AGIO

## Our Security Credentials

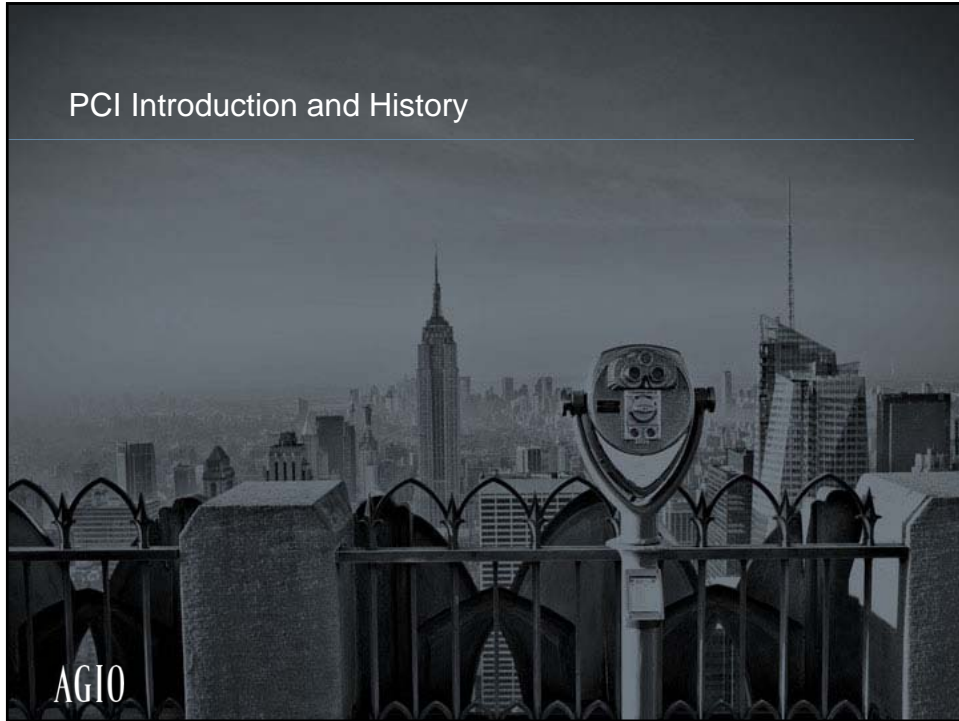
- 20+ years of continuous service as IT Security Consultants and Security VAR
- 15+ years conducting compliance-based assessments
- PCI Qualified Security Assessor (QSA) since 2009
- PCI Approved Scanning Vendor (ASV) since 2006
- HITRUST (HIPAA/HITECH) Certified Practitioners
- 1 of 9 companies pre-approved by State of NC to conduct assessments for state agencies and higher education
- Consultants hold many certifications including CISSP, SANS, etc. and have on average 15 years of experience



AGIO

## PCI Introduction and History

---



### PCI Security Standards Council Historical Data

---

- PCI DSS created in December 2004
- Original Compliance Deadline was June 2005
- PCI SSC formed in Sept of 2006 and Version 1.1 of the standard released
- Version 1.2 released October of 2008
- **Version 2.0 released October 2010** – Currently in use
- **Version 3.0 released October 2013** – Goes into effect January 1, 2015 (can be used now)

AGIO

5

## The Payment Card Industry Data Security Standard (PCI DSS)

---



### What is PCI-DSS?

1. It is a private initiative set forth by the Payment Card Industry.
2. A set of standards outlining how sensitive data is handled both operationally and technically.

AGIO

6

## The Payment Card Industry Data Security Standard (PCI DSS)

---



3. PCI DSS provides protections for all participants in a credit card transaction.
4. Applies to anyone who “stores, transmits, or processes” cardholder data.
5. Applies to both physical and electronic data, including but not limited to: servers, removable media, backup media, and documents.

