Realities of Being PCI Compliant

Miguel (Mike) O. Villegas

CISA, CISSP, GSEC, CEH, QSA, PA-QSA, ASV

Vice President- K3DES LLC

Professional Strategies – S23

Abstract

PCI DSS compliance for merchant payment processing and service provider payment services is not an option. Organizations that store, process or transmit cardholder data need PCI DSS to stay in business. The reality is this comes with a price but there are alternatives that can satisfy PCI DSS requirements.

This session will focus on some of the major realities for achieving compliance related to scope management, merchant level requirements, service provider reliance, limited budgets and management perception.

Not surprisingly, attendees may find some variances in QSA interpretation of the PCI DSS requirements but worth attendance.

The products presented in this session are for informational purposes only and does not reflect an endorsement or recommendation on the part of the presenter. Attendees are advised to perform their own due diligence in selecting the right solution for their institutions.

Questions To Answer

- Do PCI DSS compliance requirements differ by size or complexity of merchant or service provider?
- Do Qualified Security Assessors (QSAs) differ in approaches for PCI DSS compliance?
- How can I meet compliance on a limited budget?
- How much of the PCI DSS assessment can be done internally?
- How does outsource service provider services affect PCI DSS compliance?
- Does PCI DSS compliance provide assurance that my IT environment is secure?

Table of Contents

- Am I Secure if Compliant?
- Pre-Assessment Activities
- PCI Assessment (Onsite / SAQ)
- Identifying Tool Options (SIEM, FIM, IDS/IPS, AV, Encryption, Two-Factor, Wireless)
- Security Monitoring
- Technology Models
  - Vendor Solutions (payment apps)
  - Open Source (risks vs cost)
  - Managed Services (cloud, colocations)
- PCI DSS version 3.0 Overview
- Working with QSAs
- Maintaining Compliance
- Preparing for Next Year's PCI Assessment

Absolute Security Does Not Exist

But We Still Put in Controls

- Alarms
- Locks
- Sensors
- Video Cameras
- Guard Dogs
- Alert Authorities
- Insurance
- Security Awareness
- Training
- Contingency Procedures
- Stay informed / trained

What Has Changed?

- Technology
- User Technical Skillset (CBOK)
- Teenage Hackers to Nation State Backed Hackers
- Ubiquitous Mobile Technology (PC/Smart Phone/Pads)
- Cyberlaws / Cybercrime
- Strict Standards Compliance
- Everything talks to everything
- Multi-Platform/Multi-System/Multi-Application/ Multi-User Environments
- Security Software: AV, ESM, Layer 3 security devices (FW/ Router/Switches), WAF, DLP (Network/DB/EndPoint), FIM, IDS/IPS, SIEM, MDM

Security Basics

"Data security refers to protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction."

-James Martin (1973 – "Security, Accuracy and Privacy in Computer Systems")

"Data security is the protection of data from accidental or malicious modification, destruction, or disclosure."

-Official (ISC)2 Guide to the CISSP Exam (2012)

PCI DSS v3.0 Overview

- Provided a new PCI DSS Template for the Assessment. It will be easier to use and QA. Removed references to “In Place”, “Not In Place” and “Target Date/ Comments”.
- Updated language in requirements and/or corresponding testing procedures for alignment and consistency.
- Enhanced testing procedures to clarify level of validation expected for each requirement.
- Aligned language between requirement and testing procedures for consistency.
- 1.1.2 Clarified what the network diagram must include and added new requirement at 1.1.3 for a current diagram that shows cardholder data flows.
- 2.4 New requirement to maintain an inventory of all system components in scope for PCI DSS.
- 3.6.x Added testing procedures to verify implementation of cryptographic key management procedures.
- 5.1.2 New requirement to evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.

