
1st SECURE IT
A QSA Perspective
PCI DSS
3.2
By Mark Akins, PCI QSA, CISSP, CISA

Agenda

- PCI Program Overview
- PCI DSS Introduction
- Updates included in Ver. 3.2
- PCI DSS Compliance & Validation
  - Merchant / Service Provider Levels
  - Self-Assessment Questionnaires
  - Validation by Assessment (ROC)
    - Scoping
    - Gap Analysis
    - Remediation
- Emerging Technologies
- Questions

PCI Program Overview

Before 2004, each of the major card brands had their own security program.

- Visa US - Cardholder Information Security Program (CISP)

- MasterCard - Site Data Protection (SDP)

- Amex - Data Security Operating Policy (DSOP)

- Discover - Information Security & Compliance (DISC)

- JCB - Data Security Program (DSP)

As you can imagine, these disparate programs made compliance difficult for merchants and service providers.

PCI Program Overview

- PCI DSS version 1 is dated December 2004.
- On June 30, 2005, the regulations took effect.
- The PCI Security Standards Council came into existence in 2006.
- The Council became responsible for the development, management, education and awareness of the PCI Data Security Standards. Current Version of the PCI DSS is 3.2 which will be formally released in May 2016

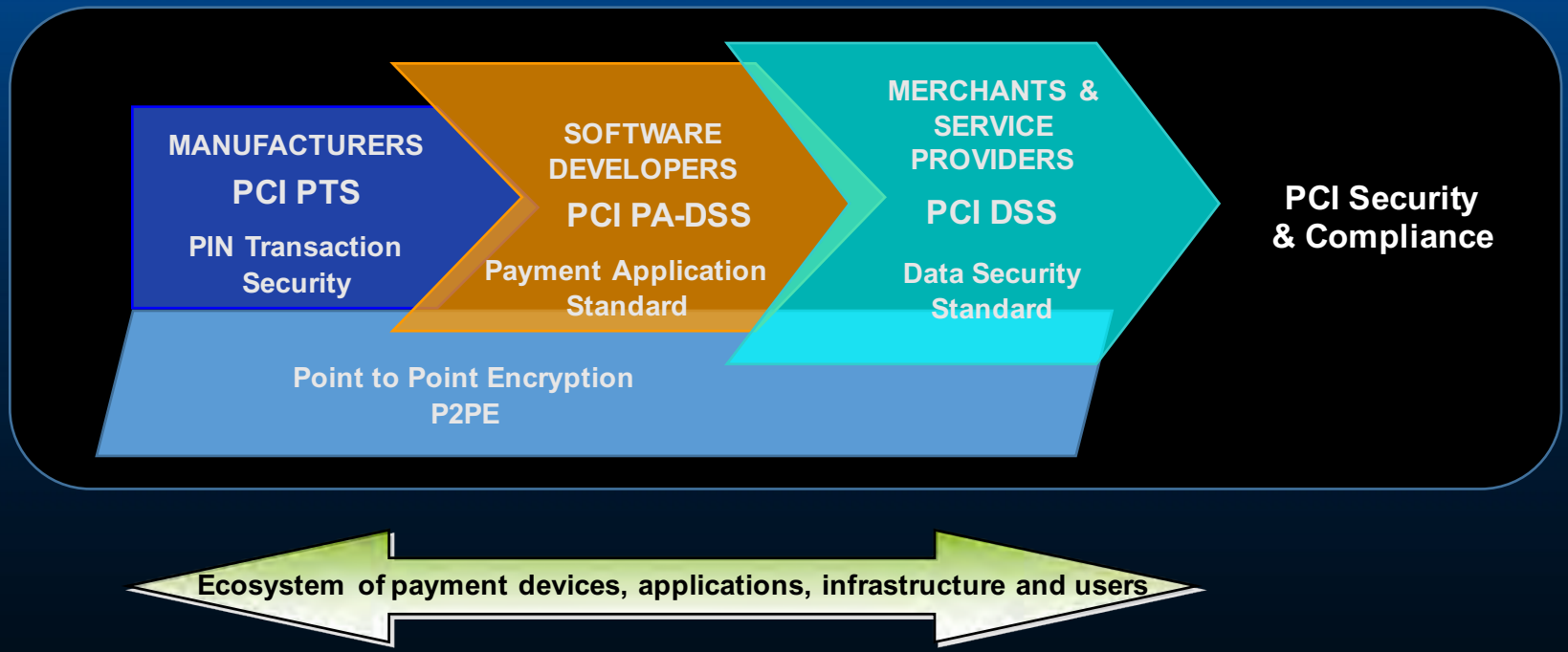
PCI Program Overview

- PCI DSS Compliance is universally agreed to and accepted, each of the Card Brands, However they still maintain their own compliance programs in accordance with their own security risk management policies for compliance, validation levels and enforcement.

- Additionally, each Card Brand has their own penalizing/fining procedures for companies who experience a data breach.

PCI Program Overview

Various PCI programs and how do they relate?



PCI Program Overview

Who is responsible for PCI Compliance?

Responsible for managing the various PCI programs and certifying QSAs

Acquiring Banks

Communicates and educates merchants on PCI DSS and reports merchant levels and compliance status to Card Brands

PCI Security & Compliance

Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Merchants & Service Providers

Responsible for safeguarding credit card data and complying with the PCI DSS

PCI DSS Introduction

What is PCI DSS?

- Payment Card Industry Data Security Standard. This standard is a set of controls used to protect Cardholder Data when stored processed or transmitted.
- Defined and evolved by the Payment Card Industry Security Standards Council (PCI SSC) with input from the Card Brands and participating organizations.
- Version 3.1 was released as an emergency revision to that addresses flaws in SSLv3 (Poodle).
- Current version is 3.2 and is on schedule to be released in May 2016
- PCI DSS v3.1 is valid until October 31, 2016, after which it is retired. All PCI DSS validations after this date must be to PCI DSS v3.2 or later.

