ISACA®

Trust in, and value from, information systems

San Francisco Chapter

S33 – Rethink PCI DSS Compliance

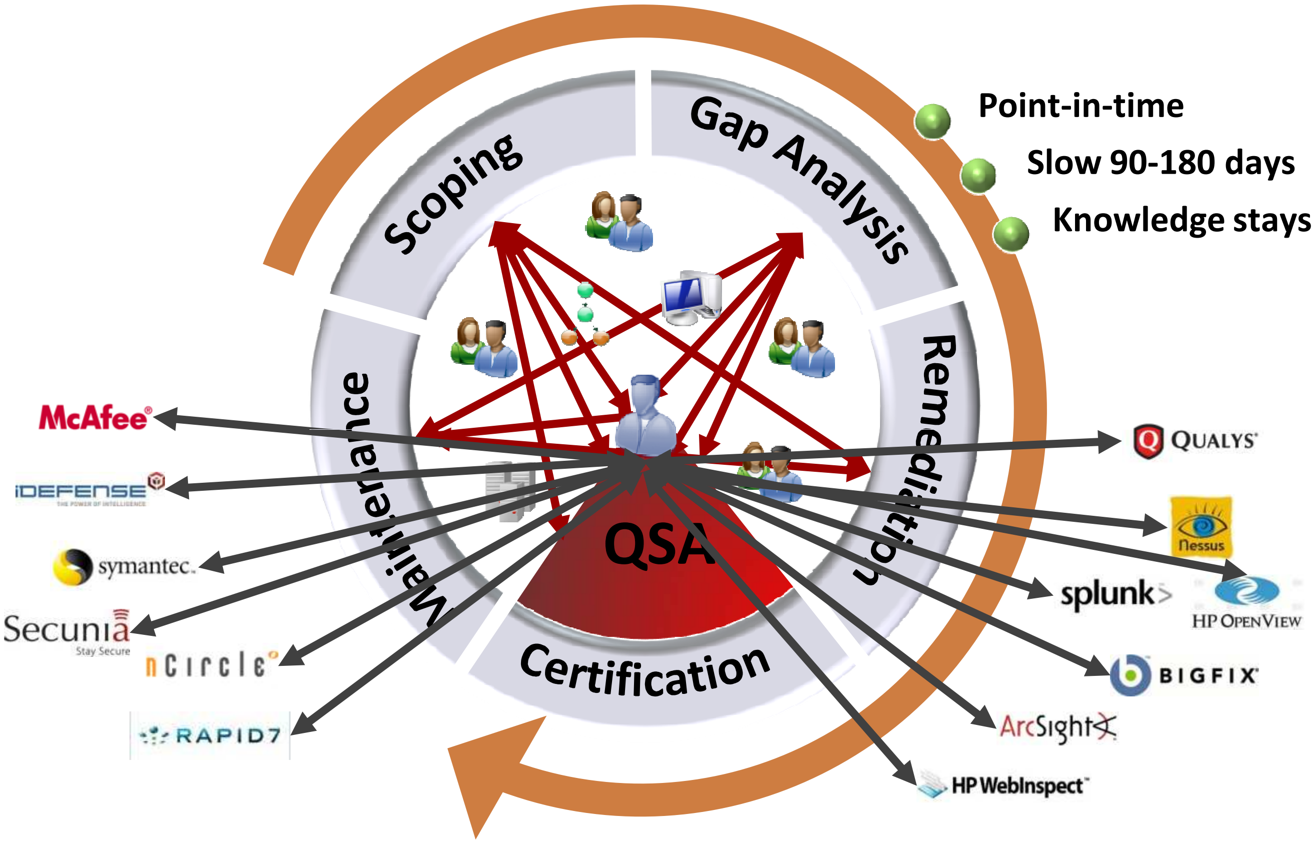
Shifting to a Life Cycle Management Approach

