We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

PCI Readiness and Compliance For Financial Services

January 24, 2024

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Session CPE Requirements

- You need to attend 50 minutes to receive the full 1 CPE credit.
- 4 Attendance Markers that read: “I’m Here,” will be launched during this session. You must respond to a minimum of 3 to receive the full 1 CPE credit.

Both requirements must be met to receive CPE credit

Learning Objectives

At the end of the session, you will be able to:

○ Identify how the core elements of the PCI DSS apply to Financial Institutions

○ Recognize key challenges faced by Financial Institutions in managing a PCI compliance program

○ Identify how a well functioning PCI compliance program can support and enhance the institutions risk management program

Cyber Security Services

Information Security offered as professional service offering for over 25 years

- Penetration Testing and Vulnerability Assessment
  - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (GLBA, FFIEC, CIS, NIST, etc…)
- **PCI-DSS Readiness and Compliance Assessments**
- Incident response and forensics
- Independent security consulting
- Internal audit support
- Regulatory compliance

PCI - DSS Overview

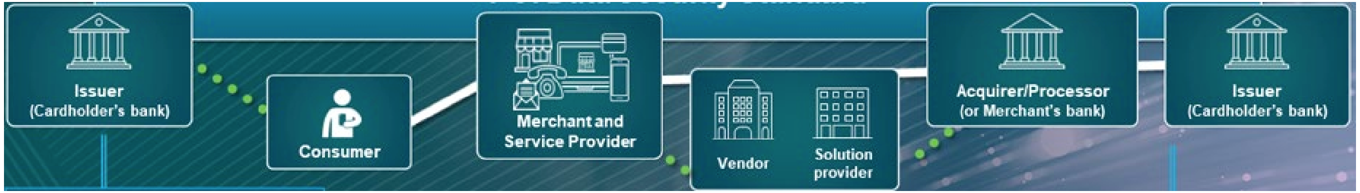
A Long Time Ago… In a Place Far Far Away…

Before PCI DSS

Each major card brand had its own separate criteria for implementing credit card security.

Merchants and processors who accepted multiple brands of cards needed to have a separate compliance program for each.

Visa's Cardholder Information Security Program
MasterCard's Site Data Protection
American Express' Data Security Operating Policy
Discover's Information Security and Compliance
JCB's Data Security Program



The Basics – How Card Processing Works

Cardholder

Consumers purchasing goods either as a “Card Present” or “Card Not Present” transaction

Issuer

FI or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa)

Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)

Merchant

Organization accepting the payment card for payment during a purchase

Acquirer

FI or entity the merchant uses to process their payment card transactions

Acquirer is also called: Merchant Bank, ISO (independent sales organization), or Payment Processor

Payment Brand - Amex, Discover, JCB can be Acquirer; Visa or MasterCard are NEVER the Acquirer

Service Provider

Business entity that is not a payment brand AND is directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.

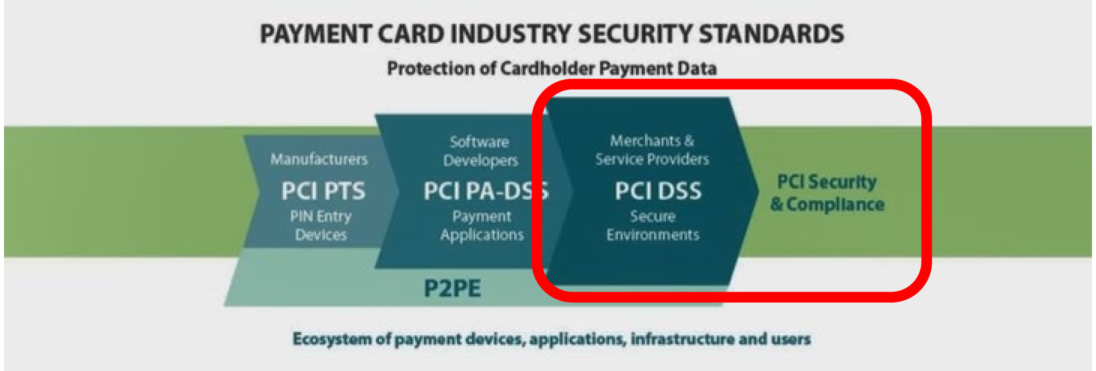
Which of these is your Institution?

The PCI Security Standards

- **2006** - Major card brands formed the Payment Card Industry Security Standards Council.

- This council developed and has continually updated the Data Security Standard (DSS).

- The DSS is a set of 12 detailed requirements that ensure maximum payment card security.

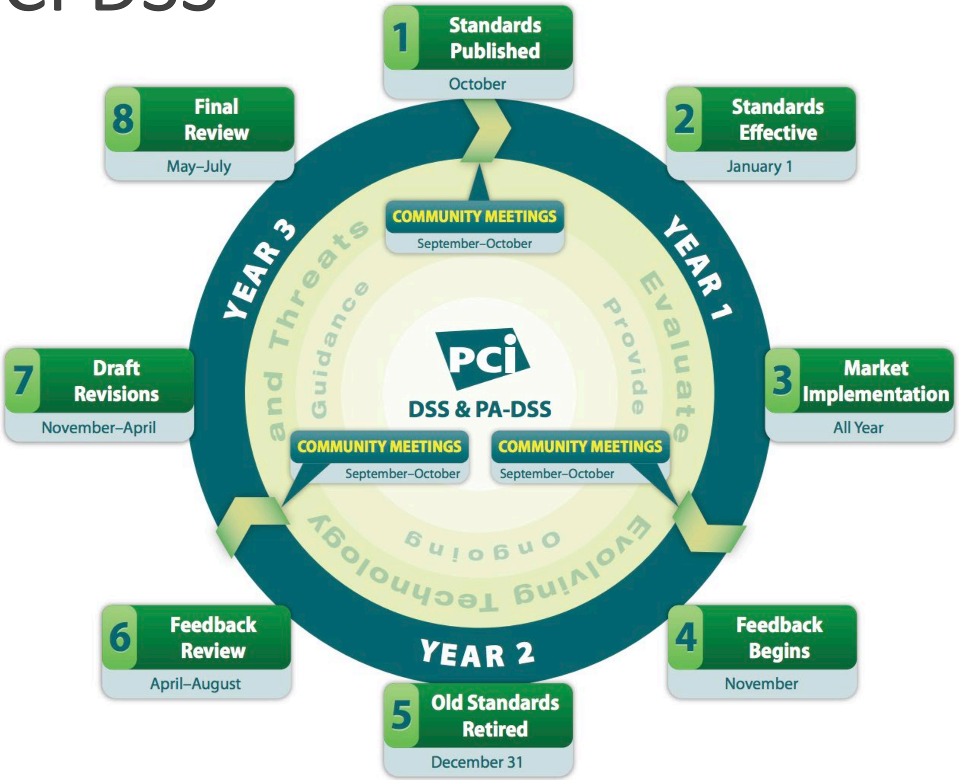

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
Manufacturers
PCI PTS
PIN Entry Devices
Software Developers
PCI PA-DSS
Payment Applications
Merchants & Service Providers
PCI DSS
Secure Environments
PCI Security & Compliance
P2PE
Ecosystem of payment devices, applications, infrastructure and users

Lifecycle Changes to PCI DSS

“Current version” is 3.2.1 (May 2018)

Version 4 released in Q1 of 2022

Compliance with Version 4 after March 31, 2024…



https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

Cardholder Data Environment (CDE)

The PCI DSS defines the CDE to be ***the people, processes and technology*** that store, process or transmit cardholder data or sensitive authentication data, ***<u>including any connected system components</u>***.”