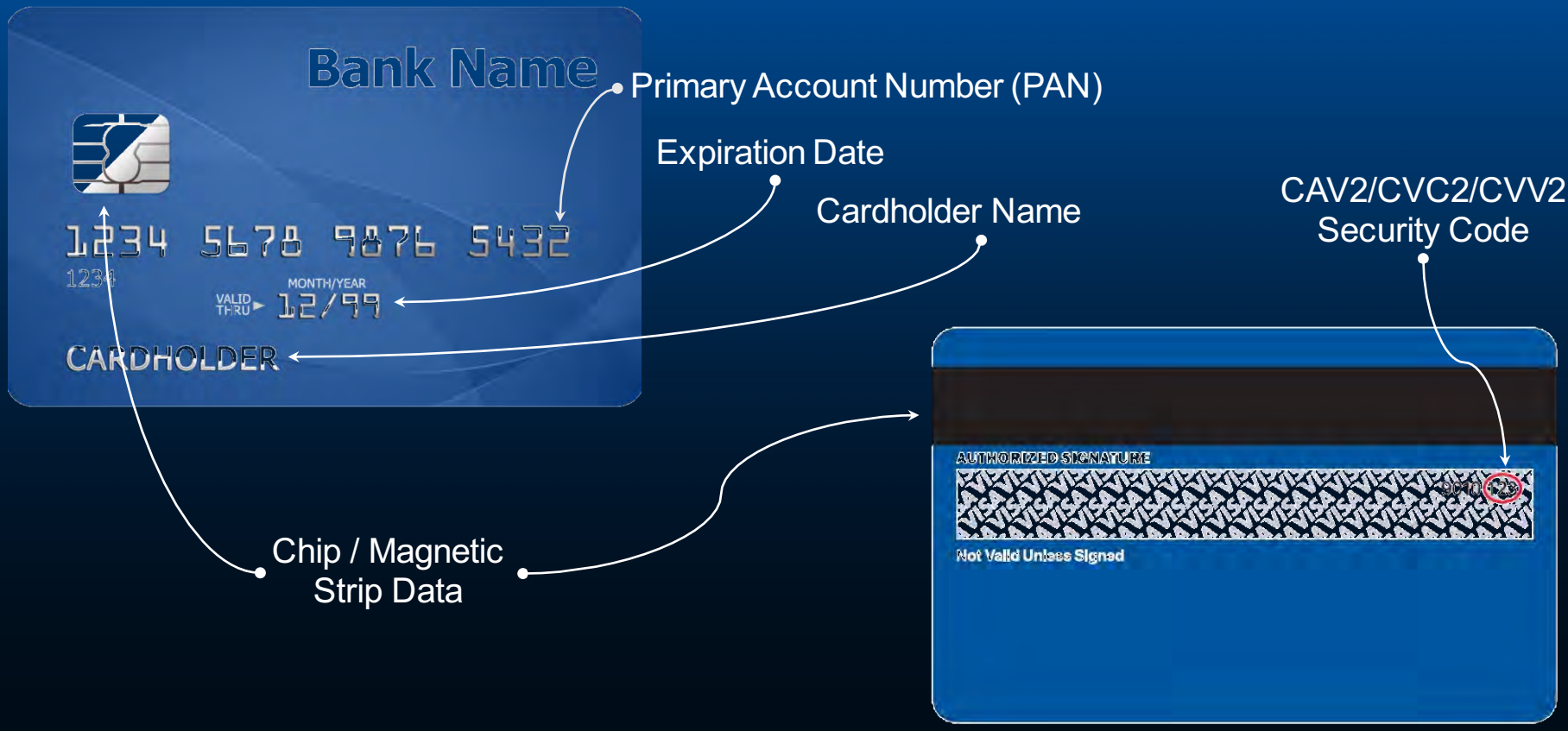
PCI DSS Introduction

What is PCI DSS?

- All entities (merchants, processors, acquirers, issuers, or service providers) that store, process or transmit cardholder data are selectively required to comply with the PCI DSS.
- Standards are on a 3 year Lifecycle.
- Version 3.0 was published in November 2013.
- Version 3.1 was published in April 2015.
- 2014 was a Transition year and 2016 is the final year for PCI 3.1
- 2016 is also a Transition year and the new PCI standard will be published in May 2016.

PCI DSS Introduction

What is Cardholder Data (CHD)?



PCI DSS Introduction

Can I store Cardholder Data (CHD)?

	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	*No
	Service Code	Yes	*No
	Expiration Date	Yes	*No
Sensitive Authentication Data	Full Magnetic Stripe or Equivalent Chip Data	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/PIN Block	No	N/A

* It is best practice to protect these data elements if stored in conjunction with the PAN.

PCI DSS Introduction

Is PCI Compliance a Law?

No federal statutes. However the following states either refer to PCI DSS directly, or make equivalent provisions:

- Minnesota established the “Plastic Card Security Act” which provides issuing banks a legal mechanism to collect the costs to reissue payment cards after a payment card security breach.
- Massachusetts established 201CMR17.00, which pulls some important concepts from the PCI DSS.
- California established CASB1386 to protect the privacy of personal information such as credit card account numbers.