PCI DSS v3.0 Overview

- 6.3 Added a note to clarify that the requirement for written software development processes applies to all internally-developed software and bespoke software.
- 6.5.6 New requirement for coding practices to document how PAN and SAD is handled in memory. *Effective July 1, 2015*
- 6.5.11 New requirement for coding practices to protect against broken authentication and session management. *Effective July 1, 2015*
- 8.3 Clarified requirement for two-factor authentication applies to users, administrators, and all third parties, including vendor access for support or maintenance.
- 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.
- New requirements to protect point-of-sale devices that capture payment card data from tampering or unauthorized modification or substitution. *Effective July 1, 2015*

PCI DSS v3.0 Overview

- 10.6.x Clarified the intent of log reviews is to identify anomalies or suspicious activity, and provided more guidance about scope of daily log reviews. Also allowed more flexibility for review of certain logs events periodically, as defined by the entity's risk management strategy.
- 11.2.1 Clarified that quarterly internal vulnerability scans include rescans as needed until all "high" vulnerabilities (as identified by PCI DSS Requirement 6.1) are resolved, and must be performed by qualified personnel.
- 11.3 New requirement to develop and implement a methodology for penetration testing. *Effective July 1, 2015. PCI DSS v2.0 requirements for penetration testing must be followed until then.*
- 11.3.4 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.
- 12.4.1 New requirement for information security responsibilities to be assigned such that separation of duties is maintained for security functions.
- 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.

Pre-Assessment Activities

Task
➢ Review Last Years Report of Compliance (ROC) and supporting documentation
➢ Review Last Years Timetable Events to Plan for This Year's Assessment
➢ Review/Update the latest versions of PCI inventories
➢ Reconfirm merchant and service provider level
➢ Determine whether organization will use outside assistance or keep in-house
➢ Initial meeting with QSA for planning and approach to assessment
➢ Identify if any process changes affect assessment ➢ Business ➢ Technical
➢ Confirm Scope of PCI DSS assessment ➢ Internally ➢ With QSA/ISA

Scope Creep – Too Many Controls?

Pre-Assessment Activities

Task

- Confirm PCI DSS organizational responsibility
  - Establishing a person or group responsible for PCI DSS compliance
  - Defining team members or groups with clear PCI DSS responsibilities
    - Management
    - In-Scope Business Units
      - Data Owners
      - Process Owners
- Assign or any additional Support Groups for PCI
  - Infrastructure Groups
  - Applications Development Groups
  - Database Administrators
  - System Administrators
  - Access Control Administrators
  - Information Security / IT Security
  - Legal
  - Third-Party/Vendor Relationship Manager
  - Human Resources
  - Internal Audit
  - Compliance Group(s)

Pre-Assessment Activities

Task

➢ Diagrams and Narratives
  ➢ Update Data Flow Diagrams
  ➢ Update Network Diagrams

➢ Reconfirm the PCI DSS reporting requirements based on merchant and service provider level by card brand and overall PCI SSC requirements
➢ Maintain PCI evidence repository updated for next assessment
➢ Maintain recurring management communications

PCI Assessment (Onsite / SAQ)

Task

- PCI DSS has always required evidence for PCI assessment, whether it is based on On-Site QSA assessment or SAQ (Self-Assessment Questionnaire)
- Establishing a PCI DSS compliance monitoring tool or process
  - GRC Tool
  - In-House Developed (web-based, Sharepoint, etc.)
  - Excel Spreadsheets
- Maintain inventory of all PCI in-scope entities
  - Network Devices
    - Firewalls
    - Routers
    - Switches
    - Other Layer 2/3 devices
  - Databases
    - Store PAN data
    - Data tables that contain PAN data
  - Servers
    - Server component types (web, appl, file, db, etc.)
    - Folders that house PAN data (file shares, archives, etc.)
  - Applications
    - Payment applications (PA-DSS)
    - Payment applications that are not PA-DSS
    - In-House payment application
    - Other apps that display or handle PAN data

PCI Assessment (Onsite / SAQ)

Task	
➢ Security Applications ➢ Active Directory / LDAP (spell out) ➢ External Security Managers (ESMs) ➢ RACF/ACF2/TopSecret ➢ Safeguard (Tandem) ➢ Linux	
➢ Maintain/Perform required scans or after significant changes	
➢ Scanning of PAN data ➢ File Shares ➢ Workstations ➢ Servers (application, file servers, etc.) ➢ Mobile devices (including backups) ➢ Mailboxes (including backups, local PSTs) ➢ Logs	➢ Databases ➢ Audio/Recording Transcript Systems (if it has meta data) ➢ Sample devices that should not have PAN data ➢ Document scanning for Linux devices from a Windows based scanner (NFS or SMB)

PCI Assessment (Onsite / SAQ)