Presented by Arti Raman and Nigel Tranter

Agenda

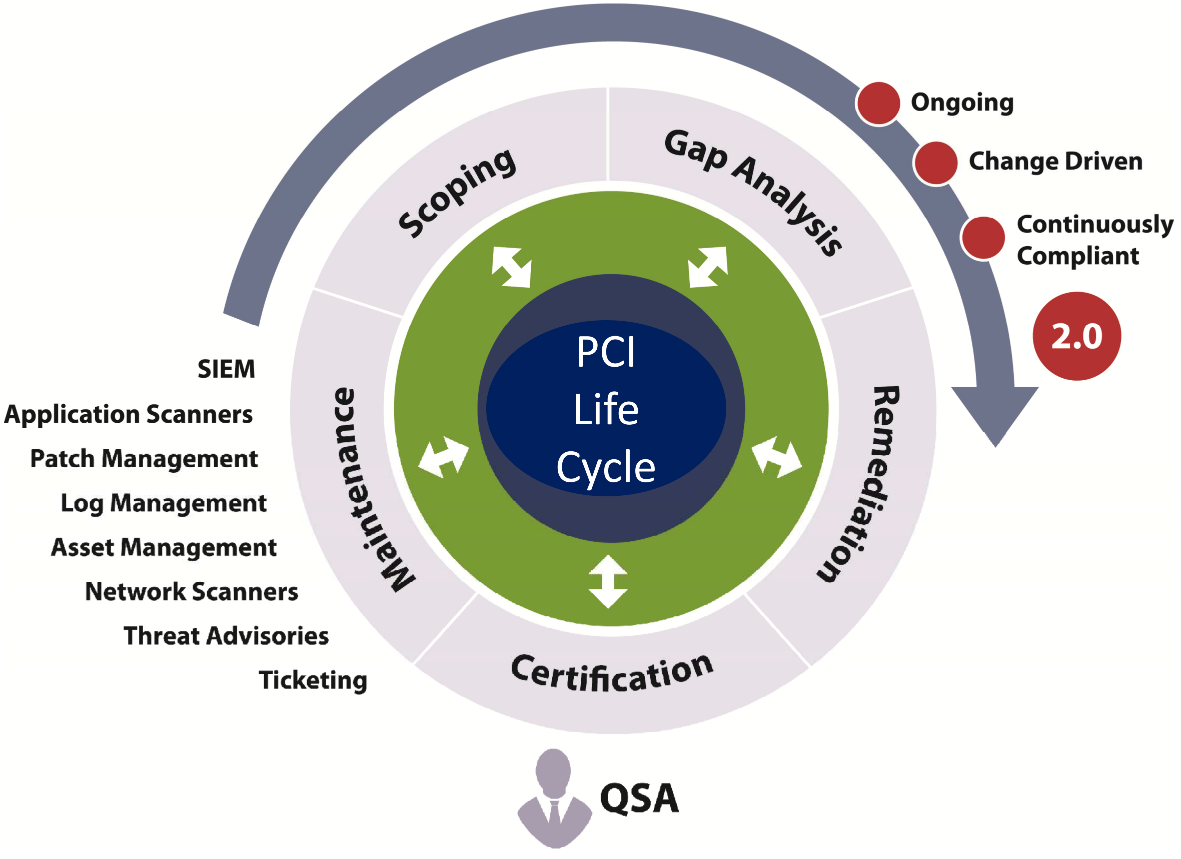
- PCI DSS Challenges
- PCI and its Principles
- Key Changes in PCI DSS 2.0
- Scoping Under PCI DSS 2.0
- PCI DSS 2.0 and Impacts on IT Operations
- PCI DSS 2.0 and Impacts on Security Operations
- Managing PCI DSS as a Life Cycle
- Case Study: bwin