- **Store** – when cardholder data is inactive or at rest (e.g., Core system, application system or database, stored backups, system component memory, paper, etc…)

- **Process** – when cardholder data is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed, etc…)

- **Transmit** – when cardholder data is being transferred from one location to another (e.g., data in motion)

➢ ***More on how to define this later…***

Compliance and Certification

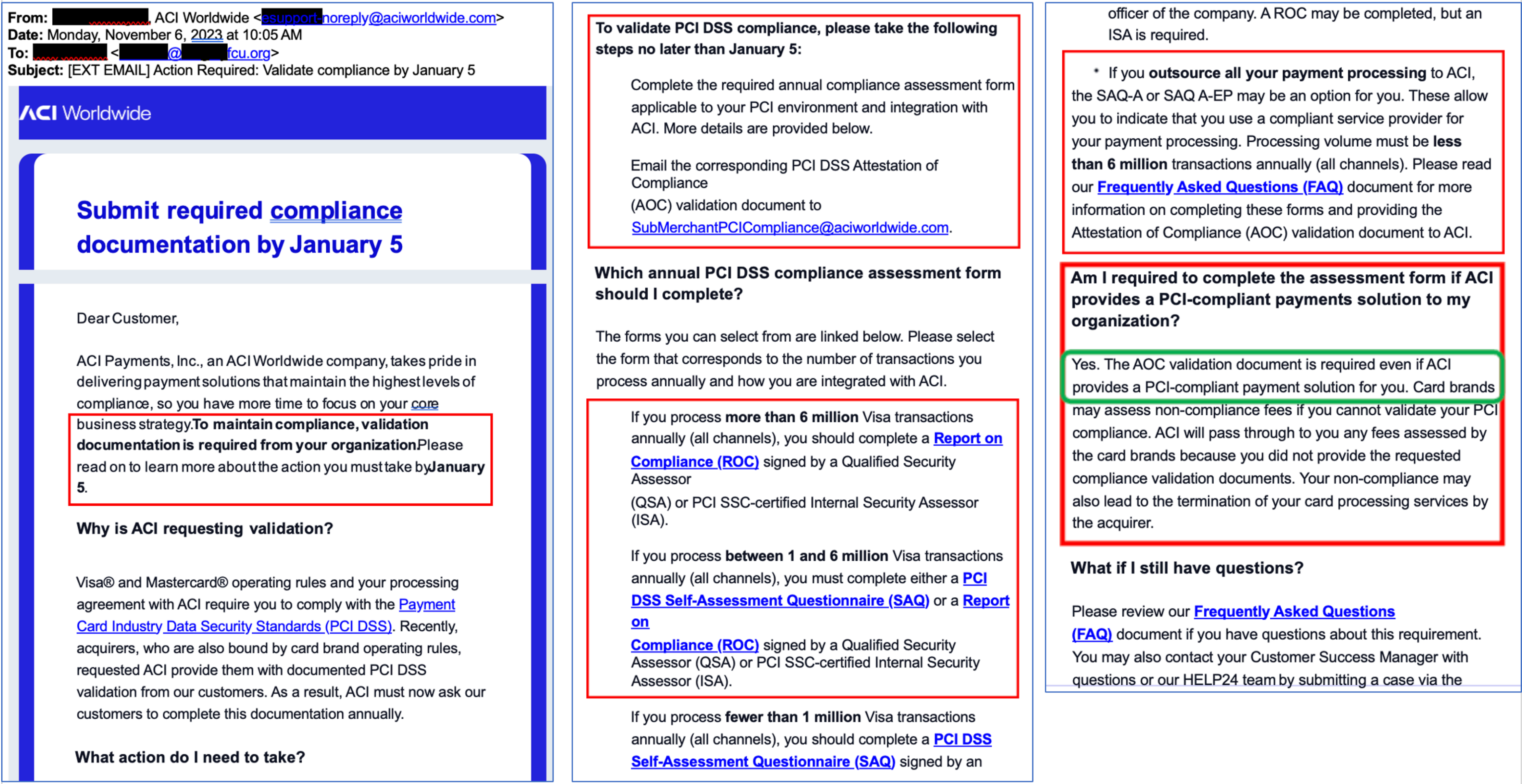
Organizations that store, process, or transmit credit card data need to comply with the DSS standards. This includes Financial Institutions, Issuers, Merchants and Service Providers.

Organizations must report compliance annually utilizing either a self assessment questionnaire (SAQ) or independent third party review and Report on Compliance (ROC).

The below link from the VISA website states that Financial Institutions and Issuers must be PCI compliant.

- https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html

- Payment Card Industry Data Security Standard (PCI DSS) compliance is required of all entities that store, process, or transmit Visa cardholder data, including financial institutions, merchants and service providers. Visa's programs manage PCI DSS compliance by requiring that participants demonstrate compliance on a regular basis.



From: [redacted], ACI Worldwide <[redacted]support-noreply@aciworldwide.com>
Date: Monday, November 6, 2023 at 10:05 AM
To: [redacted] <[redacted]@[redacted]fcu.org>
Subject: [EXT EMAIL] Action Required: Validate compliance by January 5

ACI Worldwide

Submit required compliance documentation by January 5

Dear Customer,

ACI Payments, Inc., an ACI Worldwide company, takes pride in delivering payment solutions that maintain the highest levels of compliance, so you have more time to focus on your core business strategy.**To maintain compliance, validation documentation is required from your organization**Please read on to learn more about the action you must take by**January 5**.

Why is ACI requesting validation?

Visa® and Mastercard® operating rules and your processing agreement with ACI require you to comply with the Payment Card Industry Data Security Standards (PCI DSS). Recently, acquirers, who are also bound by card brand operating rules, requested ACI provide them with documented PCI DSS validation from our customers. As a result, ACI must now ask our customers to complete this documentation annually.

What action do I need to take?

To validate PCI DSS compliance, please take the following steps no later than January 5:

Complete the required annual compliance assessment form applicable to your PCI environment and integration with ACI. More details are provided below.

Email the corresponding PCI DSS Attestation of Compliance
(AOC) validation document to SubMerchantPCICompliance@aciworldwide.com.

Which annual PCI DSS compliance assessment form should I complete?

The forms you can select from are linked below. Please select the form that corresponds to the number of transactions you process annually and how you are integrated with ACI.

If you process **more than 6 million** Visa transactions annually (all channels), you should complete a **Report on Compliance (ROC)** signed by a Qualified Security Assessor
(QSA) or PCI SSC-certified Internal Security Assessor (ISA).

If you process **between 1 and 6 million** Visa transactions annually (all channels), you must complete either a **PCI DSS Self-Assessment Questionnaire (SAQ)** or a **Report on**
Compliance (ROC) signed by a Qualified Security Assessor (QSA) or PCI SSC-certified Internal Security Assessor (ISA).

If you process **fewer than 1 million** Visa transactions annually (all channels), you should complete a **PCI DSS Self-Assessment Questionnaire (SAQ)** signed by an

officer of the company. A ROC may be completed, but an ISA is required.

- If you **outsource all your payment processing** to ACI, the SAQ-A or SAQ A-EP may be an option for you. These allow you to indicate that you use a compliant service provider for your payment processing. Processing volume must be **less than 6 million** transactions annually (all channels). Please read our **Frequently Asked Questions (FAQ)** document for more information on completing these forms and providing the Attestation of Compliance (AOC) validation document to ACI.

Am I required to complete the assessment form if ACI provides a PCI-compliant payments solution to my organization?

Yes. The AOC validation document is required even if ACI provides a PCI-compliant payment solution for you. Card brands may assess non-compliance fees if you cannot validate your PCI compliance. ACI will pass through to you any fees assessed by the card brands because you did not provide the requested compliance validation documents. Your non-compliance may also lead to the termination of your card processing services by the acquirer.

What if I still have questions?