AGIO

7

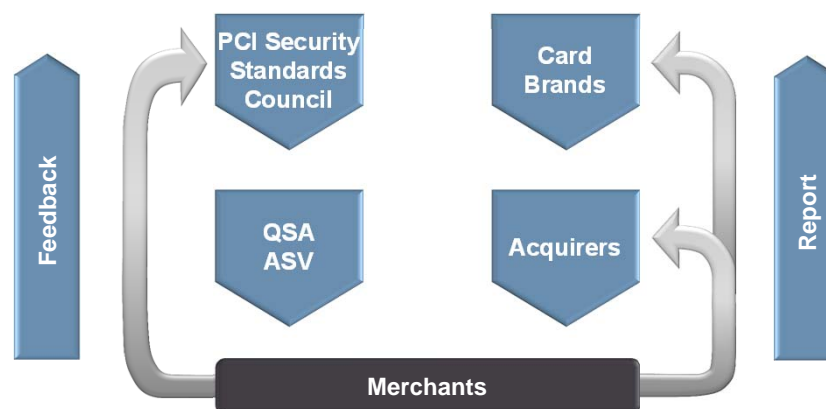
## PCI: What Does It Protect?

- The primary account number is the defining factor in the applicability of PCI DSS requirements.
- PCI DSS requirements are applicable if a primary account number (PAN) is **stored, processed, or transmitted**. If PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.
- PCI DSS applies wherever account data is stored, processed or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data.

AGIO

8

## Guidance and Enforcement – The Different Roles



AGIO

9

## PCI: What Can Be Stored and How?

	Data Element	Storage Permitted ?	Render Stored Account Data Unreadable
<b>Cardholder Data</b>	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
<b>Sensitive Authentication Data</b>	Full Magnetic Stripe Data	No	Cannot store after authorization
	CAV2/CVC2/CVV2/CID	No	Cannot store after authorization
	PIN/PIN Block	No	Cannot store after authorization

AGIO

10

## Cardholder Data



AGIO

11

## PCI DSS Is Not Law

- Through your Merchant Agreement with your acquiring bank, you are **contractually bound** to abide by all relevant PCI standards
- **No threat of incarceration** for non-compliance with PCI DSS Security Breach Notification Laws
  - See [N.C. Gen. Stat § 75-65](#) which identifies cardholder data as Personally Identifiable Data (PII) which is protected under North Carolina law

AGIO

12

## Possible Fines for Non-compliance



- **First Violation**  
Up to \$50,000
- **Second Violation**  
Up to \$100,000
- **Third Violation**  
Up to Management Discretion
- **Failure to Report a Compromise**  
Up to \$100,000
- **Egregious Violation**  
Up to \$500,000



- **Level 1 Merchant** (*6,000,000+ transactions per year*)  
Up to \$100,000  
AND... If not compliant after 60 days, MasterCard or Visa additional fines of \$10,000 per day (not to exceed \$500,000 per year)
- **Level 2 Merchant** (*150,000–6,000,000 transactions per year*)  
Up to \$50,000  
AND... If not compliant after 60 days, MasterCard or Visa additional fines of \$10,000 per day (not to exceed \$500,000 per year)
- **Level 3 Merchant** (*20,000–150,000 transactions per year*)  
Up to \$25,000  
AND... If not compliant after 60 days, MasterCard or Visa additional fines of \$10,000 per day (not to exceed \$500,000 per year)

AGIO

13

### PCI: Technical and Operational Controls

Technical	Operational
Firewalls	Policy
Intrusion Detection	Security Awareness Training
Two-factor Authentication	Incident Response Testing
Antivirus	Change Control
Encryption	Employee Screening
Security Event Logging	Risk Assessment

### PCI DSS: 6 Goals with 12 Requirements

Build and Maintain A Secure Network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect data</li> <li>2. Do not use vendor supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored data</li> <li>4. Encrypt transmission of cardholder data and sensitive information across public networks</li> </ol>
Maintain A Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Use and regularly update antivirus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>



## Payment Brand Compliance Programs



AGIO

- Each payment brand develops and maintains its own PCI DSS compliance programs in accordance with its own security risk management policies
  - American Express: Data Security Operating Policy (DSOP)
  - Discover: Discover Information Security Compliance (DISC)
  - JCB: Data Security Program
  - MasterCard: Site Data Protection (SDP)
  - Visa USA: Cardholder Information Security Program (CISP)
  - Other Visa Regions: Account Information Security (AIS) Program

16

## PCI Merchant Levels

Merchant Level	Merchant Definition	Compliance
Level 1	More than 6 million V/MC transactions annually across all channels, including eCommerce	Annual On-site PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 – 5,999,999 V/MC transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 3	20,000 – 1,000,000 V/MC eCommerce transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 4	Less than 20,000 V/MC eCommerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self-Assessment and Annual Network Scans