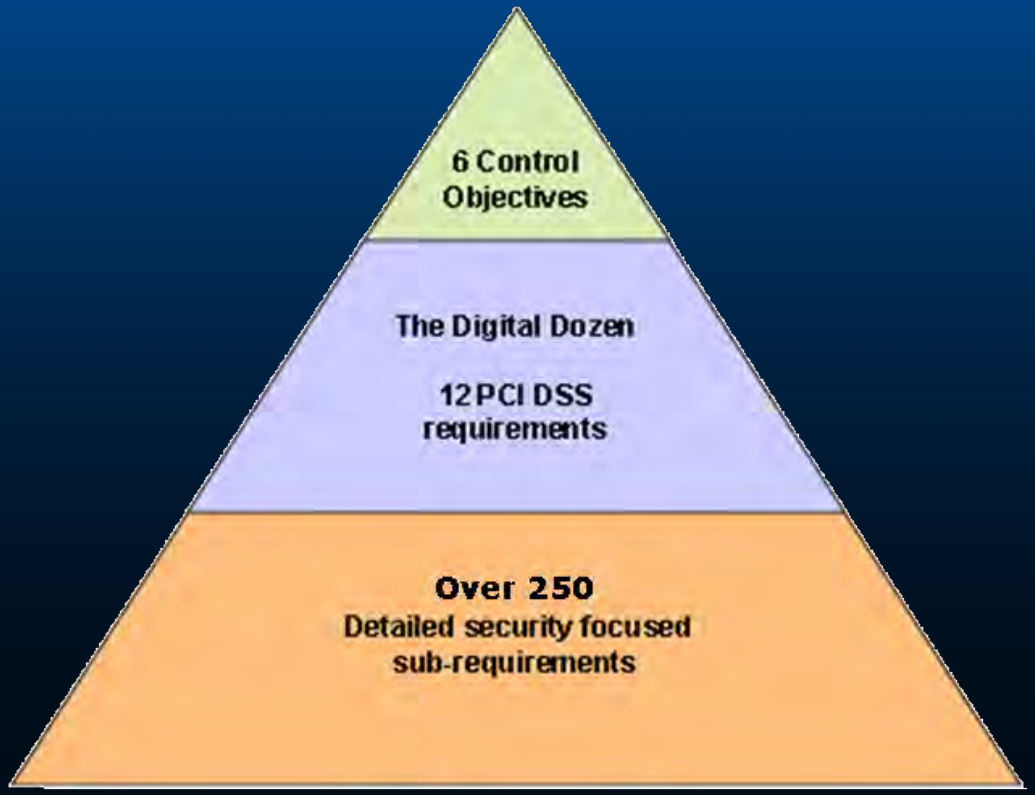
PCI DSS Introduction

Is PCI Compliance a Law?

- Washington State established HB1149 which provides issuing banks a legal mechanism to collect the costs to reissue payment cards after a payment card security breach.
- Nevada established Senate Bill 227 which has a specific requirement to comply with the Payment Card Industry Data Security Standard.
- Oregon passed ORS 646.200 which establishes fines for negligence in the event of a data breach.

PCI DSS Introduction

PCI DSS 3.2 Pyramid



PCI DSS Introduction

PCI DSS has Control Objectives

1) Build and Maintain a Secure Network
2) Protect Card Holder Data
3) Maintain a Vulnerability Management Program
4) Implement Strong Access Control Measures
5) Regularly Monitor and Test Networks
6) Maintain an Information Security Policy

PCI DSS Introduction

PCI DSS has 12 Requirements

1) Install and Maintain a firewall configuration to protect CHD

- Firewall and Router configuration standards
- Review Network Diagram
- Firewall and Router connections are restricted (inbound/outbound traffic)
- No direct internet connection to CHD (DMZ)

2) Do not use vendor-supplied defaults for system passwords and other security parameters

- Attempt to sign on with defaults
- Hardening standards and system configuration
- Non-console admin access is encrypted

PCI DSS Introduction

PCI DSS has 12 Requirements

3) Protect stored CHD

- Retention Policy and Procedures
- Quarterly process for deleting stored CHD
- Sample incoming transactions, logs, history & trace files, database schemas and content
- Do not store full track, CVV or PIN
- Render PAN unreadable (mask/truncate)
- Encryption and key management

4) Encrypt transmission of CHD across open, public networks

- Verify encryption and encryption strength (No SSL3)
- Verify wireless is industry best practice (no WEP)

PCI DSS Introduction

PCI DSS has 12 Requirements

5) Protect all systems against malware and regularly update anti-virus software or programs

- All system have AV (Linux Malware Review)
- AV is current, actively running and logging

6) Develop and maintain secure systems and applications

- Configuration change management
- Patch management – current within one month
- ID new security vulnerabilities with risk rating
- Custom code is reviewed prior to release
- Change management process
- Developers are trained in secure coding techniques

PCI DSS Introduction

PCI DSS has 12 Requirements

7) Restrict access to CHD by need-to-know

- Review access policies
- Confirm access rights and controls for privileged users
- Confirm access controls default with “deny-all”

8) Identify and authenticate access to system components

- Verify all users have a unique ID
- Verify authentication with ID/PW combination
- Verify two-factor (MFA) authentication for remote access
- Verify terminated users are deleted
- Inspect configurations for PW controls

PCI DSS Introduction

PCI DSS has 12 Requirements

9) Restrict physical access to CHD

- Access to computer rooms and data centers
- Video cameras are in place and video is secure
- Network jacks are secure – not in visitor area
- Process for assigning badges
- Storage locations are secure (offsite media)

10) Track and monitor all access to network resources

- Review audit trails – actions, time, date, user, etc.
- Time server updates and distribution
- Process to review security logs

PCI DSS Introduction

PCI DSS has 12 Requirements

11) Regularly test security systems and processes

- Test for wireless access points
- Internal and external network vulnerability scans
- Internal and external penetration testing annually
- File integrity monitoring tools are used

12) Maintain a policy that addresses information security

- Policies are reviewed at least annually
- Explicit approval is required for access
- Auto disconnect for inactivity-internal and remote
- Security awareness program is in place
- Risk Assessment and Incident Response Plan

Updates included in Ver. 3.2

Errata & Clarifications	Clarifies intent of requirement. Ensures that concise wording in the standard portrays the desired intent of requirement. ***No Errata and 47 new clarifications in version 3.2***
Additional Guidance	Explanation, definition and/or instruction to increase understanding or provide further information or guidance on a particular topic. ***Three areas of additional guidance in version 3.2***
Evolving Requirements	Changes to ensure that the standards are up to date with emerging threats and changes in the market. ***Eight new evolving requirements in version 3.2***

Updates included in Ver. 3.2

Errata & Clarifications	• Removed examples of “strong” or “secure” protocols from a number of requirements, as these may change at any time. • Clarified correct term is multi-factor authentication, rather than two-factor authentication, as two or more factors may be used. • Removed examples of “insecure” protocols as these may change in accordance with industry standards. • Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.