Today's Takeaways



- Point-in-time
- Slow 90-180 days
- Knowledge stays with QSA

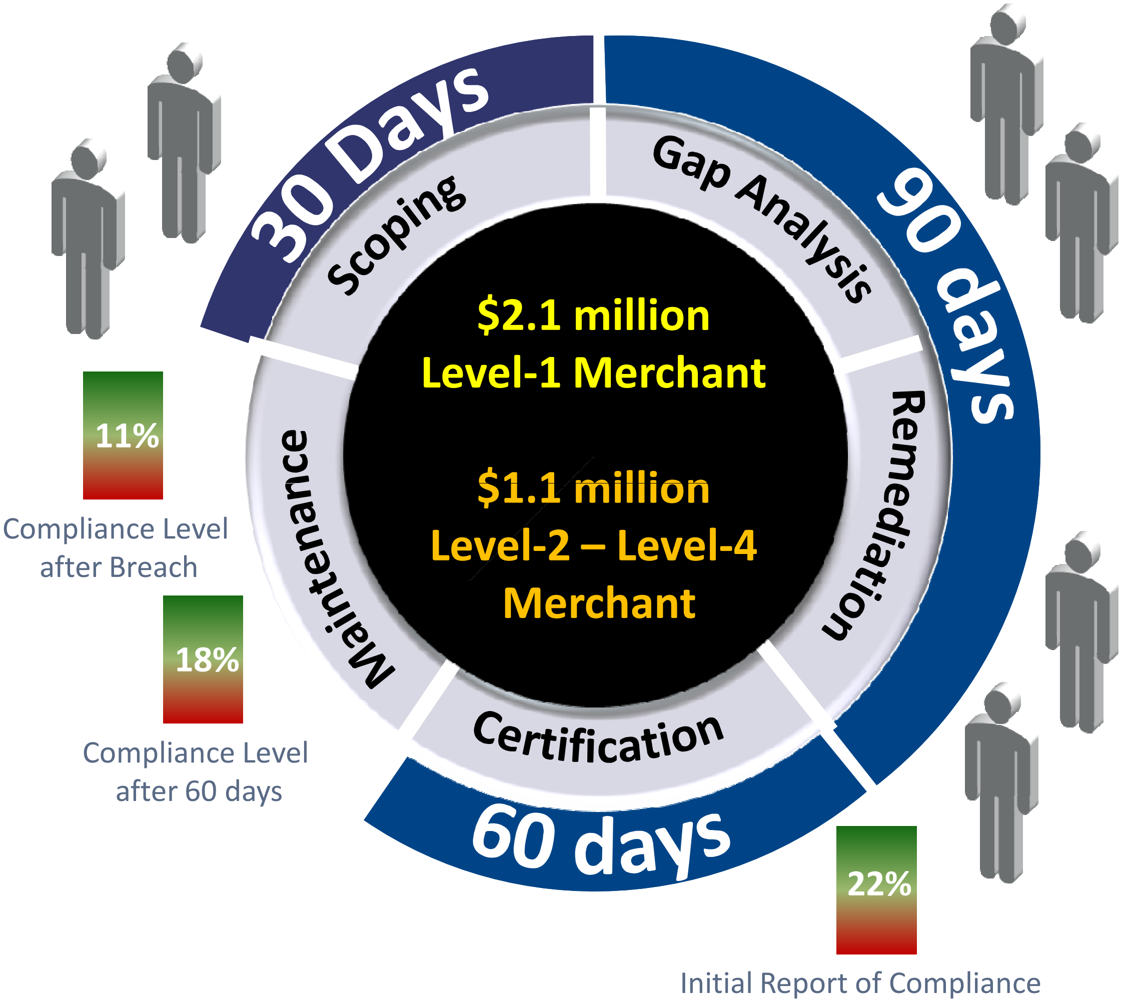
Today’s Takeaways (continued)



Today’s Takeaways (continued)

- Establish the challenges of managing PCI DSS
- Discover key changes in PCI DSS 2.0
- Begin to understand how these changes may impact your organization
- Learn how to think about a life cycle management program when it comes to PCI DSS 2.0