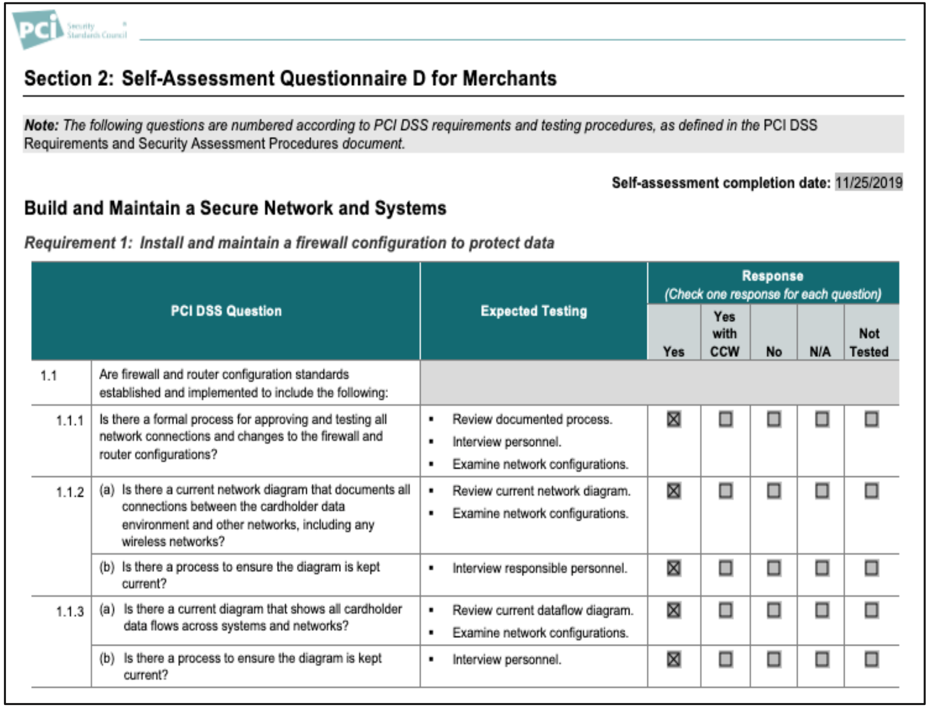
Please review our **Frequently Asked Questions (FAQ)** document if you have questions about this requirement. You may also contact your Customer Success Manager with questions or our HELP24 team by submitting a case via the

PCI DSS Compliance Reporting Self-Assessment Questionnaire (SAQ)

The PCI DSS SAQ consists of two components:

1. Questions corresponding to the PCI DSS requirements
   - Minimal to no Narrative
   - Yes, Yes w/CCW, No, NA, Not Tested

2. Attestation of Compliance
   - Organization certification of eligibility to perform and have performed the appropriate Self-Assessment. The correct Attestation will be packaged with the SAQ selected.
   - This is a summary



Section 2: Self-Assessment Questionnaire D for Merchants

***Note:** The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document.*

Self-assessment completion date: 11/25/2019

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect data

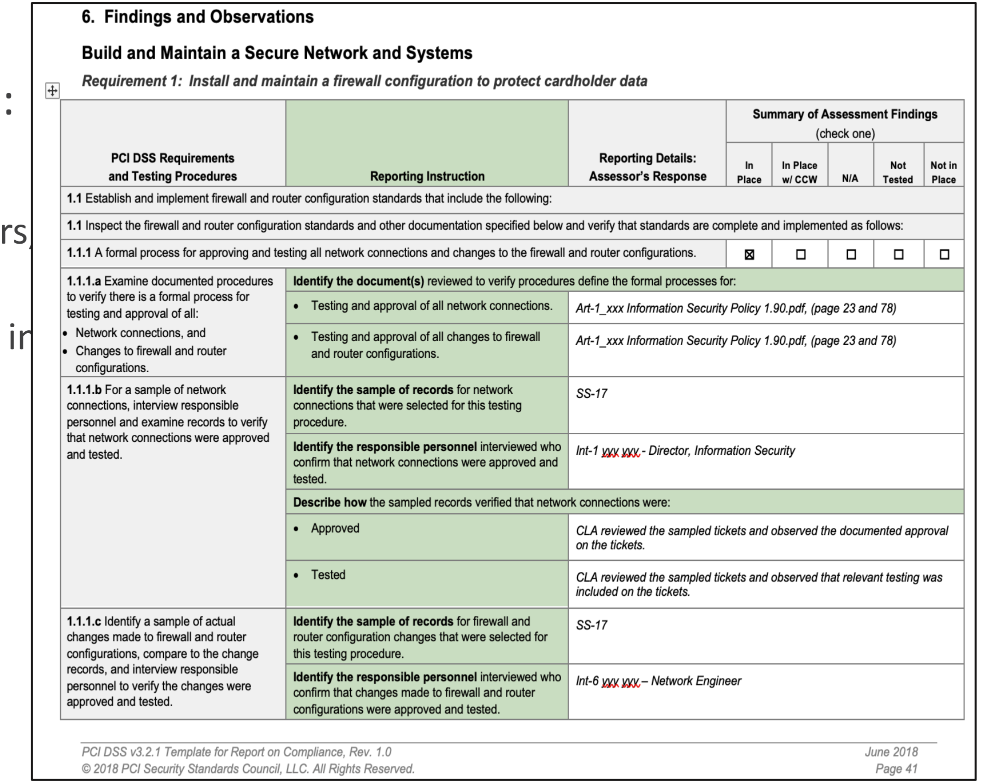
PCI DSS Question		Expected Testing	Response *(Check one response for each question)*				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1	Are firewall and router configuration standards established and implemented to include the following:						
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	▪ Review documented process. ▪ Interview personnel. ▪ Examine network configurations.	☒	□	□	□	□
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	▪ Review current network diagram. ▪ Examine network configurations.	☒	□	□	□	□
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview responsible personnel.	☒	□	□	□	□
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	▪ Review current dataflow diagram. ▪ Examine network configurations.	☒	□	□	□	□
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview personnel.	☒	□	□	□	□

PCI DSS Compliance Reporting
Report on Compliance (ROC)

The PCI DSS ROC consists of two components:

1. ROC is a detailed narrative of controls
   - Appropriate to financial institutions, issuers, service providers, merchants
   - In Place, In Place w/CCW, NA, Not Tested, Not in place
   - ***Reference to evidence***
   - ***Narrative description***

2. Attestation of Compliance
   - Summary of the ROC



6. Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

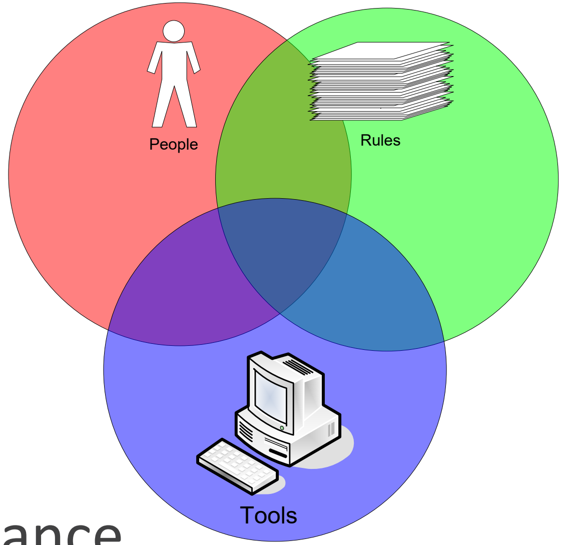
			Summary of Assessment Findings (check one)				
PCI DSS Requirements and Testing Procedures	**Reporting Instruction**	**Reporting Details: Assessor's Response**	**In Place**	**In Place w/ CCW**	**N/A**	**Not Tested**	**Not in Place**
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.			☒	□	□	□	□
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	• Testing and approval of all network connections.	*Art-1_xxx Information Security Policy 1.90.pdf, (page 23 and 78)*					
	• Testing and approval of all changes to firewall and router configurations.	*Art-1_xxx Information Security Policy 1.90.pdf, (page 23 and 78)*					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	**Identify the sample of records** for network connections that were selected for this testing procedure.	*SS-17*					
	Identify the responsible personnel interviewed who confirm that network connections were approved and tested.	*Int-1 yyy yyy - Director, Information Security*					
	Describe how the sampled records verified that network connections were:						
	• Approved	*CLA reviewed the sampled tickets and observed the documented approval on the tickets.*					
	• Tested	*CLA reviewed the sampled tickets and observed that relevant testing was included on the tickets.*					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	**Identify the sample of records** for firewall and router configuration changes that were selected for this testing procedure.	*SS-17*					
	Identify the responsible personnel interviewed who confirm that changes made to firewall and router configurations were approved and tested.	*Int-6 yyy yyy – Network Engineer*					

PCI DSS v3.2.1 Template for Report on Compliance, Rev. 1.0 *June 2018*
© 2018 PCI Security Standards Council, LLC. All Rights Reserved. *Page 41*