Updates included in Ver. 3.2

Errata & Clarifications	• New Appendix to incorporate the "Designated Entities Supplemental Validation" (DESV), which was previously a separate document. • Clarified that change control processes are not limited to patches and software modifications. • Clarified that the list of service providers includes a description of the service provided.

Updates included in Ver. 3.2

Additional Guidance	• Added guidance that security threats are constantly evolving, and payment applications that are not supported by the vendor may not offer the same level of security as supported version • New section to describe how this new version of PCI DSS impacts the previously-effective version. • Added guidance that service provider responsibility will depend on the particular service being provided and the agreement between the two parties.

Updates included in Ver. 3.2

Evolving Requirements	*Effective February 1, 2018* • New requirement for change control processes to include verification of PCI DSS requirements impacted by a change. • Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE. • New requirement for service providers to detect and report on failures of critical security control systems.

Updates included in Ver. 3.2

Evolving Requirements	*Effective February 1, 2018* • New requirement for service providers to perform penetration testing on segmentation controls at least every six months. • New requirement for service providers' executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program. • New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures.

Addressing SSL in in Ver. 3.2

- **New in Appendix A2**
  - New implementations must not use SSL or early TLS as a security control.
  - All service providers must provide a secure service offering by June 30, 2016.
  - After June 30, 2018, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet below).
  - Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
  - POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after June 30, 2018.

Merchant / Service Provider Levels

- The Compliance road map is determined based on the merchant or service providers “Level”
- The merchant or service providers “Level” is based on the cardholder transaction volume within a 12-month period
- All merchants will fall into one of four merchant levels
- All service providers will fall into one of two service provider levels

Merchant Levels

Merchant Levels According to Visa and MasterCard

Merchant Level	Merchant Criteria
1	• Any merchant that has suffered a hack or an attack that resulted in an account data compromise • Any merchant having more than six million total combined Visa, MasterCard and Maestro transactions annually • Any merchant that Visa or MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system
2	• Any merchant with more than one million but less than or equal to six million total combined Visa, MasterCard and Maestro transactions annually
3	• Any merchant with more than 20,000 combined Visa, MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually
4	• All other merchants

Merchant Levels

Validation Requirements According to Visa and MasterCard

Merchant Level	Validation	Validated By
1	• Annual Onsite Assessment • Quarterly Network Scan conducted by an ASV	• Qualified Security Assessor (QSA) • Approved Scanning Vendor (ASV)
2	• Annual Self-Assessment • Onsite Assessment at Merchant Discretion • Quarterly Network Scan conducted by an ASV	• Qualified Security Assessor (QSA) • Approved Scanning Vendor (ASV) • Internal Auditor (ISA)
3	• Annual Self-Assessment • Quarterly Network Scan conducted by an ASV	• Merchant or QSA • Approved Scanning Vendor (ASV)
4	• Annual Self-Assessment • Quarterly Network Scan conducted by an ASV	• Merchant or QSA • Approved Scanning Vendor (ASV)

Service Provider Levels

Service Provider Levels According to Visa and MasterCard

Service Provider Level	Merchant Criteria
1	• All MasterCard Third Party Processors(TPPs) • All VisaNet Processors • Any service provider that stores, processes and/or transmits over 300,000 Visa or MasterCard transactions per year
2	• Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions per year

Service Provider Levels

Validation Requirements According to Visa and MasterCard

Service Provider Level	Validation	Validated By
1	• Annual Onsite Assessment • Quarterly Network Scan conducted by an ASV	• Qualified Security Assessor (QSA) • Approved Scanning Vendor (ASV)
2	• Annual Self-Assessment • Onsite Assessment at Service Provider Discretion • Quarterly Network Scan conducted by an ASV	• Qualified Security Assessor (QSA) • Approved Scanning Vendor (ASV)