Task

- Identify ASV for external vulnerability scans
- Identify external third party for internal vulnerability scans or whether they will be performed in-house
- Quarterly External Vulnerability Scan – Pass
- Quarterly Internal Vulnerability Scan – Pass (as defined in 6.2)
- Identify external/internal penetration tester (third party or independent internal pen tester)
  - Third-party is not required to be an ASV
  - Skilled to perform pen test
  - Independent of processes pen tested
  - All exploitable vulnerabilities need to be remediated and retested
- Identify web application vulnerability testing approach
  - External web application vulnerability test
  - Internal web application vulnerability test
- Quarterly Wireless Scans (rouge APs, Peer-to-Peer APs, unauthorized bridges)
  - Physical walkthroughs
  - Vendor Wireless Management Systems
  - Ongoing scans

PCI Assessment (Onsite / SAQ)

Task
➢ Determine whether PCI DSS required processes are in place
➢ Policies ➢ List of policies ➢ Current / Approved
➢ Baselines ➢ Need to be based on Industry Best Practices (CIS, NIST, etc.) ➢ Current
➢ Hardening Guidelines ➢ Layer 2/3 (network) ➢ Servers ➢ Workstations / Laptops / Mobile

PCI Assessment (Onsite / SAQ)

Task

➢ Risk Assessment
  ➢ Current / Approved
  ➢ Formal Annual Process
  ➢ Standardized Methodologies (ISO, NIST)

➢ Incident Response
  ➢ IR Plan
  ➢ IR annual testing and results
  ➢ Maintain incident documentation for past incidents

➢ Security Awareness Plan
  ➢ Current / Relevant
  ➢ Evidence that plan is being executed
➢ Confirmation of Employee Acceptable Use Agreements
  ➢ Evidence
  ➢ Annual

➢ Data Retention Plan
  ➢ Retention Plan
  ➢ Evidence of Data Retained and Disposed of Beyond Retention Date
➢ Media Disposal Plan
➢ Retired media disposal (degauss, destruction firm, etc.)

PCI Assessment (Onsite / SAQ)

Task
➢ Encryption
➢ Encryption and Key Management ➢ What is encrypted ➢ How (algorithm / standard) ➢ Key management
➢ Key Custodian Agreements (Annual)
➢ Disk Encryption
➢ Retail Site Visits
➢ Router/Lan Room
➢ Storage of Card Receipts
➢ Physical security
➢ PAN data disposal / storage (receipts, reports, etc.)
➢ Workstation / Register controls

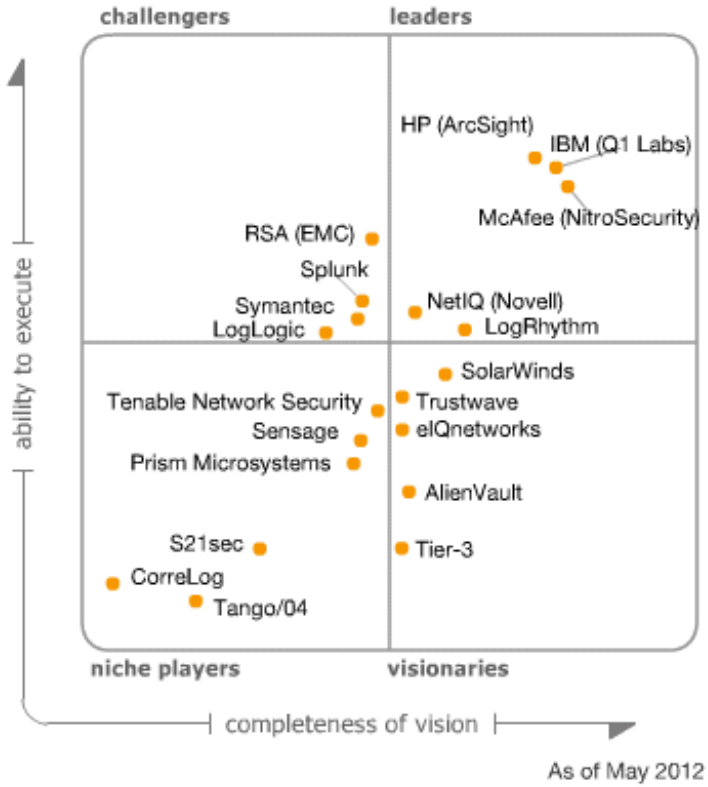
Monitoring Tools

Task
➢ SIEM ➢ File Integrity Monitoring
➢ IPS/IDS
➢ WAF
➢ Database Monitoring
➢ Two-Factor Authentication
➢ Hard Tokens
➢ Soft Tokens
➢ Network Monitoring
➢ TLS/SSL/EV
➢ Data Loss Prevention (DLP)