PCI - DSS
The Framework

Policies and Standards

- Compliance and Security are not the same
- People, Rules and Tools
  - What do we expect to occur?
  - How do we conduct business?
  - Who is responsible for what?
- Standards based operations from a governance or compliance framework:
  - GLBA, FFIEC, (State Laws?)----- *Regulatory*
  - **PCI – DSS**, CMMC ----- ***Contractual***
  - CIS Critical Controls, NIST ----- *Operational standards*



PCI is Contractional Obligation

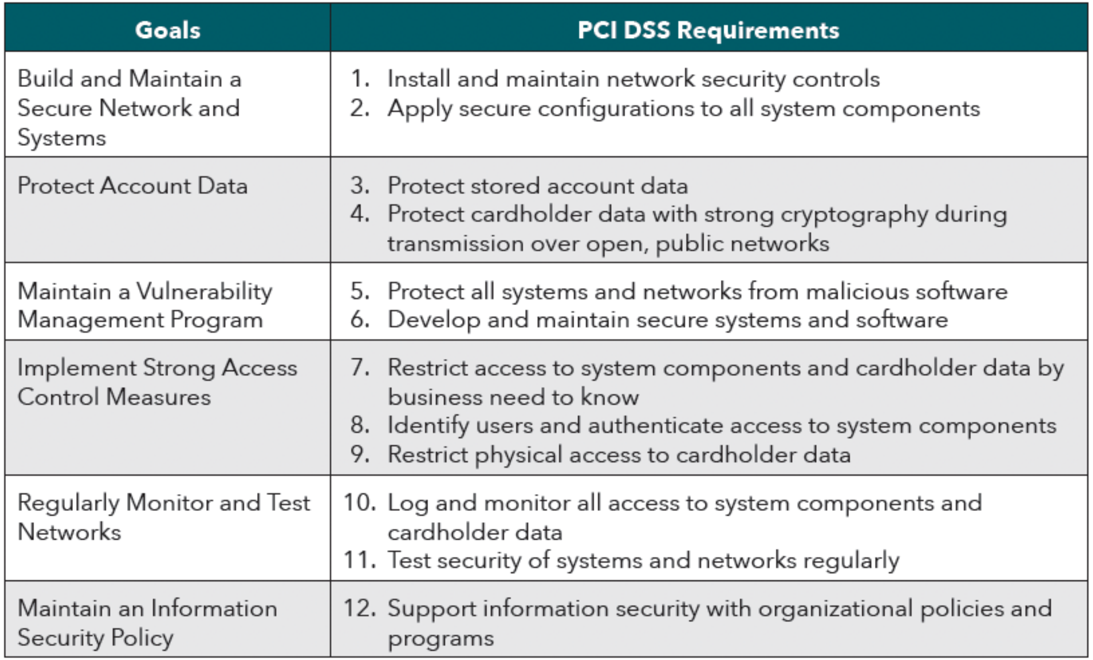
Overview – PCI DSS – “Digital Dozen”

Six Goals & Twelve Requirements

- Approximately 140 Controls
- A cadence of three for each control
  - Policies/Standards/Procedures
  - People
  - Evidence

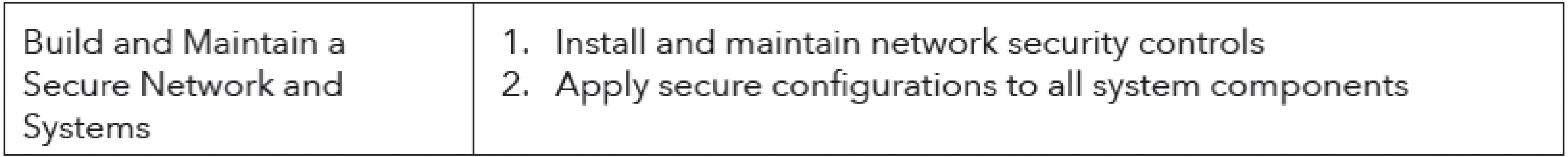
→ Over 400 “things to address”

→ PCI is all about
“Daily Business as Usual”



Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

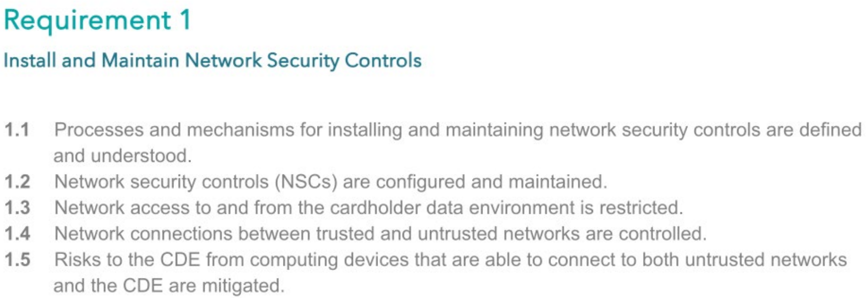
PCI DSS – Build & Maintain a Secure Network



Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components

Changes throughout:

- **Organizations must now properly communicate roles, responsibilities, and ownership of all requirement tasks**
- **Responsibilities must be formally documented, assigned, and understood by the owner**



Requirement 1

Install and Maintain Network Security Controls

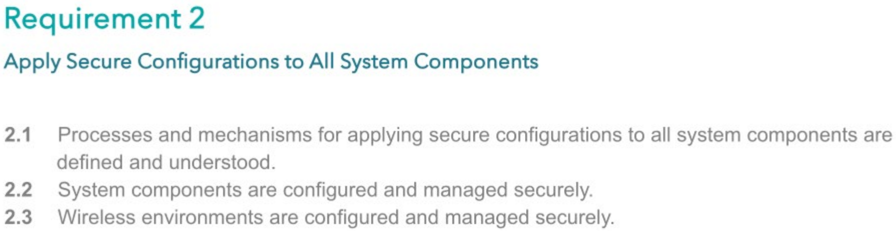
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

1.2 Network security controls (NSCs) are configured and maintained.

1.3 Network access to and from the cardholder data environment is restricted.

1.4 Network connections between trusted and untrusted networks are controlled.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.



Requirement 2

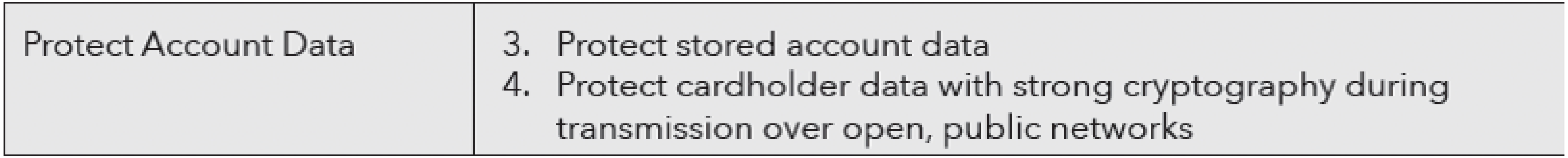
Apply Secure Configurations to All System Components

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

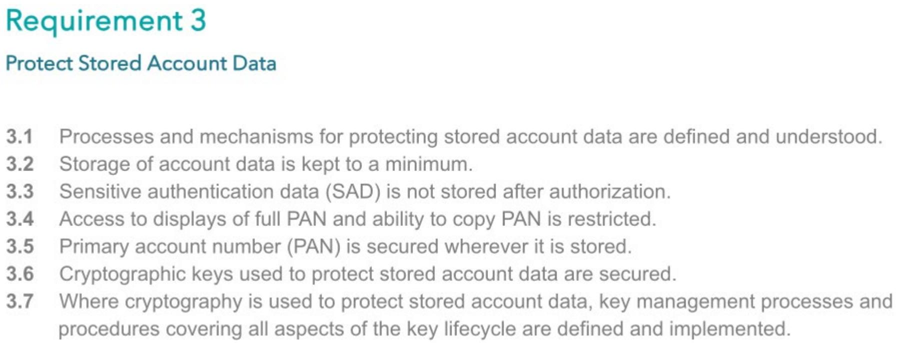
2.2 System components are configured and managed securely.