PCI DSS Challenges



- Costly
- Project-driven
- Resource intensive
- Slow (up to 180 days)
- Point-in-time
- Low compliance levels
- Knowledge stays with auditor
- Creates audit fatigue
- Pressure from card brands

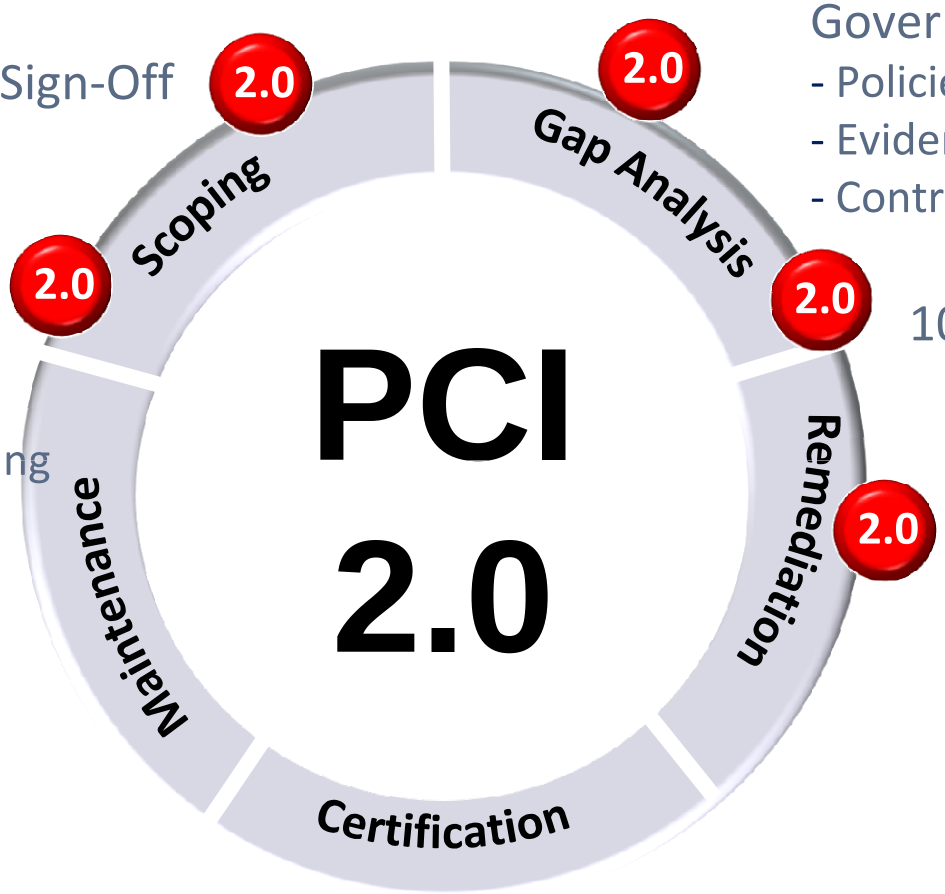
Sources: Verizon 2010 Payment Card Industry Report, Gartner Survey: PCI Compliance Activity Shifts Downstream as Aggressive Enforcement Continues, Gartner, June 2011

PCI and its Principles

The core of the PCI DSS is a group of principles and accompanying requirements around which the specific elements of the standard are organized. There are 12 such principles in the standard.

1. Firewall Configuration
2. Vendor-Supplied Defaults
3. Stored Cardholder Data (CHD)
4. Transmission of CHD
5. Anti-Virus Software
6. Secure Systems / Applications
7. CHD Access Restrictions
8. Unique IDs
9. Physical Access Control
10. Logical Access Control
11. Security Testing
12. IT Security Policy

Key Changes in PCI DSS 2.0



QSA Sign-Off

Governance
- Policies and controls
- Evidence of execution
- Controls for virtualized assets

Virtual Assets
- Mapping to PCI
- Evidence
- Method for scoping

100% Asset Coverage

Risk Correlation
- Risk model for tolerance and mitigation
- Risk-based remediation prioritization
- Automated evidence collection