Magic Quadrant

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2012)

A GOOD START

- Gardner Magic Quadrant
- Forrester Wave

DON'T BUY A CADILLAC
IF
A CHEVY TRUCK WILL DO

“Some” Vendor’s Approach

Security Information & Event Monitor (SIEM)

COMMERCIAL

OPEN SOURCE

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

File Integrity Monitoring

COMMERCIAL

tripwire

NNT WORKPLACE SOLUTIONS

LogRhythm

NetIQ.

nCircle a Tripwire company

Trustwave®
(For End-User Computing Only)

cimtrak detecting the unknown

IBM

PowerTech your security expert

OPEN SOURCE

TRIPWIRE

OSSEC

AIDE

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

IDS/IPS

COMMERCIAL

Check Point SOFTWARE TECHNOLOGIES LTD.

cisco

enterasys Secure Networks

TippingPoint

IBM

JUNIPER NETWORKS

McAfee

nitrosecurity

radware

SOURCEfire

STONESOFT

OPEN SOURCE

OSSEC

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

Web Application Firewalls

COMMERCIAL

OPEN SOURCE

ESAPI Web Application Firewall (ESAPI WAF)

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current attack vendors

Database Monitoring

COMMERCIAL

OPEN SOURCE

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

Two-Factor Authentication

- Multi-factor authentication (also Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors
  - Something I know
  - Something I have
  - Something I am

EMC²

- RSA SecurID

PhoneFactor

PhoneFactor offers instant integration with a wide range of applications, including all leading remote access VPN solutions, single sign-on systems, cloud applications, online banking, and websites as well as custom applications. PhoneFactor also integrates with Active Directory and LDAP servers for centralized user management.

Networking Monitoring

- **A detailed analysis of vulnerabilities** found within your IP addresses or domain, classified by High, Medium or Low severity
- **Step-by-step instructions on how to remediate threats**, so you can immediately address the most serious vulnerabilities

Data Loss Prevention

- Detect, block or control the usage of (for example, saving, printing or forwarding) specific content based on established rules or policies.
- Monitor network traffic for, at a minimum, e-mail traffic and other channels/ protocols (HTTP, IM, FTP) and analyze across multiple channels, in a single product and using a single management interface.
- End-Point / Network / Discovery

Technology Models

- Both Merchants and Service Providers can opt to use the following technology model for IT
  - Vendor Solutions (payment apps)
  - Open Source (risks vs cost)
  - Managed Services (cloud, colocations)
  - In-House developed

PCI DSS v3.0 Overview

- Provided a new PCI DSS Template for the Assessment. It will be easier to use and QA. Removed references to “In Place”, “Not In Place” and “Target Date/ Comments”.
- Updated language in requirements and/or corresponding testing procedures for alignment and consistency.
- Enhanced testing procedures to clarify level of validation expected for each requirement.
- Aligned language between requirement and testing procedures for consistency.
- 1.1.2 Clarified what the network diagram must include and added new requirement at 1.1.3 for a current diagram that shows cardholder data flows.
- 2.4 New requirement to maintain an inventory of all system components in scope for PCI DSS.
- 3.6.x Added testing procedures to verify implementation of cryptographic key management procedures.
- 5.1.2 New requirement to evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.

PCI DSS v3.0 Overview

- 6.3 Added a note to clarify that the requirement for written software development processes applies to all internally-developed software and bespoke software.
- 6.5.6 New requirement for coding practices to document how PAN and SAD is handled in memory. *Effective July 1, 2015*
- 6.5.11 New requirement for coding practices to protect against broken authentication and session management. *Effective July 1, 2015*
- 8.3 Clarified requirement for two-factor authentication applies to users, administrators, and all third parties, including vendor access for support or maintenance.
- 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.
- New requirements to protect point-of-sale devices that capture payment card data from tampering or unauthorized modification or substitution. *Effective July 1, 2015*

PCI DSS v3.0 Overview

- 10.6.x Clarified the intent of log reviews is to identify anomalies or suspicious activity, and provided more guidance about scope of daily log reviews. Also allowed more flexibility for review of certain logs events periodically, as defined by the entity's risk management strategy.
- 11.2.1 Clarified that quarterly internal vulnerability scans include rescans as needed until all "high" vulnerabilities (as identified by PCI DSS Requirement 6.1) are resolved, and must be performed by qualified personnel.
- 11.3 New requirement to develop and implement a methodology for penetration testing. *Effective July 1, 2015. PCI DSS v2.0 requirements for penetration testing must be followed until then.*
- 11.3.4 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.
- 12.4.1 New requirement for information security responsibilities to be assigned such that separation of duties is maintained for security functions.
- 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.