Self-Assessment Questionnaire

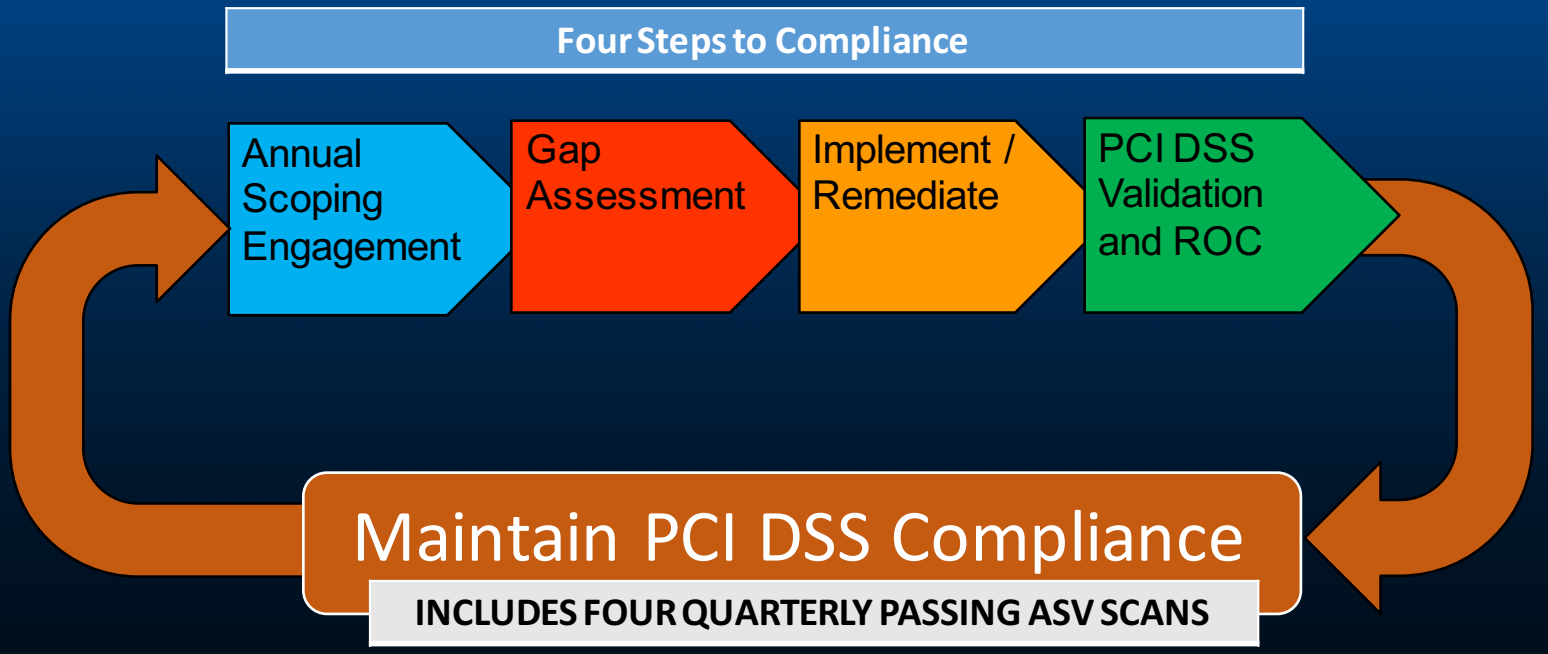
PCI DSS 3.1 SAQs

SAQ	Description	ASV Scan
A	Ecommerce Card Not Present – Entire site or payment page is fully outsourced	No
A-EP	Ecommerce Card Not Present – Payment page is partially outsourced or payment page direct post	Yes
B	Face to Face / MOTO with Payment Terminal not connected to Internet	No
B-IP	Face to Face / MOTO with Payment Terminal connected to Internet	Yes
C-VT	Face to Face / MOTO with Internet Virtual Terminal – Segmented and manually keyed (not swiped)	No
C	Face to Face / MOTO / Ecommerce connected to Internet – No CHD Storage*	Yes
D	Face to Face / MOTO / Ecommerce connected to Internet – CHD Storage*	Yes
HW-P2PE	Point of Sale managed with Point to Point Encryption – No CHD Storage	No
D - SP	Level 2 Service Providers - Face to Face / MOTO / Ecommerce	Yes

*Ecommerce Payment Application not outsourced and must be PA-DSS compliant

Validation by Assessment

Report on Compliance (ROC) Methodology



Annual Scoping Engagement

PCI DSS 3.1 (Page 10)

The first step of a PCI DSS assessment is to accurately determine the scope of the review. 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 identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope.

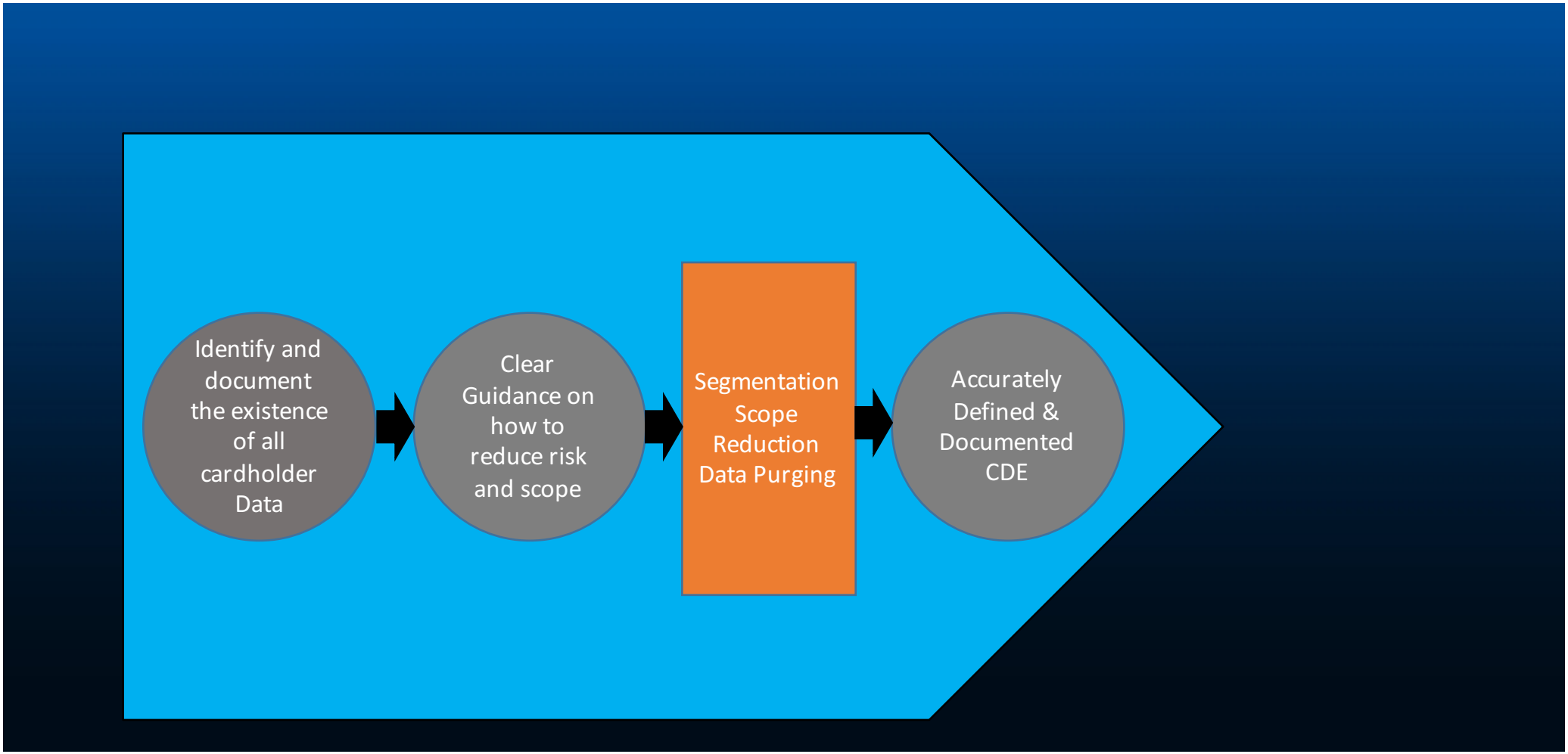
To confirm the accuracy of the defined CDE, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined CDE.
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data.