Scoping Under PCI DSS

Process

- Identify demarcation of responsibility
- Identify points of interaction
- Identify cardholder data flows throughout the organization

Objectives

- Find people handling cardholder data
- Understand processes
- Find technology

Savage Chickens
by Doug Savage
I NEED TO TALK TO YOU ABOUT PROCESS IMPROVEMENT
OK. JUST FILL OUT THIS "IMPROMPTU CONVERSATION PROPOSAL" FORM
©2007 BY DOUG SAVAGE
www.savagechickens.com

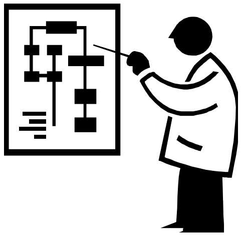
Scoping: Identify Points of Interaction

- Capture all points of interaction
  - ✓ Card brand
  - ✓ Payment type
  - ✓ Transaction type

- Full life cycle and all card handling steps
  - ✓ Reconciliation
  - ✓ Adjustments
  - ✓ Disputes
  - ✓ All

Scoping: Identify Cardholder Data Flow

- Most difficult and time consuming
- For defined point of interaction
  - ✓ Use network equipment to identify and sniff traffic
  - ✓ Define flow through all networked system components
  - ✓ Identify manual processes
    - ▪ Include name of the individual
    - ▪ Job function or role
    - ▪ Document procedures
  - ✓ Capture evidence on data flows
    - ▪ “tcpdump” or PCAP files for network
    - ▪ CC data discovery tools on servers and hosts
  - ✓ Draw clear diagram and report



Scoping Under PCI DSS 2.0

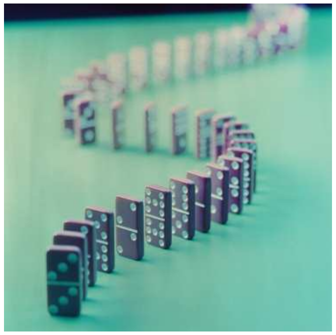
Change in approach and responsibilities:

“At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope.”

Scoping Section, PCI DSS 2.0

Scoping Under PCI DSS 2.0 (continued)

- Process (as stated in PCI DSS 2.0)
  - ✓ The assessed entity identifies and documents the existence of all cardholder data (CHD) in their environment
  - ✓ Once all locations of CHD are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (e.g., results may be a diagram or inventory of CHD locations)
  - ✓ The entity considers any CHD found to be in scope of the PCI DSS
  - ✓ The entity retains documentation that shows how PCI DSS scope was confirmed and the results



Scoping Under PCI DSS 2.0 (continued)

- Entity assertion
  - ✓ The entity defines scope
  - ✓ Entity must also explain and define segmentation
  - ✓ Entity must have evidence that fully supports conclusions (such that 12 people selected at random would agree with conclusion)

- The Qualified Security Assessor (QSA) is required to review and reference results documented by entity in last bullet

PCI DSS 2.0 and Impacts on IT Operations

- Expansion of Existing Requirements
  - ✓ Testing procedures replace bulleted items
  - ✓ Rewording of test procedures to address new issues
  - ✓ Limits on sampling for actual testing
- Redefinition of Past Requirements
  - ✓ *Clarification* of definitions for terms included in standard
  - ✓ Greater emphasis on people and processes
- New Requirements
  - ✓ Inclusion of new risk-based approach across several requirements
  - ✓ Introduction of metrics to evaluate vulnerabilities

IT Impacts: Stored Data Protection

Requirement	Impact
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)	Inclusion of “chip equivalent data” will impact processes related to RFID, NFC, and EMV
3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms	Exhaustive identification of location for encryption key storage
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod	Establishment of cryptoperiod based on industry standard and implementation of processes for that cryptoperiod