AGIO

17

## Self Assessment Questionnaire (SAQ)

---

- 9 different SAQ's (3 additional since v 2.0)
  - Binary standard: “in place” or “not in place”
  - What is your bank/processor asking for?
- Qualifiers/Disqualifiers
  - Electronic storage of CHD (just because you don't store CHD doesn't necessarily mean you don't have to use SAQ D)
  - Read the “Before You Begin” section

AGIO

18

## Self Assessment Questionnaire (SAQ) (Cont'd)

---

- **A:** Card-not-present Merchants, All CHD functions fully outsourced
  - “Completely outsourced to “validated” third parties
- **A-EP:** Partially Outsourced E-commerce Merchants using third-party Website for Payment Processing
  - Your e-commerce website does not receive CHD but controls how consumers, or their CHD, are redirected to a validated third-party processor
- **B:** Imprint Machines or Standalone dial-out terminals
- **B-IP:** IP connected PTS Point-of-interaction (POI) terminals

AGIO

19

## Self Assessment Questionnaire (SAQ) (Cont'd)

---

- **C:** Payment applications connected to the Internet, No CHD storage
  - POS directly connected to the Internet
  - Not connected to any other systems in the environment
- **C-VT:** Web-based Virtual Payment Terminals, No CHD storage
  - Manually enter a single transaction at one time
  - Terminal solution is provided and hosted by a validated third-party processor
  - No card readers attached
  - Organization does not transmit CHD through any other channels

AGIO

20

## Self Assessment Questionnaire (SAQ) (Cont'd)

---

- **P2PE-HW:** Hardware Payment Terminals in a PCI-Listed P2PE Solution, No CHD
  - The implemented solution is listed on the PCI SSC's list of "validated" Point-to-Point Encryption solutions
- **D:** All other SAQ-Eligible Merchants
  - Network = D
- **D:** SAQ-Eligible Service Providers

AGIO

21

## Common PCI DSS Violations

---

- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing malicious users in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2 and 8.3)
- Default system settings and passwords not changed when system was set up (Requirement 2.1)
- Unnecessary and insecure services not removed or secured when system was set up (Requirements 2.2.2 and 2.2.4)
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5); redirect from website
- Missing and outdated security patches (Requirement 6.1)

AGIO

22

## Common PCI DSS Violations (Cont'd)

---

- Lack of logging (Requirement 10)
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5)
- Poorly implemented network segmentation resulting in the cardholder data environment being unknowingly exposed to weaknesses in other parts of the network that have not been secured according to PCI DSS (for example, from unsecured wireless access points and vulnerabilities introduced via employee e-mail and web browsing) (Requirements 1.2, 1.3 and 1.4)

AGIO

23

## What Should I Do?

---

- Identify all payment channels (methods of processing payment)
  - Group the Merchant IDs MIDs
  - Location
  - Applications
  - Storage
- Identify all systems used in the process (scoping)
  - Asset inventory
- Conduct gap assessment
  - Apply the standard to the “in scope” systems

AGIO

24

## PCI Compliance

---

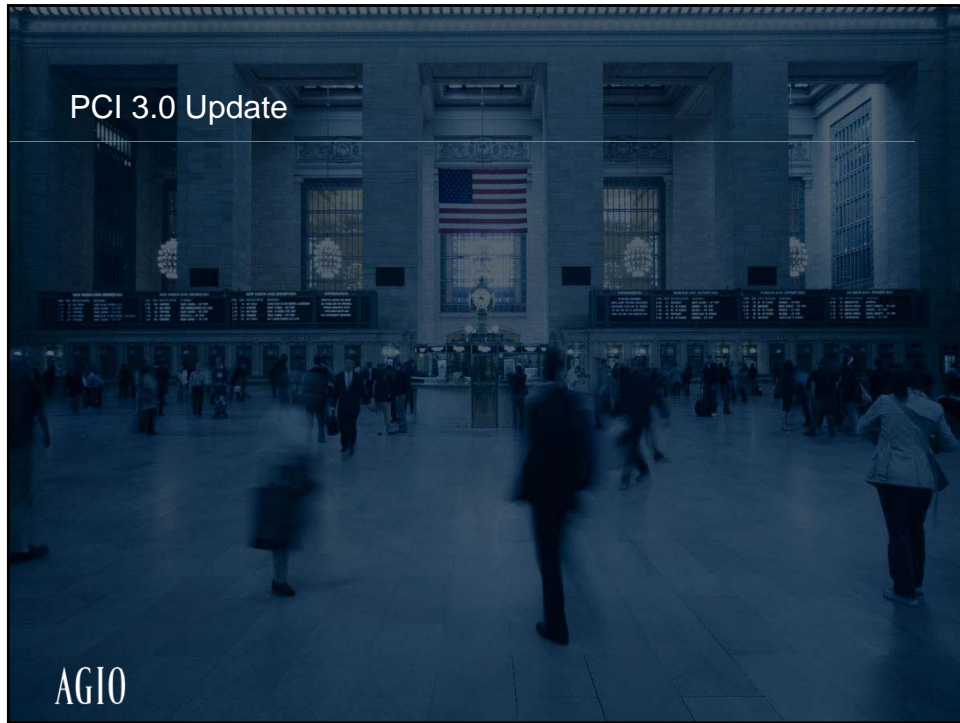
### PCI-DSS is NOT merely about checking boxes