The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.

Annual Scoping Engagement



Scoping

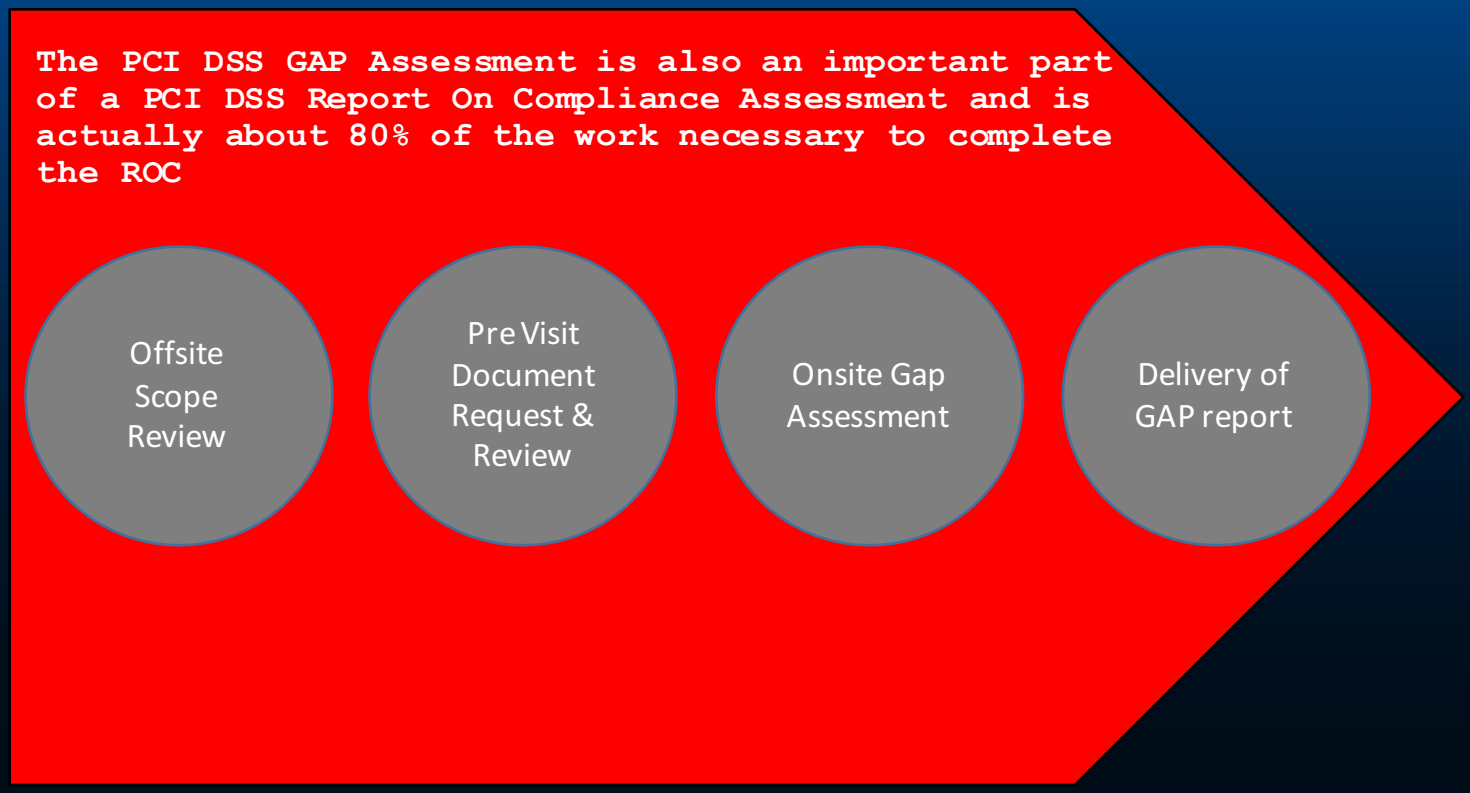
Free Credit card scanning software

ccsrch:
http://sourceforge.net/projects/ccsrch/

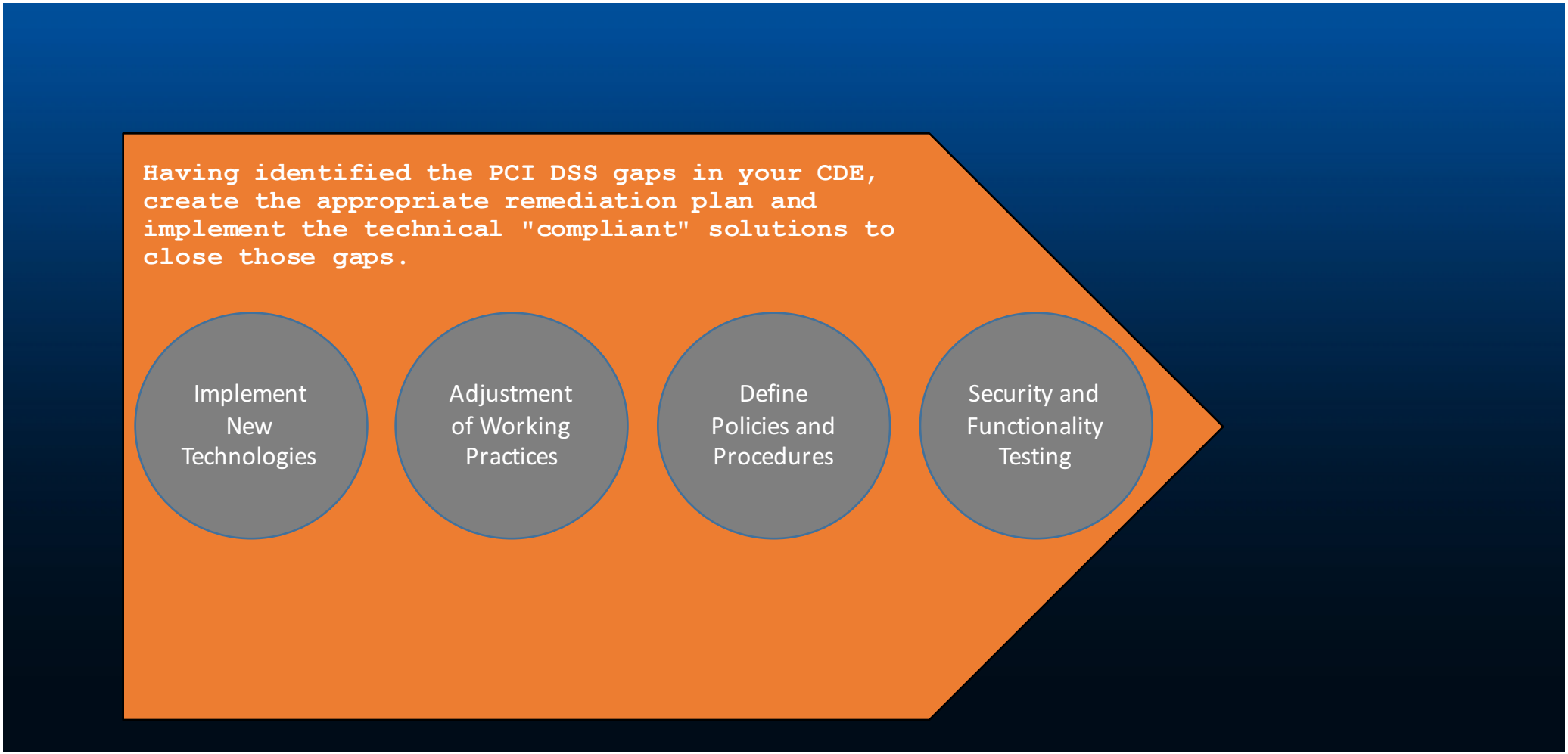
Sensitive Number Finder (SENF):
http://www.utexas.edu/its/products/senf/

Spider from Cornell:
http://www2.cit.cornell.edu/security/tools/

Gap Assessment



Implement / Remediate



Implement / Remediate

The PCI DSS ROC remediation plan should take into account that most QSAs mandate a 60 day window for remediation. Otherwise the merchant would have to re-perform the GAP audit. Additionally the remediation phase should also include any necessary remediation for the annual penetration test, external Approved Scanning Vendor (ASV) scans, and internal vulnerability scans.

Implement / Remediate

Compensating Control Litmus Test

(1) Meet the intent and rigor of the original PCI DSS requirement;

(2) Provide a similar level of defense as the original PCI DSS requirement;

(3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and

(4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Appendix C: Compensating Controls Worksheet

