What to expect from a PCI QSA led assessment

Fiona Pattinson, CISSP, QSA

Why would you need a QSA assessment?

Does your organization handle credit card information?

- Does it *store* credit card information?

- Does it *process* credit card information?

- Does it *transmit* credit card information?

What is a QSA assessment?

Security Assurance !!!

- Each brand had their own security program and standards
- This meant duplication and some inconsistencies and gave the opportunity for rationalization
- "**All for one and one for all**"
  - **Remove duplication of effort**
  - **Focus resources more effectively**

- PCI SSC was formed to create common standards
- The brand's individual security programs continue

PCI Security Standards Council

The council manages consolidated standards for PCI compliance

- PCI Data Security Standard
- PCI Data Security Standard for Payment Applications
- Requirements for Approved Scanning Vendors

Each of the brands still runs <u>its own security program</u>

- They set different requirements for compliance
  - E.g. When an assessment by an external QSA is necessary
- They all use the same standards

The card brand security programs

Security Program	URL
The MasterCard Site Data Protection Program (SDP)	http://www.mastercard.com/us/sdp/index.html
Visa Cardholder Information Security Program (CISP)	http://usa.visa.com/merchants/risk_management/cisp_overview.html
American Express Data Security Operating Policy Compliance Program (DSOP)	https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=spinfo&ln=en&frm=US&tabbed=complienceRequirement
Discover Information Security & Compliance (DISC)	http://www.discovernetwork.com/fraudsecurity/disc.html
JCB	http://www.jcb-global.com/english/pci/

All use the current version of the PCI DSS (currently 1.2.1)
- available from https://www.pcisecuritystandards.org/index.shtml

Non compliance

- If non-compliant and a breach occurs…

  - *Merchants/Service Providers have liability for the acquirer bank's losses and card re-issuance costs*

  - Fines per incident from Visa (against acquiring bank)

  - Restrictions imposed by card companies (prohibiting future credit card processing)

  - Investigative and Legal costs

  - Repayment of losses may exceed the ability to pay and cause total failure of the organization

- Other potential consequences:
  - Damaged Brand Reputation
  - Invasive media attention
  - Loss of customers

How do you know if you need a QSA?

- For most merchants the requirements will come from your merchant bank or acquiring bank.

- If you take several card brands (e.g. MasterCard, VISA , Discover, JCB and AmEx) then it will likely be the one with the greatest requirements

- Sometimes the rules are different if you have already had a security breach

The compliance requirements

- Requirements for compliance are very complex.
  - Merchant levels. (levels 1-4 are defined by payment brands)
    - Levels are based on transaction volume as determined by Acquiring banks
    - There are exceptions (e.g. if you have had a breach in the past)
  - Service Provider levels (defined by payment brands)
    - Determined by the brand, acquirer, merchant or service provider
- Comply with the PCI DSS
  - Show that you do using an Attestation of Compliance
  - PLUS a completed
    - Self Assessment Questionnaire (SAQ) or
    - A Report of Compliance (ROC)

The compliance requirements

- Secondly everyone **storing, processing or transmitting** card holder data has to comply with the PCI DSS.

  - Depending on the merchant or Service Provider level you will need to demonstrate compliance annually through one of:

    - Completing an Self Assessment Questionnaire (SAQ): There are four different kinds of SAQ from SAQ A to SAQ D or

    - Undergoing an assessment from an external organization accredited by the PCI SSC. These are called Qualified Security Assessors

    - NOTE: Providing proper separation can be employed and conflict of interest avoided, the company may be able to perform it's own assessments using Internal Security Assessors (ISAs) qualified by the PCI SSC.