The intent of PCI-DSS is to prevent fraud and protect customers. Requirements must be met, but the goal is to provide robust information security within your organization.

AGIO

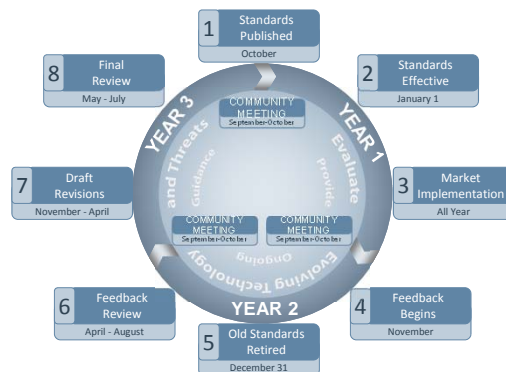
25



## The PCI DSS Lifecycle

- The PCI DSS follows a three-year lifecycle
- PCI DSS 3.0 was released in October 2013
- Optional (but recommended) in 2014; Required in 2015

### Lifecycle for Changes to PCI DSS and PA-DSS



## Key Themes

---

- Education and awareness
- Flexibility and consistency
- Security as a shared responsibility
- Emerging threats

AGIO

28

## Best Practices for Implementing PCI DSS Into Business As Usual (BAU) Processes

---

- Continuous compliance with due diligence needed
- PCI DSS is not a “once-a-year” activity
- Don’t forget about the people and processes

AGIO

29

## Administrative Improvements

---

- Enhanced sampling examples and testing procedures for each requirement
- Enhanced reporting guidance
  - Navigation Guide integrated into PCI DSS v 3.0
- New templates (ROC/SAQ)
  - ROC reporting instructions built into the ROC template
  - Easier to complete, more concise
  - Visual queues for when diagrams are needed
- Policy and procedure requirements moved from Section 12 to each individual section

AGIO

30

## Administrative Improvements (Cont'd)

---

- Added flexibility to meet requirements:
  - Passwords
  - Web application firewalls
  - File integrity monitoring (FIM)
  - Inventory/labeling options
- **NEW** requirements listed in this presentation are either a requirement as of January 1, 2015 or a best practice until June 30, 2015, after which they become mandatory requirements (see list).
- Note: Cannot mix and match v 2.0 and v 3.0 in 2014 – must use one or the other this year

AGIO

31



## Scoping Guidance

---

- Improper scoping leads to increased risk
  - Look at people and process
- Focus on security, rather than compliance
- Not a one-time-a-year activity
- Confirm effectiveness of PCI scope (penetration test)
- Goal: reduce complexity and create more efficient security
- Risk assessments as scoping aid

AGIO

32

## Clarifications for Segmentation

---

- Isolation is clarified
- Controlled access means a connection exists, therefore those systems are in scope (AD, AV, DNS, time servers, etc.)
- Improved language to verify effectiveness

AGIO

33

## Changes – Requirement 1 “Build and Maintain a Secure Network and Systems”



### Clarifications:

- Configuration standards must be documented and implemented (1.1.x)
- Network diagram & CHD flows (1.1.2-1.1.3)
- Insecure services, protocols, ports (1.1.6)
- Securing router configuration files (1.2.2)
- Wireless access control to CDE (1.2.3)
- Anti-spoofing (1.3.4)
- Access to CDE from untrusted networks (1.3.7)
- Requirement and testing procedures (1.4)