IT Impacts: User Authentication

Requirement	Impact
8.3 Incorporate two-factor authentication for remote access	Not new. Missing reference to “individual certificates”, implies that actual two-factor authentication mechanism is required

IT Impacts: Logging

Requirement	Impact
10.7.b Verify that audit logs are available for at least one year and processes are in place to *immediately* restore at least the last three months' logs for immediate analysis	One word change sets an expectation on the ability to query and obtain access to three months worth of logs

IT Impacts: Security Testing

Requirement	Impact
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis … must be sufficient to detect and identify any *unauthorized devices*	Significant impact to retailers and companies with multiple locations. Mechanisms to detect "any" unauthorized devices requires significant investment, especially devices connected to USB ports

IT Impacts: Conclusion

- Primary impact appears to affect retailers with multiple sites
- IT Staff and Headcount
  - ✓ Scoping and segmentation:
    - ▪ 5 to 8 days for SME organization, service providers, and e-tailers; up to 20 man days to complete for retailers
- Readiness
  - ✓ CAPEX for upgrades to networking equipment and infrastructure
- Assessment
  - ✓ Collection of evidence for assessment can be twice as long as prior years
  - ✓ Reporting requirements on QSA mandate requires a large amount of additional information to be captured
  - ✓ Budget is 2 - 3x higher than prior year’s engagement

PCI DSS 2.0 and Security Operations

"Securing information assets is not achieved by passing PCI DSS"

→ Constant maintenance and vigilance required

- ✓ 79% of breached companies are not in compliance with PCI
- ✓ 86% had evidence of breach in log files
- ✓ 61% of cases were discovered by external, third-party
- ✓ 96% avoidable through operational security controls

Security Operations as the “Long Pole”

“Focus activities on security, compliance will happen as a result”

→ The IT security dividend

- ✓ Improved reliability of systems
- ✓ Greater availability
- ✓ Easier maintainability
- ✓ Trust through integrity
- ✓ Confidence through privacy

Routine Security Controls under PCI DSS 2.0

Control	Requirement	Frequency
1.1.6	Review router and firewall configurations	Every 6 months
3.1	Audit that stored data does not exceed retention period	Quarterly
3.6.4	Rotation of encryption keys	Annual
9.9.1	Media inventory	Annual
10.6	Review of logs	Daily
11.1	Wireless Analyzer testing	Quarterly
11.2.a	Internal network, host and application scans	Quarterly or after change
11.2.b	External "ASV" scans	Quarterly or after change
11.3	Internal and external penetration testing	Annual or after change
11.5	Review of file integrity monitoring events	Weekly

Routine Security Controls under PCI DSS 2.0

Control	Requirement	Frequency
12.1.2	Risk assessment	Annual
12.1.3	Review of policies	Annual
12.6.1	Security awareness training	Annual
12.9.2	Incident response testing	Annual