The 12 requirements of PCI-DSS

Build and Maintain a Secure Network	
1	**Install and maintain a firewall configuration to protect cardholder data**
2.	**Do not use vendor-supplied defaults for system passwords and other security parameters**
Protect Cardholder Data	
3.	**Protect stored cardholder data**
4.	**Encrypt transmission of cardholder data sent across open, public networks**
Maintain a Vulnerability Management Program	
5.	**Use and regularly update anti-virus software**
6.	**Develop and maintain secure systems and applications**
Implement Strong Access Control Measures	
7.	**Restrict access to cardholder data by business need-to-know**
8.	**Assign a unique ID to each person with computer access**
9.	**Restrict physical access to cardholder data**
Regularly Monitor and Test Networks	
10.	**Track and monitor all access to network resources and cardholder data**
11.	**Regularly test security systems and processes**
Maintain an Information Security Policy	
12.	**Maintain a policy that addresses information security – Connected Entities and Contracts**

Some Characteristics of PCI DSS

Some attributes of the PCI DSS that can be used to compare it to other standards

- It is a <u>compliance</u> standard

- PCI DSS is relatively new (PCI DSS 1.0 was December 2004) although the basis : Note that Card Brand standards are older (e.g. VISA 's AIS as part of the CISP since 2001)

- The requirements are based on a risk analysis for the Card Brands

- Risk management process in the standard is not a driver of the controls

Some Characteristics of PCI DSS

- PCI DSS is relatively new …

Timeline:

- 1992 SAS 70
- 1995 BS 7799
- 1996 CoBIT
- 2000 ISO/IEC 17799
- 2001 MasterCard SDP
- 2001 VISA AIS
- 2003 PCI DSS
- 2005 ISO.IEC 27002

1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010
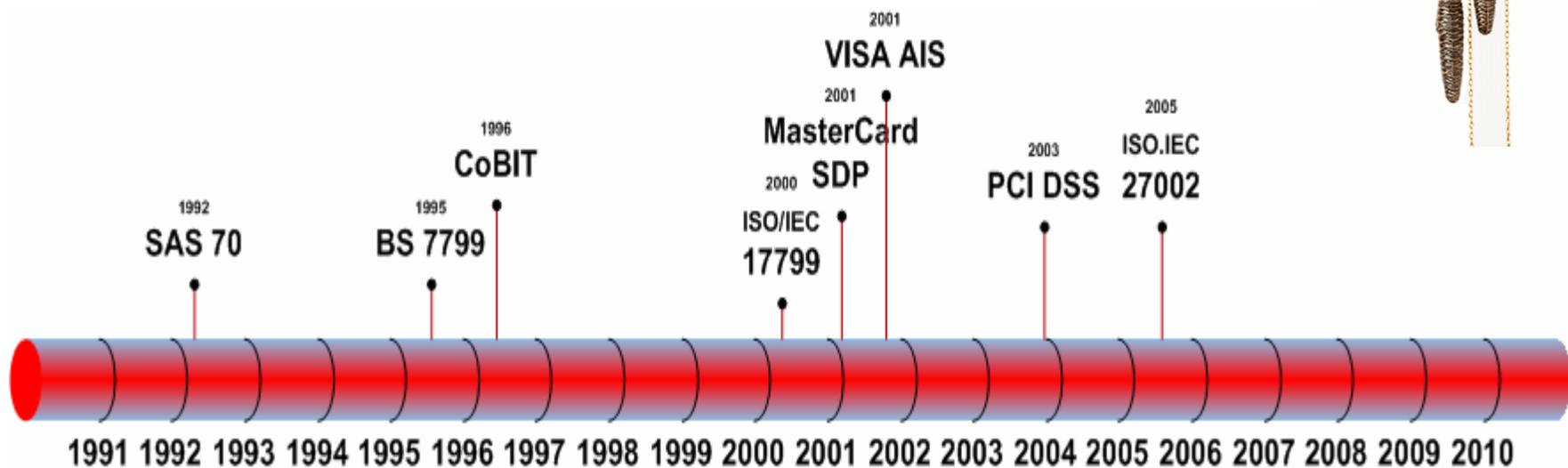
What to expect from a QSA led assessment