2.3 Wireless environments are configured and managed securely.

PCI DSS – Protect Cardholder Data



Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks



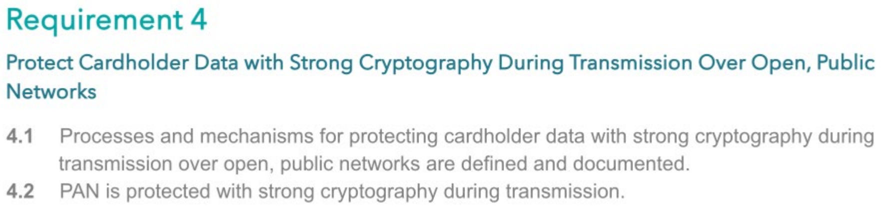
Requirement 3

Protect Stored Account Data

3.1 Processes and mechanisms for protecting stored account data are defined and understood.
3.2 Storage of account data is kept to a minimum.
3.3 Sensitive authentication data (SAD) is not stored after authorization.
3.4 Access to displays of full PAN and ability to copy PAN is restricted.
3.5 Primary account number (PAN) is secured wherever it is stored.
3.6 Cryptographic keys used to protect stored account data are secured.
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

Minimize storage of CHD.
Limited access based on business need
Changes:
- must encrypt entire pan, not just parts
- disk encryption for removeable media only

Encryption does not take a data source out of scope

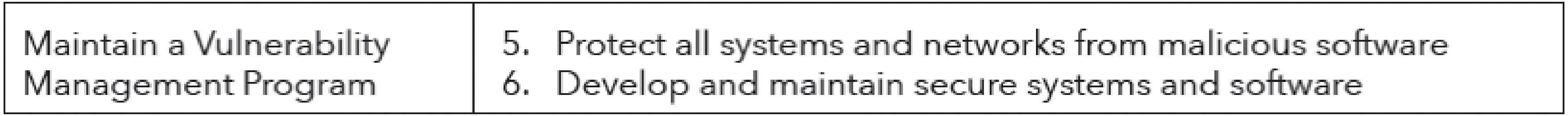


Requirement 4

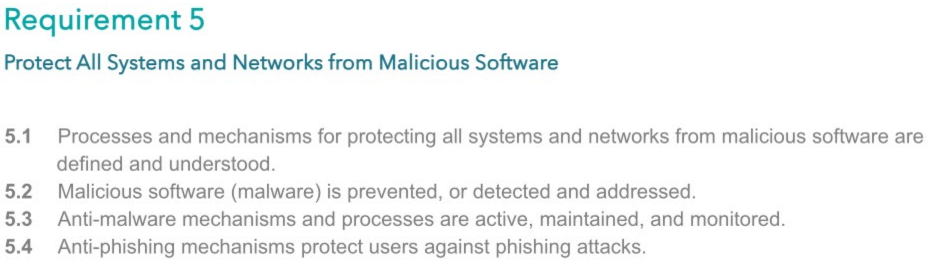
Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.
4.2 PAN is protected with strong cryptography during transmission.

PCI DSS – Maintain Vulnerability Management Program



Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software



Requirement 5

Protect All Systems and Networks from Malicious Software

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

There is “overlap” between Requirement 5 and Requirement 10 related to AV logging and monitoring.

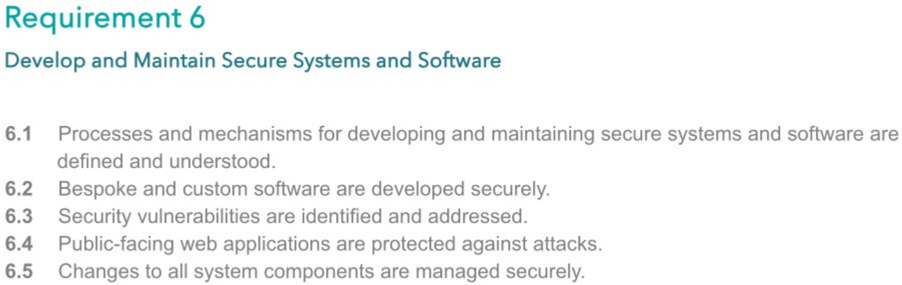
CHANGES:

- more flexibility regarding anti-virus

- controls for detection and prevention of phishing

There is “overlap” between Requirement 6 and Requirement 11 related to vulnerability classifications and management.

Hardening guidelines from:
CIS: http://www.cisecurity.org/
NIST : National Checklist Repository
Microsoft: Security Baselines



Requirement 6

Develop and Maintain Secure Systems and Software

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

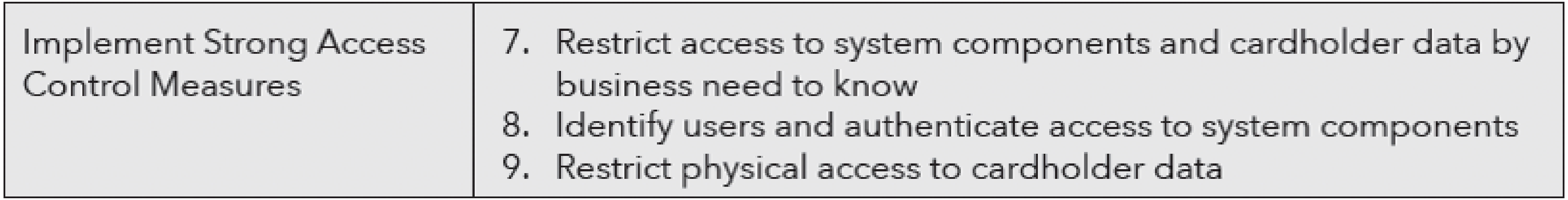
6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

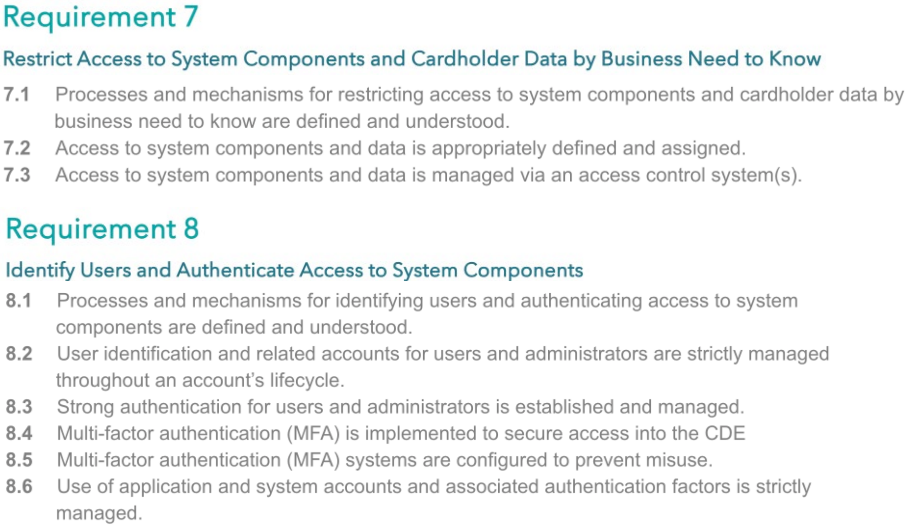
6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

PCI DSS – Implement Strong Access Controls



Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data



Requirement 7

Restrict Access to System Components and Cardholder Data by Business Need to Know

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

7.2 Access to system components and data is appropriately defined and assigned.

7.3 Access to system components and data is managed via an access control system(s).

Requirement 8

Identify Users and Authenticate Access to System Components

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

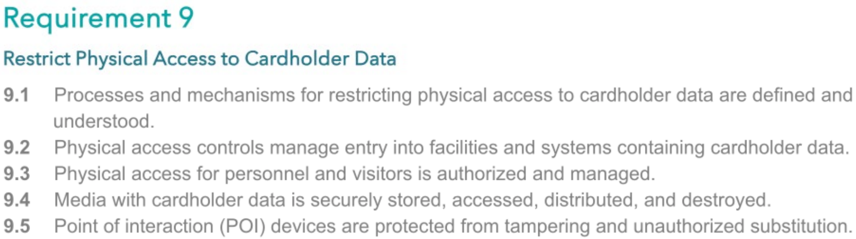
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.