AGIO

34

## Changes – Requirement 2 “No Vendor Defaults”



### Clarifications:

- Change all default passwords; remove unnecessary default accounts (2.1)
- Change all wireless default passwords at installation (2.1.1)
- Include the above in Configuration Standards (2.2)
- Enable only necessary/secure services, protocols, and ports (2.2.2-2.2.3)

AGIO

35

## Changes – Requirement 2 “No Vendor Defaults”



### NEW Requirement:

- REQUIRED BY  
JAN 1, 2015** – Maintain an inventory of all systems and components that are in scope for PCI DSS

AGIO

36

## Changes – Requirement 3 “Protect Stored Cardholder Data (CHD)”



### Clarifications:

- Data Retention and Disposal (3.1.x)
- Sensitive Authentication Data (SAD) proper destruction after authorization (3.2)
- Primary Account Number (PAN) masking (3.3)
- Separation of OS and Disk-level encryption authentication mechanisms (3.4.1)
- Key Management procedures (3.5)
- Provided flexibility with more options for secure storage of cryptographic keys (3.5.2-3.5.3)
- Testing implementation of crypto key management (3.6.x)
- Crypto key “split-knowledge” and “key control” (3.6.6)

AGIO

37

## Changes – Requirement 4 “Encrypt Transmission of CHD Across Untrusted Networks”



### Clarifications:

- Expanded examples of open public networks (4.1)

AGIO

38

## Changes – Requirement 5 “Maintain a Vulnerability Management Program”



### Clarifications:


- Ensure all AV mechanisms are maintained properly (5.2)

### **NEW** Requirements:

- REQUIRED BY  
JAN 1, 2015 – Systems not commonly affected by malware must be evaluated (5.1.2)
- REQUIRED BY  
JAN 1, 2015 – Ensure AV is running and cannot be disabled/altered (5.3)

AGIO

39



## Changes – Requirement 6


### “Develop & Maintain Secure Systems and Applications”

---

**Clarifications:**

- Identifying, risk ranking, and patching critical vulnerabilities (6.1-6.2)
- Written software development procedures (6.3)
- Development and Test environments (6.3.1)
- Enhanced testing procedures that include document reviews (6.4)
- Enforce separation of production and development environments with access controls (6.4.1)
- Updated list of current and emerging coding vulnerabilities and secure coding guidelines (6.5.x)
- Options beyond Web Application Firewall provided (6.6)

**AGIO**
40



## Changes – Requirement 6

### “Develop & Maintain Secure Systems and Applications”

---

**NEW Requirements:**

- Handling of PAN and SAD in memory (6.5)
- REQUIRED BY JUL 1, 2015 – Coding practices to protect against broken authentication and session management (6.5.10)

**AGIO**
41

## Changes – Requirement 7 “Restrict Access to CHD by Business Need-to-Know”



### Clarifications:

- Revised testing procedures (7.1)
- Definition of access needs for each role (7.1.1)
- Restrict Privileged User IDs to least necessary (7.1.2)
- Assign access based upon role/classification (7.1.3)

AGIO

42

## Changes – Requirement 8 “Identify and Authenticate Access to System Components”



### Clarifications:

- User identification (8.1)
- Remote vendor access (8.1.5)
- User authentication (8.2)
- Changed passwords to passphrases/authentication credentials
- Requirements apply to 3rd Party Vendors
- Strong cryptography for authentication credentials (8.2.1)
- Authenticate users prior to modifying credentials (8.2.2)

AGIO

43

## Changes – Requirement 8

### “Identify and Authenticate Access to System Components”



#### Clarifications:

- Requirements 8.1.1, 8.1.6-8.1.8, 8.2, 8.5, and 8.2.3-8.2.5 are not intended to apply to user accounts within a point-of-sale (POS) application that only has access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).
- Two-factor authentication applies to users, administrators, and all third-parties (8.3)
- How to protect authentication credentials (8.4)

AGIO

44

## Changes – Requirement 8

### “Identify and Authenticate Access to System Components”




#### NEW Requirements:

- REQUIRED BY JAN 1, 2015** – Options provided beyond passwords (tokens, smart cards, and certificates) for equivalent variations (8.2.3)
- REQUIRED BY JUL 1, 2015** – Service Providers with access to customer environments must use a unique authentication credential (e.g., password) for each customer environment (8.5.1)
- REQUIRED BY JAN 1, 2015** – Physical security tokens must be capable of being linked to an individual account (8.6)