Phase 1: Preparation

Scoping → Gap Analysis → Remediation

Phase 2: Formal Assessment

QSA Assessment → Reporting

Phase 3: Maintenance & Monitoring

Monitoring

An Approach for Compliance
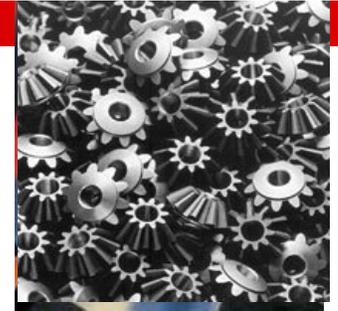
The first time is always the hardest

Build security measurement, and assess-ability into the business processes

Always be ready for an assessment

- A properly prepared organization shouldn't need to do much preparation. They should be ready at ANY time.
- Be aware of changes in the standards.
  - Keep up to date with them.
  - Reviewing for changes once a year - one month before the assessment leads to problems.

An Approach for Compliance

Understand the assessment requirements and how your technology choices supports you in meeting them.

- There may be differences in how controls can be met or interpretations needed for your environment. e.g.:
  - Malware requirements in PCI DSS
 - File Integrity Checking for PCI

Have a GOOD and effective risk management process.

- That matches YOUR organization

Specify compensating controls wisely

- Too many are a red flag: but they are probably necessary!

An Approach for Compliance

Reuse other assessment results

- COBIT, FISMA, ISO/IEC 27001, SAS/70, SOX, etc.

Use assurance given by product certifications:
   Vendors spend a lot of resource and money giving you this assurance

- Common Criteria, FIPS 140-2 etc.

Integrate security management systems:

- Awareness training, HR processes, internal audit of organizational processes and others are common

- BUT each assessor needs to make his or her own determination

Do not reinvent the wheel!

Use it!

Leverage systems

SHARE

Who is involved?

The key people in the subject organization

- Security officer / team – typically lead the project
- IT department
- Developers
- Operations (e.g. call center)
- Management, internal auditors, HR, other relevant departments

Third party providers

- Hosting providers, ISP, Payment Processors, backup providers
- Consultants , expert in PCI compliance (May be the QSA)
- A QSA company
- QSA assessment team

Scoping

- **Work with your QSA to discuss the scope of the assessment**
  - It is the QSA's responsibility to determine the scope
- **Determine the extent of the card holder data environment**
  - Where is sensitive data (PAN and track data) held?
  - Systems, PCs, call center records (voice recordings, videos)
  - Spreadsheets, E-mails, Instant messaging etc?
  - Accounts department? Development department? Test machines?
- **Reduce the scope**
  - Are networks segmented?
  - Is encryption or tokenization used?
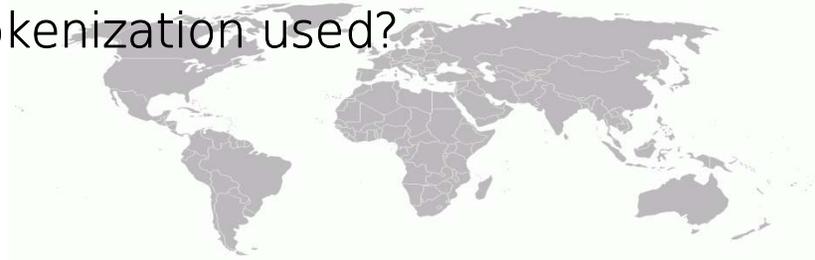
Gap analysis / readiness assessment.

For a first time assessment allow for this to be a significant effort.

For subsequent efforts focus on improvements, efficiencies and maintenance of compliance

May be performed by a QSA or consultant. Note this is not a PCI SSC formal activity – It is performed on a consultancy basis

In order to achieve compliance, be prepared to discuss and implement appropriate:

- compensating controls and

- remediation

Remediation

It happens to all of us!