Requirement 9

Restrict Physical Access to Cardholder Data

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

Principle of minimum access – defined business need

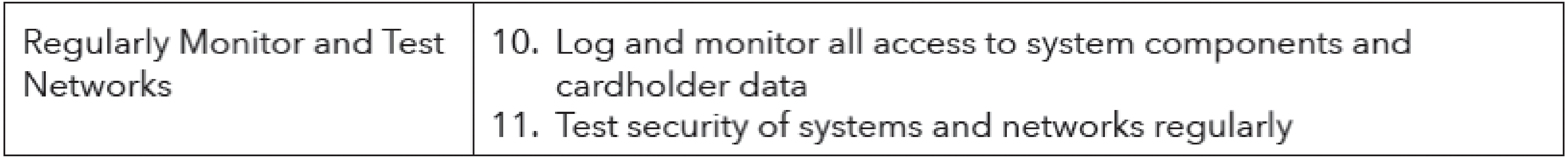
Limit and monitor physical access – track media

CHANGES:

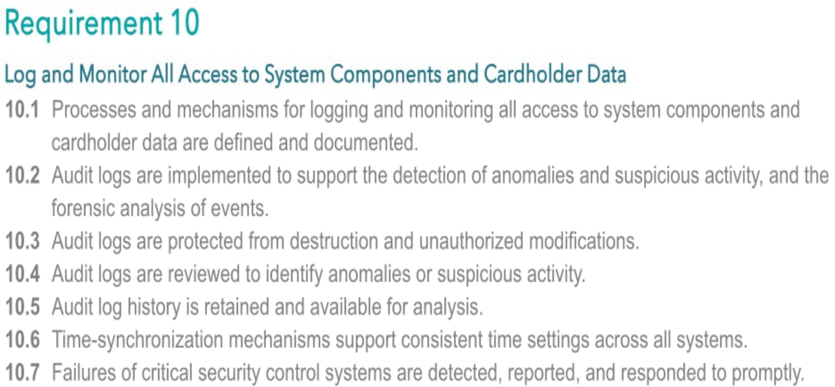
- Password "rules" are changing…

- MFA requirements are changing

PCI DSS – Regularly Monitor and Test Networks



Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly



Requirement 10

Log and Monitor All Access to System Components and Cardholder Data

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

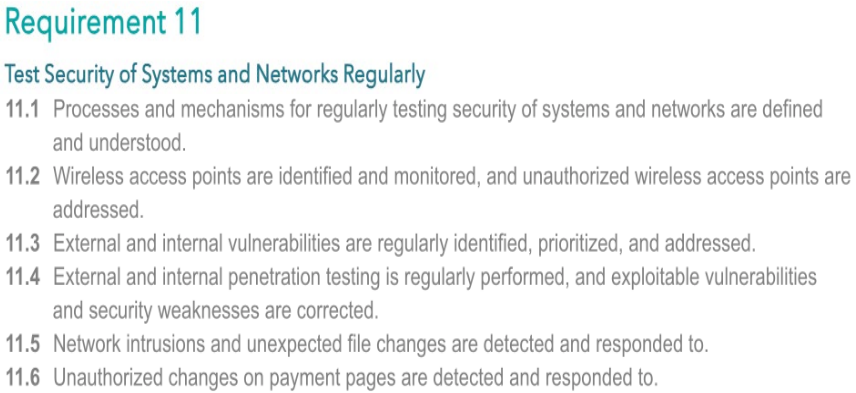
10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Secure the logs and limit access
Audit log access and retention – 3 Months/12 months
Log review automation

CHANGES:

- Only automated mechanisms allowed for reviewing



Requirement 11

Test Security of Systems and Networks Regularly

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

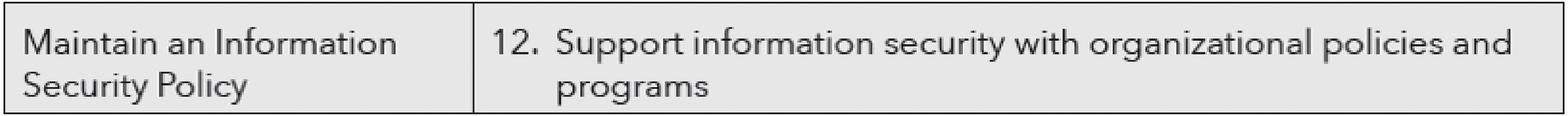
11.6 Unauthorized changes on payment pages are detected and responded to.

Testing cycles: Quarterly, Semi-Annually, Annually…
AND… after significant change
Independent from the administration responsibility

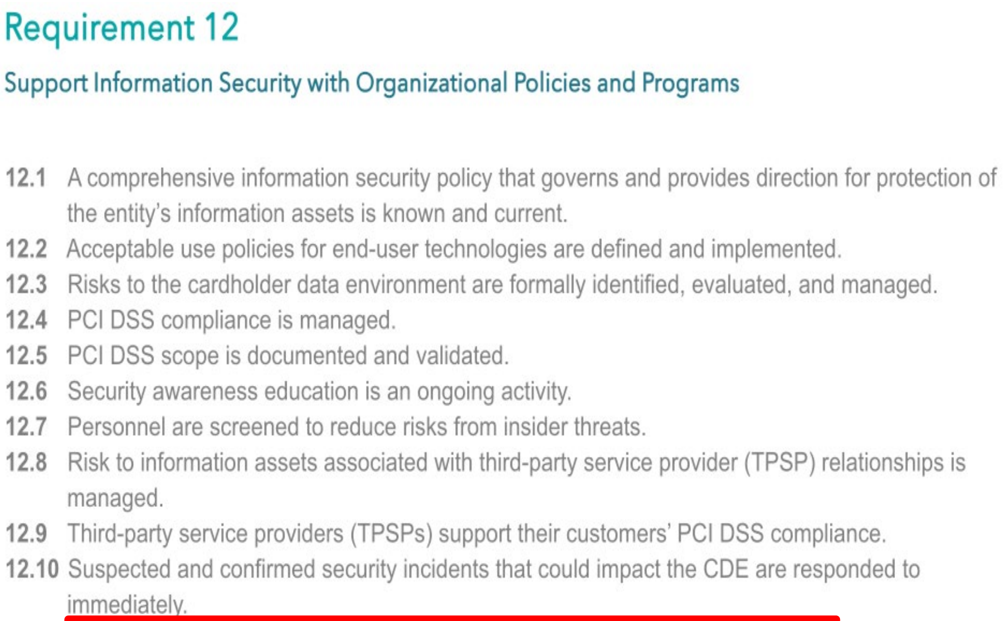
CHANGES:

- Internal vulnerability scans must be authenticated
- Web applications must have automated WAF's
- Additional payment page protections…

PCI DSS – Maintain Information Security Policy



Maintain an Information Security Policy	12. Support information security with organizational policies and programs



Requirement 12

Support Information Security with Organizational Policies and Programs

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

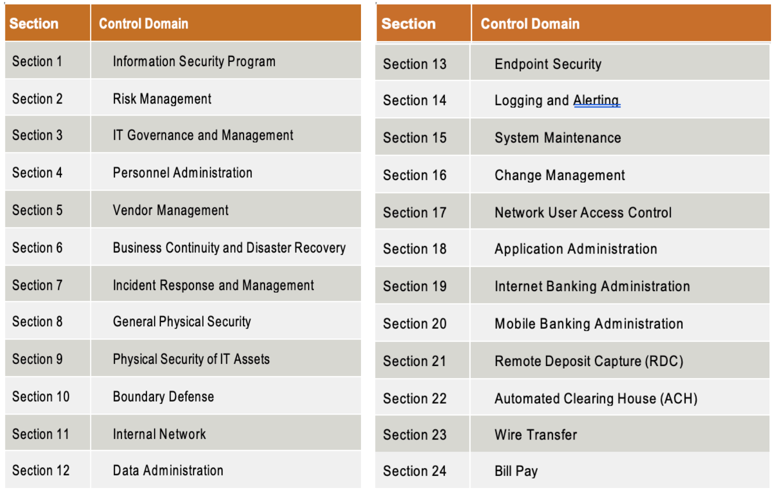
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