AGIO

45



## Changes – Requirement 9

### “Restrict Physical Access to Cardholder Data”


---

Clarifications:

- Protection of network jacks (9.1.2)
- Differentiation between on-site personnel and visitors – options made available (9.2.x)
- Visitor audit trails (9.4.x)

**AGIO**

46



## Changes – Requirement 9

### “Restrict Physical Access to Cardholder Data”

---


**NEW** Requirements:

- REQUIRED BY  
JAN 1, 2015 – Control physical access to sensitive areas for on-site personnel (9.3)
- REQUIRED BY  
JUL 1, 2015 – Protect POS terminals and devices from tampering or substitution (9.9)

**AGIO**

47




Changes – Requirement 10   
“Track and Monitor All Access to Network Resources and Cardholder Data”

---

Clarifications:

- Audit trails linked to individuals (10.1)
- Clarified the intent and scope of daily log reviews (10.6)

AGIO 48


Changes – Requirement 10   
“Track and Monitor All Access to Network Resources and Cardholder Data”

---

**NEW** Requirements:

- REQUIRED BY JAN 1, 2015 – All changes to identification and authentication mechanisms and all changes to root or administrator access must be logged (10.2.5)
- REQUIRED BY JAN 1, 2015 – Pausing, stopping, and restarting of audit logs must be logged (10.2.6)

AGIO 49




## Changes – Requirement 11 “Regularly Test Security Systems and Processes”

---

Clarifications:

- Added guidance regarding multiple scan reports (11.2)
- Quarterly internal vulnerability scans must be repeated until a passing scan results (11.2.2)
- Internal and External scans must be performed after significant changes (11.2.3)
- Correct all vulnerabilities detected during a Penetration Test (11.3.3)
- Methods expanded for detecting changes to files (11.5)

**AGIO** 50



## Changes – Requirement 11 “Regularly Test Security Systems and Processes”

---

**NEW** Requirements:

- REQUIRED BY  
JAN 1, 2015 – Have an inventory and business justification for wireless access points (11.1.x)
- REQUIRED BY  
JUL 1, 2015 – Implement a methodology for penetration testing, and perform penetration tests to verify that the segmentation methods are operational and effective (11.3)
- REQUIRED BY  
JAN 1, 2015 – Develop process to respond to change detection alerts (11.5.1)

**AGIO** 51

## Changes – Requirement 12

### “Maintain a Policy that Addresses Security for all Personnel”



#### Clarifications:

- Policy and procedure requirements moved from Section 12 to each individual section
- Added options regarding identification (labeling) of devices (12.3.4)
- Testing of remote access timeouts (12.3.8)
- Management of Service Providers (12.8)
- Further defined the components of Incident Response plan (12.10.x)

AGIO

52

## Changes – Requirement 12

### “Maintain a Policy that Addresses Security for all Personnel”



#### NEW Requirements:

- REQUIRED BY  
JAN 1, 2015 – Risk Assessment should be performed at least annually and after significant changes (12.2)
- REQUIRED BY  
JAN 1, 2015 – Maintain separation of duties for security responsibilities (12.4.1)
- REQUIRED BY  
JAN 1, 2015 – Clarified essential components of Service Provider agreements (12.8.2)
- REQUIRED BY  
JAN 1, 2015 – Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity (12.8.5).
- Service providers to acknowledge REQUIRED BY  
JUL 1, 2015 responsibility for maintaining applicable PCI DSS requirements. (12.9)

AGIO

53

## Next Steps – How to Prepare for 3.0

---

- Review the clarifications to ensure compliance
- Verify effective segmentation of CDE
- Look at day-to-day PCI compliance efforts
  - Are configuration standards current?
  - Are diagrams current?
  - Are security procedures current and being followed?
- Review asset inventory process (2.x); ensure it includes all CDE systems and any wireless access points (11.2)
- Consider AV options for increased coverage (5.1.2)
- Ensure AV is locked down (5.3)

AGIO

54

## Next Steps – How to Prepare for 3.0 (Cont'd)

---

- Ensure the **Risk Ranking Procedure** is documented and followed (6.2)
- Review *PA DSS Implementation Guides*
  - How is PAN/SAD stored in memory managed? (6.5.6)
- Review session management coding practices (6.5.11)
- Review how service providers are managed
  - Access management - no shared IDs/accounts (8.5.1)
  - Fully PCI compliant (12.8)
  - Review contracts, clearly define responsibilities (12.8.2)
  - Ensure the Service Provider acknowledges responsibilities (12.9)