PCI DSS is a compliance standard

That means there is little leeway for non-compliance. Compensating controls can be considered where reasonable

The costs of remediation depend on how close you are to meeting the standard
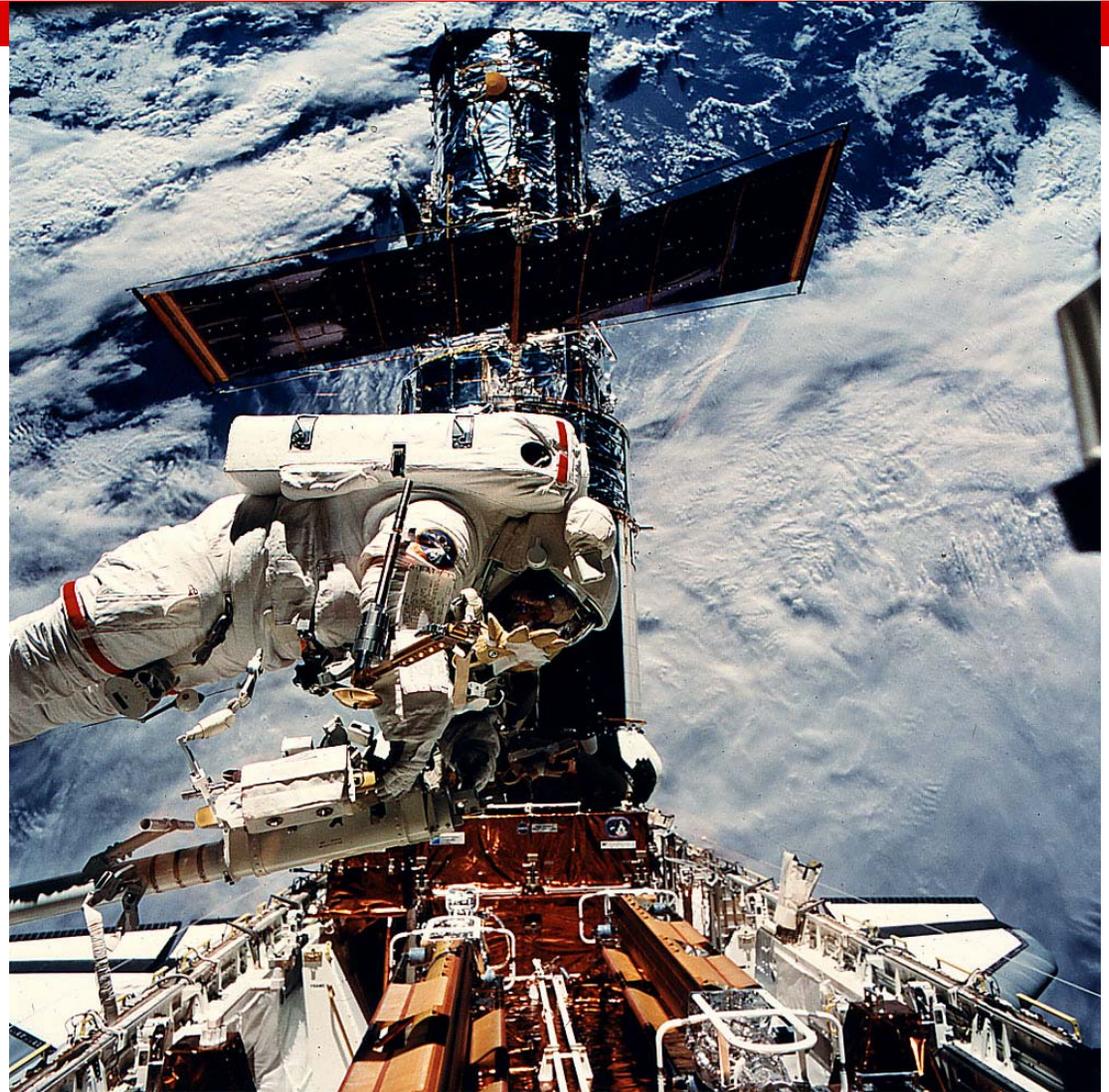
Some things you will need

These are requirements that are often not in place for the first time assessment and often need records showing compliance for a year:

- Quarterly external network vulnerability scanning from an ASV

- Internal and External network penetration tests

  - Annual or after each major change (Consider this if remediation involves significant change.)