Working with QSAs

- PCI states that the QSA determine the scope of the PCI DSS assessment, especially if client is using **tokenization**
- Schedule kick-off meeting to determine documentation requested is ready when QSA arrives including logistics
- QSA should tell you if there are any PCI requirements that have changed since last year's assessment and its impact
- Provide QSA information and documentation on any business model, infrastructure or application changes within PCI scope
- If a new QSA from the same firm, make sure the transition is smooth and determine impact to timing and documentation required
- Schedule quarterly reviews with QSA to ensure continued communication

Maintaining Compliance

- Whether the merchant or service provider, regardless of the level, and whether they have a ROC or SAQ
- Integrate PCI DSS into the business culture
- Deliver periodic (monthly) PCI DSS compliance posture to executive management
- Review PCI impact prior to infrastructure or business model changes
- Stay in communication with QSA and solicit input whenever major changes are planned
- Stay informed on PCI SSC announcements / guidances
- Maintain periodic required scans/reviews current
- Maintain required documents current (policies, network diagrams, acceptable use agreements, etc.)

PCI Scheduled Activities

Frequency	PCI Control	Activity
Annually	3.6.4	Periodic cryptographic key changes: • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually
Annually	6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. • Installing a web-application firewall in front of public-facing web applications.
Annually	9.5	Store media back-ups in a secure location, preferably an off-site facility such as an alternate or backup site or a commercial storage facility. Review the location's security at least annually.
Annually	9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.
Annually	11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.
Annually	12.1.2	Annual process that identifies threats, vulnerabilities, and results in a formal risk assessment.
Annually	12.1.3	Perform a Security Policy review at least once a year and update when the environment changes.
Annually	12.6.1	Educate employees upon hire and at least annually.
Annually	12.6.2	Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.
Annually	12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually
Annually	12.9.2	Test Incident Response Plan at least annually.

PCI Scheduled Activities

Frequency	PCI Control	Activity
Bi-annually	1.1.6	Review firewall and router rule sets at least every six months.
Quarterly	3.1	Review, at least quarterly, retained data to verify that stored cardholder data does not exceed requirements defined in the data retention policy.
Quarterly	6.1	Install less critical devices and system updates within three months.
Quarterly	8.5.5	Remove/disable inactive user accounts at least every 90 days.
Quarterly	8.5.9	Change user passwords at least every 90 days.
Quarterly	9.1.1.	Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
Quarterly	10.7	Ensure that three months of audit logs are immediately available for review.
Quarterly	11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploy a wireless IDS/IPS to identify all wireless devices in use.
Quarterly	11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

PCI Scheduled Activities

Frequency	PCI Control	Activity
Monthly	6.1	Install critical security patches within one month of release.
Weekly	11.5	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.
Daily	10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
Daily	12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).
Immediately	8.5.3	Set first-time passwords to a unique value for each user and change immediately after the first use.
Immediately	8.5.4	Immediately revoke access for any terminated users.
Immediately	12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.

Summary

Challenges	What To Do
QSA Firm	Chose those who have implemented not just audited
ASV Firm	Need internal skills for remediations
Pen Testing	Need internal skills for internal pen test
Security & Monitoring	Even if outsourced, merchant/SP still responsible
Secure Code/WAF	OWASP/NIST – WAF (Tap or SPAN Port)
Segmentation	Could be significant cost, skills, hardware, maintain
Payment Applications	PA-DSS or in-house developed (biggest challenge)
CSIRT	Time consuming and costly (annually)
Encryption	Annual master key change procedures (execute)
FIMs	Picking the right FIM. Cadillac vs Chevy
Mainframes	Don't assume OK just because it's mainframe

BIO

Miguel (Mike) O. Villegas is a Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/ IEC 27001:2005 program. Mike was previously Director of Information Security at Newegg, Inc. for five years.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC and CEH. He is also a QSA, PA-QSA and ASV as Director for K3DES.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 15 years.