CHANGES:

- "Targeted Risk Assessments"

Polices and standards need to reference specificity called for by PCI controls



Section	Control Domain	Section	Control Domain
Section 1	Information Security Program	Section 13	Endpoint Security
Section 2	Risk Management	Section 14	Logging and Alerting
Section 3	IT Governance and Management	Section 15	System Maintenance
Section 4	Personnel Administration	Section 16	Change Management
Section 5	Vendor Management	Section 17	Network User Access Control
Section 6	Business Continuity and Disaster Recovery	Section 18	Application Administration
Section 7	Incident Response and Management	Section 19	Internet Banking Administration
Section 8	General Physical Security	Section 20	Mobile Banking Administration
Section 9	Physical Security of IT Assets	Section 21	Remote Deposit Capture (RDC)
Section 10	Boundary Defense	Section 22	Automated Clearing House (ACH)
Section 11	Internal Network	Section 23	Wire Transfer
Section 12	Data Administration	Section 24	Bill Pay

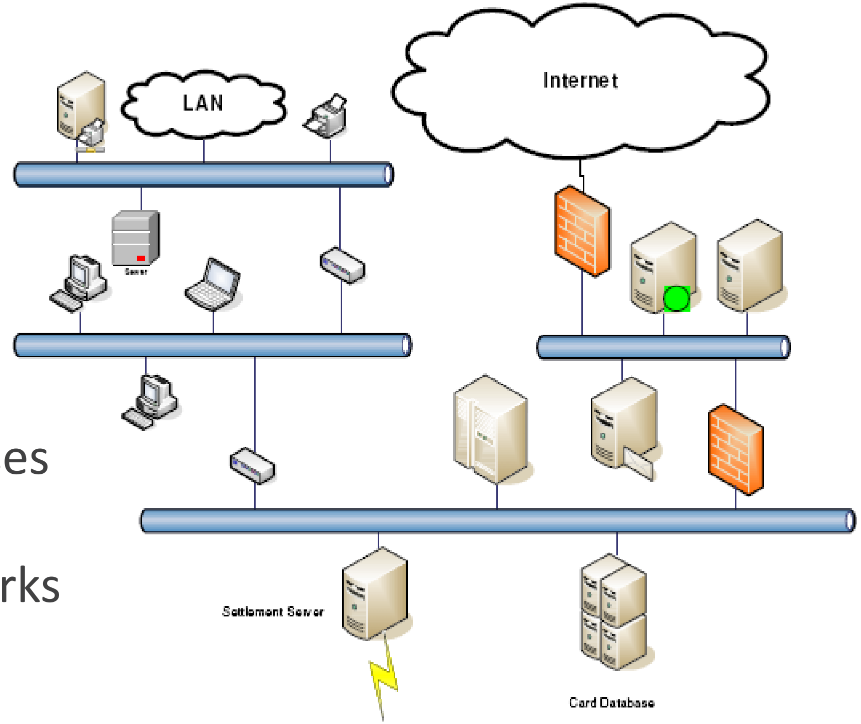
How PCI Relates to Financial Institutions

Define scope of People, Processes and Technology

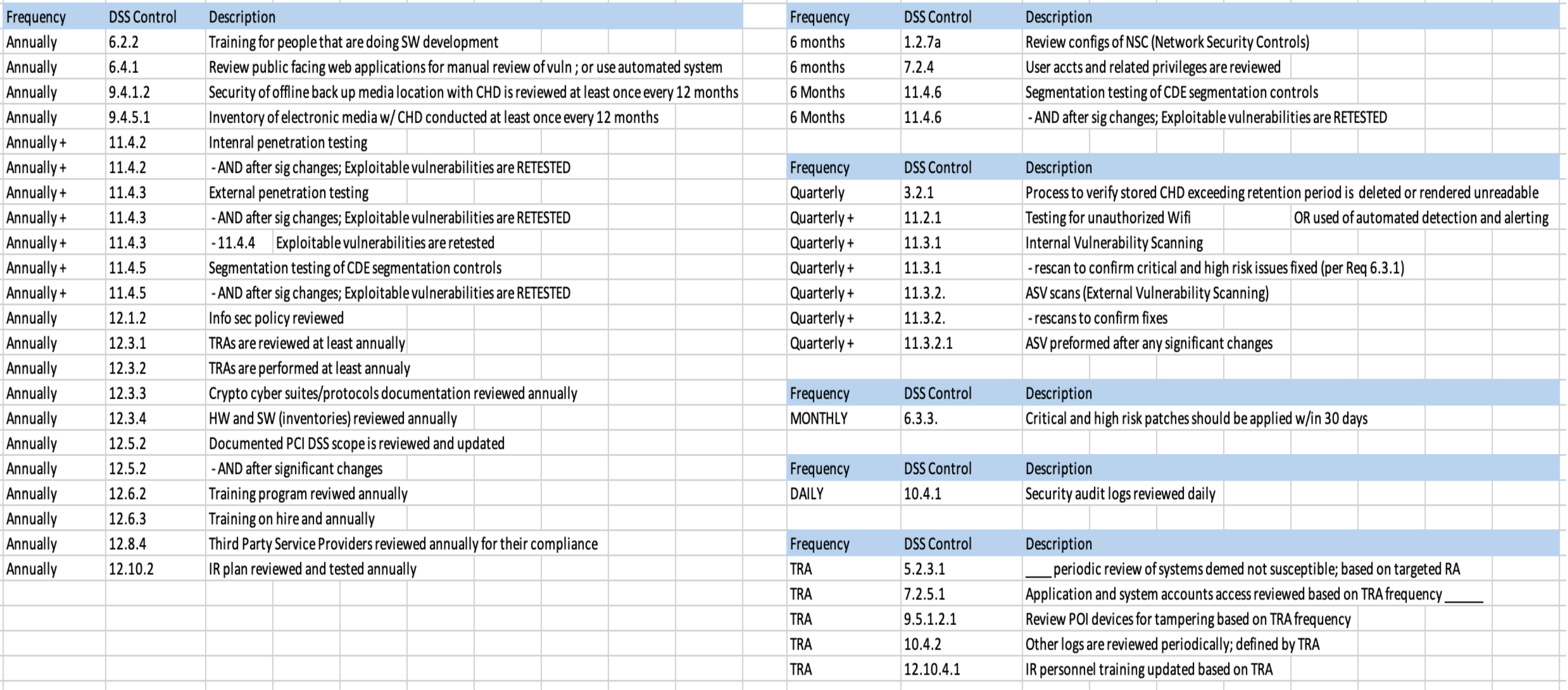
- How do you accept CC payment “in-person”?
- How do you accept CC payment over the phone?
- How do you accept CC payment via a website?
- How do you rely on a vendor to host or manage any of your data systems?
- How do you store or process CC data for your members?
- How do you store or process CC data for someone else?
- Where do you have instant issue capabilities?
- How are ATMs connected “on your network”?

Understand Where Your Data Lives

- Develop data inventory
  - Payment/data flow
  - Where static data resides
- Understand which systems/applications are linked (interfaces)
- Who is mining data and for what purposes
- Understand how the back up system works



Schedule of Things That Need To Occur Regularly



Frequency	DSS Control	Description
Annually	6.2.2	Training for people that are doing SW development
Annually	6.4.1	Review public facing web applications for manual review of vuln ; or use automated system
Annually	9.4.1.2	Security of offline back up media location with CHD is reviewed at least once every 12 months
Annually	9.4.5.1	Inventory of electronic media w/ CHD conducted at least once every 12 months
Annually +	11.4.2	Intenral penetration testing
Annually +	11.4.2	- AND after sig changes; Exploitable vulnerabilities are RETESTED
Annually +	11.4.3	External penetration testing
Annually +	11.4.3	- AND after sig changes; Exploitable vulnerabilities are RETESTED
Annually +	11.4.3	- 11.4.4 Exploitable vulnerabilities are retested
Annually +	11.4.5	Segmentation testing of CDE segmentation controls
Annually +	11.4.5	- AND after sig changes; Exploitable vulnerabilities are RETESTED
Annually	12.1.2	Info sec policy reviewed
Annually	12.3.1	TRAs are reviewed at least annually
Annually	12.3.2	TRAs are performed at least annualy
Annually	12.3.3	Crypto cyber suites/protocols documentation reviewed annually
Annually	12.3.4	HW and SW (inventories) reviewed annually
Annually	12.5.2	Documented PCI DSS scope is reviewed and updated
Annually	12.5.2	- AND after significant changes
Annually	12.6.2	Training program reviwed annually
Annually	12.6.3	Training on hire and annually
Annually	12.8.4	Third Party Service Providers reviewed annually for their compliance
Annually	12.10.2	IR plan reviewed and tested annually