AGIO

55

### Next Steps – How to Prepare for 3.0 (Cont'd)

---

- Review security tokens and ensure each is linked to a unique individual (8.6)
- Review on-site personnel access controls to sensitive areas (9.3)
- Consider methods to prevent tampering with POS equipment (9.9)
- Review log security settings (admins, stop/start, etc.) (10.2.5-6)
- If wireless is used, document the business justification (11.1)
- Ensure penetration test methodology is documented (11.3)
- Ensure vulnerabilities detected are corrected and then retest to ensure compliance for internal scans (11.2.2) and penetration tests (11.3.3)

AGIO

56

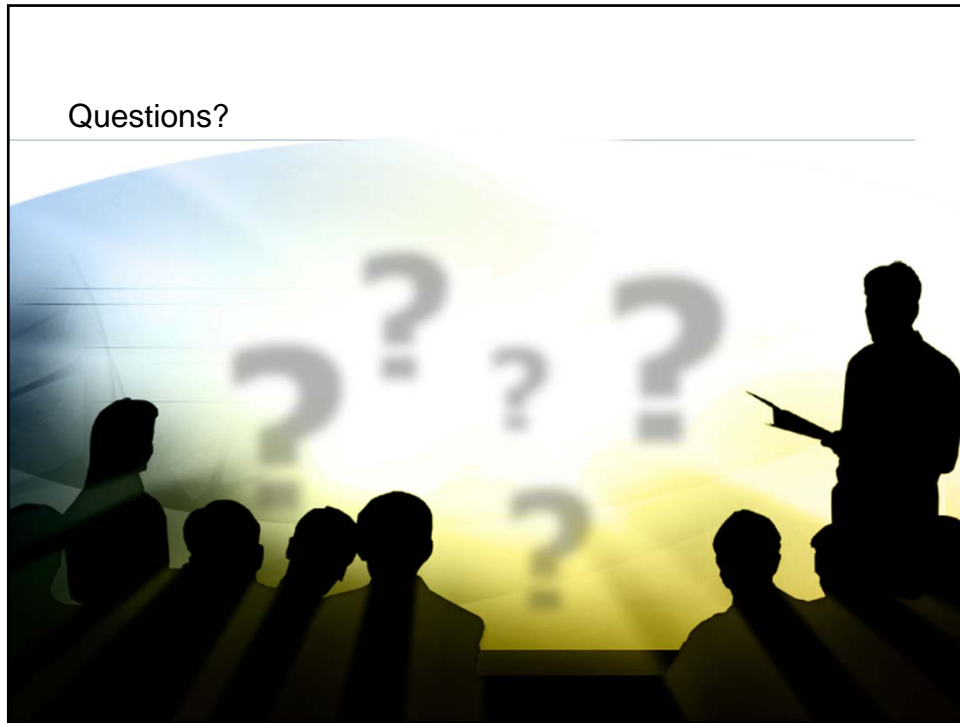
### Next Steps – How to Prepare for 3.0 (Cont'd)

---

- Ensure security alerts (FIM/IDS/etc.) are integrated into incident response process (11.5.1)
- Verify that remote access timeouts are working properly (12.3.8)
- Verify that risk assessments are performed both annually and after significant changes to CDE are made (12.2)
- Ensure separation of duties exists for information security (12.4.1)
- Review and update the incident response plan (12.10)

AGIO

57



## PCI Security Awareness Training

---

Thank you!

Agio has performed network and application security assessments for over 14 years. Agio is recognized by the Payment Card Industry Security Standards Council (PCI SSC) as both a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV).

We are happy to help you with any and all compliance efforts.

919 380 7979

Agio | [agio.com/security](http://agio.com/security)

**AGIO**

59

## Contact Us

---

**Sherry Worthington**

*Account Manager*  
[sherry.worthington@agio.com](mailto:sherry.worthington@agio.com)

**Laurie Leigh**

*Director of Sales*  
[laurie.leigh@agio.com](mailto:laurie.leigh@agio.com)

**Shawn Ryan**

*Senior Security Engineer and Lead  
QSA*

**Agio**

909 Aviation Parkway, Suite 600  
Morrisville, NC 27560  
phone 919 380 7979  
fax 919 380 9055  
web [www.agio.com/security](http://www.agio.com/security)

AGIO

60