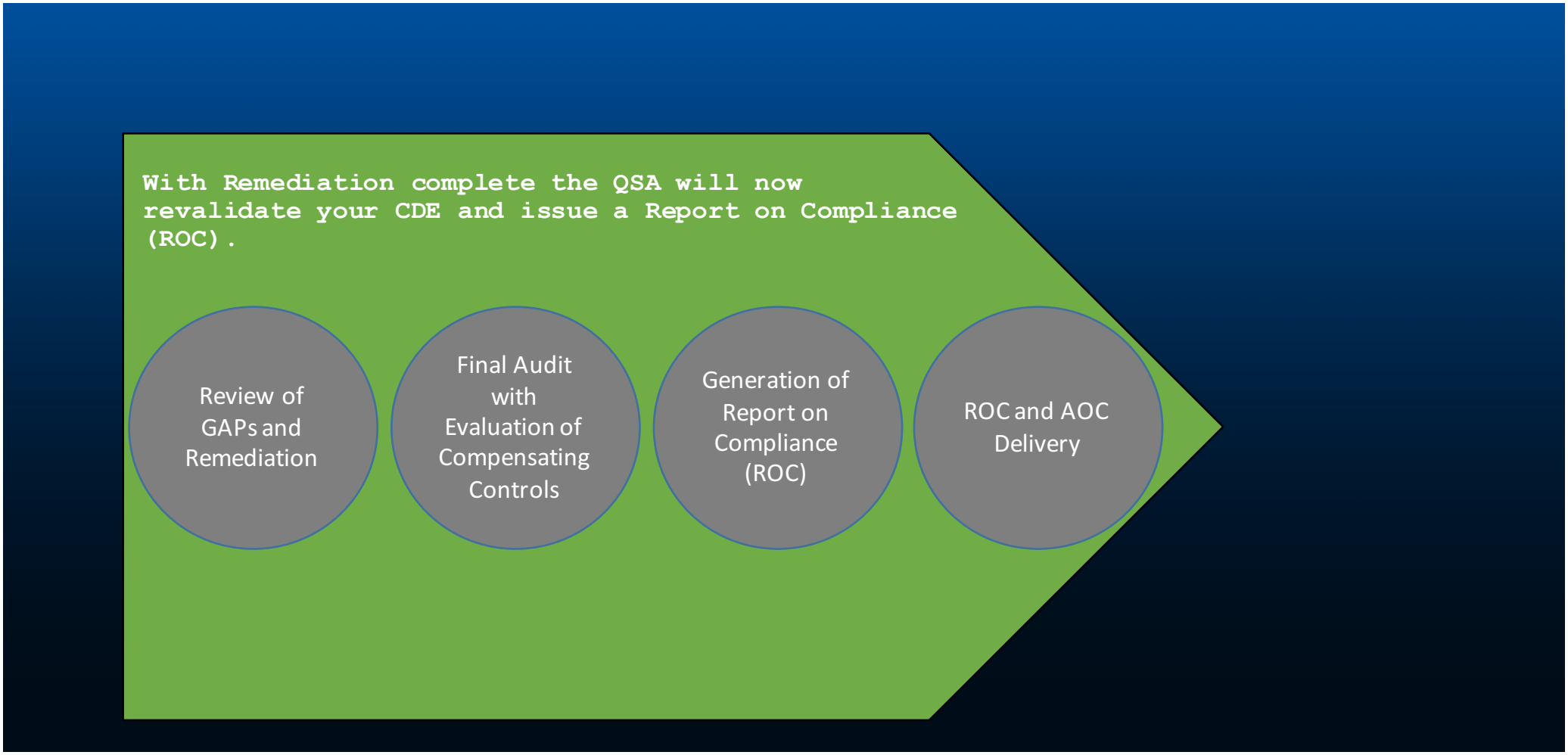
Use this worksheet to define compensating [illegible] for [illegible]quirement where "YES" was checked and compensating controls were mentioned in [illegible] Special".

***Note:** Only companies that have undertak[illegible] a risk [illegible]ysis a[illegible] have legitimate technological or documented business constraints can co[illegible]r th[illegible]e of co[illegible]ensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. **Constraints**	List constraints precluding compliance with the original requirement.	
2. **Objective**	Define the objective of the original control; identify the objective met by the compensating control.	
3. **Identified Risk**	Identify any additional risk posed by the lack of the original control.	
4. **Definition of Compensating Controls**	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. **Validation of Compensating Controls**	Define how the compensating controls were validated and tested.	
6. **Maintenance**	Define process and controls in[illegible] maintain compensating[illegible]	

PCI DSS Validation and ROC



Emerging Technologies

Chip & PIN– or EMV (Europay, MasterCard, Visa)

- Contact and Contactless - Near Field Communication
- Required vs. Encouraged
- Liability Shift in the U.S. effective October 1, 2015
  - Merchants not using EMV will take the financial hit on fraudulent, card-present transactions.
- Benefit - Physical Cards are less likely to be used fraudulently.
- Benefit – Works well with Mobile Wallets
- Compliance Reduction
  - As of October 2012, if more than 75% of merchant transactions originate from EMV-compliant POS terminals that support both contact and contactless transactions, the merchant may apply for relief from the audit requirement for PCI compliance.

Emerging Technologies

Point to Point Encryption

- P2PE is not the same as E2EE
  - P2PE is a subset of E2EE. This is because the major difference between P2PE and E2EE is that P2PE does not allow the merchant to be a manager of the encryption keys.
- Benefit
  - significant PCI DSS Scope Reduction.
- Downside
  - Depending on the P2PE solution, you may be stuck with your processor. That is because most processors offering P2PE are only offering one P2PE solution. To change processors you may have to replace your terminals and possibly other equipment.
  - Unless a validated solution, it requires Acquiring Bank & QSA approval.

Emerging Technologies

Mobile Payments

- Mobile Payment Applications
  - 3 categories of Mobile Payment Applications
  - Only Category 1 (PTS-approved) and 2 (purpose-built and bundled) devices will be considered for PA-DSS.
  - Category 3 devices (smartphones/iPod touch) are becoming more prominent. Does not mean Category 3 applications cannot be used, but need to be custom built for merchants or delivered as part of a service. The solution provider is responsible for PCI DSS Compliance. (Square)
- PCI SSC published and FAQ for mobile applications
  - This guide educates merchants on the risk factors that need to be addressed in order to protect card data when using mobile devices to accept payments.

Emerging Technologies

Cloud Computing

- PCI Compliance is possible, but know what you are getting into
- Identify a couple options for Cloud Service Providers (CSP)
- Make sure the CSP is PCI validated (Ask for their current AOC)
- Insist on getting a responsibility document from the CSP

Emerging Technologies

Tokenization

A Token is surrogate value which is substituted for the actual data (ex: credit card number) while the actual data is encrypted and stored elsewhere. (Typically with the service provider)

Benefits

- Reduces Scope of PCI DSS by not storing CHD (Data Devaluation)
- (Data Devaluation) Tokens have no value since the original data values cannot be mathematically derived from tokens.

Downside

- Using payment processor specific tokenization, for instance, locks organizations into a particular payment processor.

1st SECURE IT

Mark Akins
1st Secure IT, LLC
PCI QSA, CISA, CISSP
makins@1stsecureit.com

Questions?