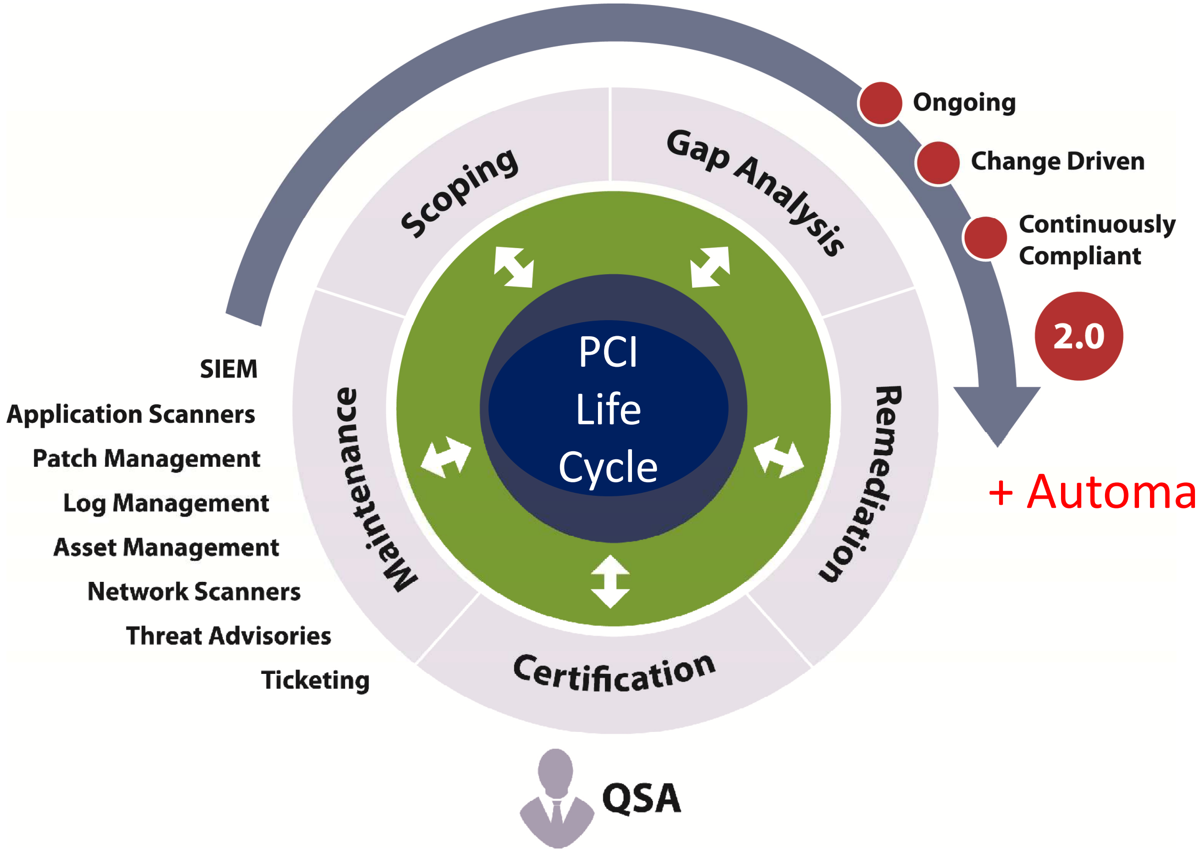
Routine Security Controls under PCI DSS 2.0

Control	Requirement	Recommended Frequency
6.1	Identification of critical security patches	Weekly, if all sources of patches do not have push notification, like e-mail
6.2	Identification of newly discovered security vulnerabilities	Weekly, if sources of vulnerabilities do not have push (e.g., email) notification
8.5.5	Disable users over 90 days inactive	Monthly, if not automatic within AAA systems
12.8.4	Monitor (downstream) service provider’s PCI DSS status	Quarterly
12.9.4	Train incident first responders	Annually

Importance of Threat and Vulnerabilities

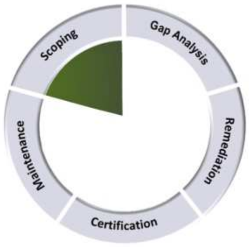
Reference	Description
2.2.b	Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2
10.4.a	Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2
11.2.1b	Review the scan reports and verify that the scan process includes re-scans until passing results are obtained, or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved
11.2.3.b	For internal scans, a passing result is obtained or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved

Managing PCI DSS as a Life Cycle



+ Automation + Collaboration

Automation of Scoping

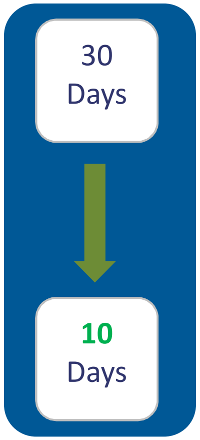


Challenges

- Large asset base, no current inventory
- Asset sharing and hierarchies
- Virtualization
- Scoping process required for PCI 2.0