- Developer compliance with OWASP or similar programs for security assurance in development processes

Formal assessment

The formal assessment by a QSA will involve:

- Determining sampling methods

- Agreeing compensating controls

- Analysing documentation

  - Process, configuration standards, records etc.
- Reviewing systems and device configurations

- Interviewing

Reporting

A document that is typically very lengthy.

QA processes for the document by the QSA are thorough. Expect this to take some time.

YOUR representative must also have time to read it. They must sign it asserting that :

- the ROC has been reviewed and that no errors or omissions known to the representative are present in the report.
- that all information provided to the QSA is correct and that no relevant information has been withheld from them.

CUSTOMER

Report on Compliance

A QSA led assessment of compliance validation according to the Payment Card Industry Security Standards Council Standards and Security Assessment Procedures

Report Date: 2010-03-26
The assessment remains valid for 12 months
Report Number: XXX-01
atsec information security
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

PCi Security Standards Council ™

QUALIFIED SECURITY ASSESSOR

Version: 1.0
©2010 atsec information security

confidential: REDACTED report

Status: Released
Page 1 of 197

Ongoing Monitoring

- Clarifications

    - merchant/organization clarifies/updates report statements (if applicable) upon bank request

- Further advice and consulting post-assessment

- Preparation for the next annual assessment
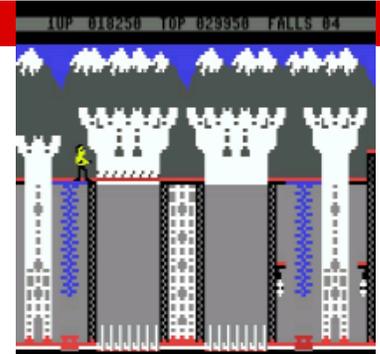
Pitfalls: Choosing Your Assessor

Choosing you assessor (skills and competency)

- Do they have experience with your technology choices?
- Do they understand the additional security built in to such systems, or do they try and map it to more common paradigms?

Conflict of Interest

- Don't choose assessor that tries to sell you their product, a partner's product, or consultancy

Transfer of Risk!

- Your assessor assumes risk when they make statements about your systems. Are they mature enough to realize this?

Pitfalls: Snake Oil & Silver Bullets

Unfortunately there are no

- Silver bullets
- Magic tools
- Wondrous applications

'Pay no attention to the man behind the curtain'

Resources

The PCI SSC Web Site: https://www.pcisecuritystandards.org/index.shtml

PCI Quick Reference Guide:
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

SAQs: https://www.pcisecuritystandards.org/saq/index.shtml#saq

Cryptographic Algorithms for the Payment Card Industry

http://www.atsec.com/downloads/white-papers/cryptographic_algorithms_PCI.pdf

Payment Card Industry Compliance For Large Computing Systems White Paper

http://www.atsec.com/us/pci-lcs.html

Popular overview of PCI requirements:
http://www.youtube.com/watch?v=OceYWri86Ts

Ads!

Webinar: "Is your mainframe securing your sensitive data? It can!"

Wednesday, October 27th at 2 p.m. EST

https://www1.gotomeeting.com/register/597695160

2010 Annual Computer Security Applications Conference

December 6–10, 2010 | Four Seasons Hotel | Austin, Texas, USA

http://www.acsac.org/ :

Thank you for listening: Questions?