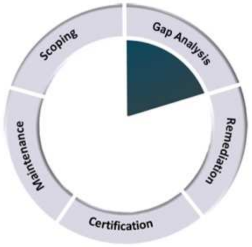
Benefits

- Scalable asset-centric risk management database
- Assess once, comply to many
- Automated scoping triggered by database changes


30 Days

10 Days

Automation of Gap Analysis

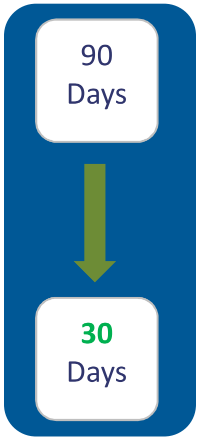


Challenges

- Large number of assessments
- Duplication across assets, assessments, and years
- Large evidence requirements
- Resource intensive and slow

Benefits

- Unlimited automated assessments and control checks
- Pre-built connectors, pre-built surveys
- Reuse across owners, assets, assessments, and years



90 Days

30 Days

Automation of Remediation

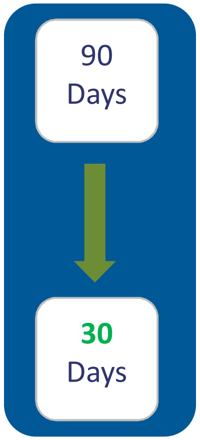
Scoping
Gap Analysis
Remediation
Certification
Maintenance

Challenges

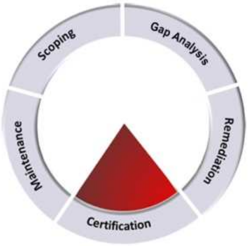
- Large number of evidence requirements
- Special approval for compensating controls
- Risk-based remediation for vulnerabilities

Benefits

- Evidence, incident, and exception management
- Evidence repository mapped to requirements



Streamlining of Certification Process

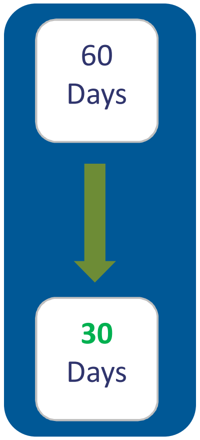


Challenges

- Time and resource consuming
- Project-based with extensive preparation
- Enormous demands for documentation, process and evidence

Benefits

- Current executive and organizational readiness maintained
- Standardized testing procedures, evidence, and documentation


60 Days

30 Days

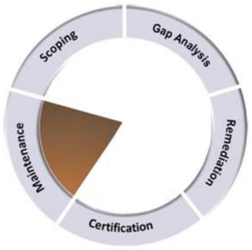
Inclusion of Maintenance Phase

Challenges

- Most commonly overlooked
- Impossible to attain via project-based approach
- Constantly changing CDE and ownership

Benefits

- CDE change triggered continuous scoping
- Scoping triggered automated assessments
- Ongoing gap analysis and remediation



Previously Not Possible

Case Study: bwin

Background

- The world's leading name in online betting and real money gaming
- 2.1 million active customers
- 2.5 billion Euro turnover
- 70,000 payment transactions per day

Benefits

- Reduced PCI compliance certification process from 180 to 60 days

Summary

- Review and understand changes to PCI DSS 2.0
  - ✓ Stay connected
  - ✓ Get opinions on impact of changes
- Perform internal pre-assessment
- Collect and prepare evidence
  - ✓ Obtain collection tools from assessor
  - ✓ Get a head start

- Collect evidence and logs from maintenance controls
- Apply life cycle concept to your PCI compliance process
- Automate all phases of the PCI compliance process
- Don’t wait until it is too late… the clock is ticking.

Questions and Answers

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

http://www.agiliance.com/infocenter/whitepaper.html

Arti Raman
Agiliance Inc.
840 W California Ave., Suite 240
Sunnyvale, CA 94086
USA

araman@agiliance.com

Tony Bates
Payment Software Company, Inc.
1340 South De Anza Blvd., Suite 204
San Jose, CA 95129
USA

tony@paysw.com