Frequency	DSS Control	Description
6 months	1.2.7a	Review configs of NSC (Network Security Controls)
6 months	7.2.4	User accts and related privileges are reviewed
6 Months	11.4.6	Segmentation testing of CDE segmentation controls
6 Months	11.4.6	- AND after sig changes; Exploitable vulnerabilities are RETESTED

Frequency	DSS Control	Description
Quarterly	3.2.1	Process to verify stored CHD exceeding retention period is deleted or rendered unreadable
Quarterly +	11.2.1	Testing for unauthorized Wifi OR used of automated detection and alerting
Quarterly +	11.3.1	Internal Vulnerability Scanning
Quarterly +	11.3.1	- rescan to confirm critical and high risk issues fixed (per Req 6.3.1)
Quarterly +	11.3.2.	ASV scans (External Vulnerability Scanning)
Quarterly +	11.3.2.	- rescans to confirm fixes
Quarterly +	11.3.2.1	ASV preformed after any significant changes

Frequency	DSS Control	Description
MONTHLY	6.3.3.	Critical and high risk patches should be applied w/in 30 days

Frequency	DSS Control	Description
DAILY	10.4.1	Security audit logs reviewed daily

Frequency	DSS Control	Description
TRA	5.2.3.1	___ periodic review of systems demed not susceptible; based on targeted RA
TRA	7.2.5.1	Application and system accounts access reviewed based on TRA frequency _____
TRA	9.5.1.2.1	Review POI devices for tampering based on TRA frequency
TRA	10.4.2	Other logs are reviewed periodically; defined by TRA
TRA	12.10.4.1	IR personnel training updated based on TRA

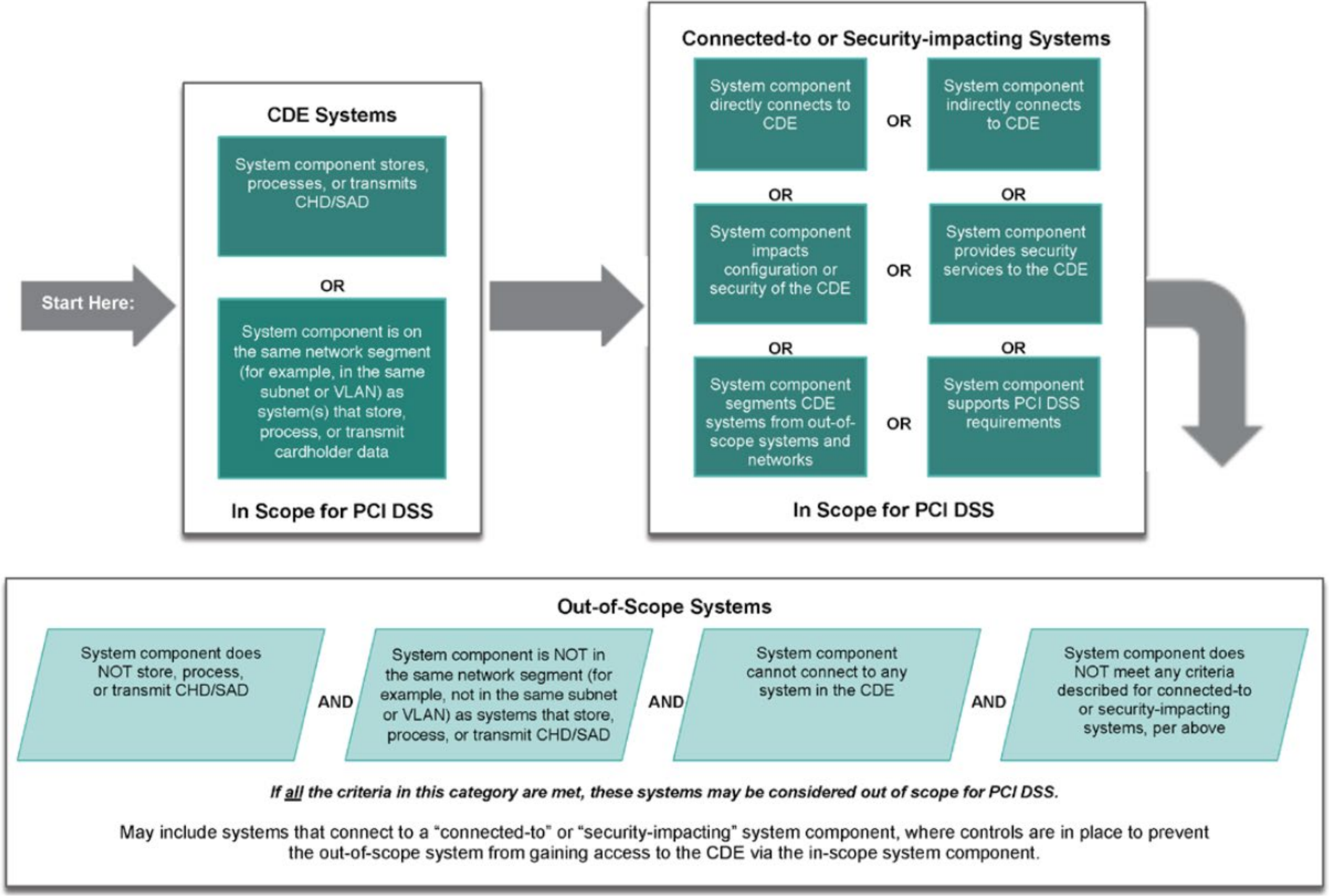
Use of Third-Party Service Providers

- If a third-party stores, process, or transmits CHD on your behalf they are in scope for your assessment

- Third-parties may provide an Attestation of Compliance (AOC) which must be reviewed during your assessment

- Outsourcing a process to a third party does not eliminate your responsibility… (1) for the data, (2) for compliance, or (3) for a breach

- You need a Service Provider Responsibility Matrix



Start Here:

CDE Systems

System component stores, processes, or transmits CHD/SAD

OR

System component is on the same network segment (for example, in the same subnet or VLAN) as system(s) that store, process, or transmit cardholder data

In Scope for PCI DSS

Connected-to or Security-impacting Systems

System component directly connects to CDE

OR

System component indirectly connects to CDE

OR

OR

System component impacts configuration or security of the CDE

OR

System component provides security services to the CDE

OR

OR

System component segments CDE systems from out-of-scope systems and networks

OR

System component supports PCI DSS requirements

In Scope for PCI DSS

Out-of-Scope Systems

System component does NOT store, process, or transmit CHD/SAD

AND

System component is NOT in the same network segment (for example, not in the same subnet or VLAN) as systems that store, process, or transmit CHD/SAD

AND

System component cannot connect to any system in the CDE

AND

System component does NOT meet any criteria described for connected-to or security-impacting systems, per above

If all the criteria in this category are met, these systems may be considered out of scope for PCI DSS.

May include systems that connect to a “connected-to” or “security-impacting” system component, where controls are in place to prevent the out-of-scope system from gaining access to the CDE via the in-scope system component.

Common Challenges for Financial Institutions

- Isolation/segmentation is difficult (or impossible)
  - CHD is in the core – everything/everyone interacts with the core

- Card data is received over the phone
  - Phone calls contain PAN – transmitted electronic CHD
  - Service center records phone calls – stored electronic CHD
  - Phone systems is Voice over IP
    - touches everything… is integrated to everything…

➢ This makes all systems on the network in scope

Common Challenges for Financial Institutions

- Data warehouse and analytics…
  - Reports (PDF, XLSX, etc.) contain PAN
    - Core/vendor software generates reports with PAN data
    - These reports exist in email and on network file shares

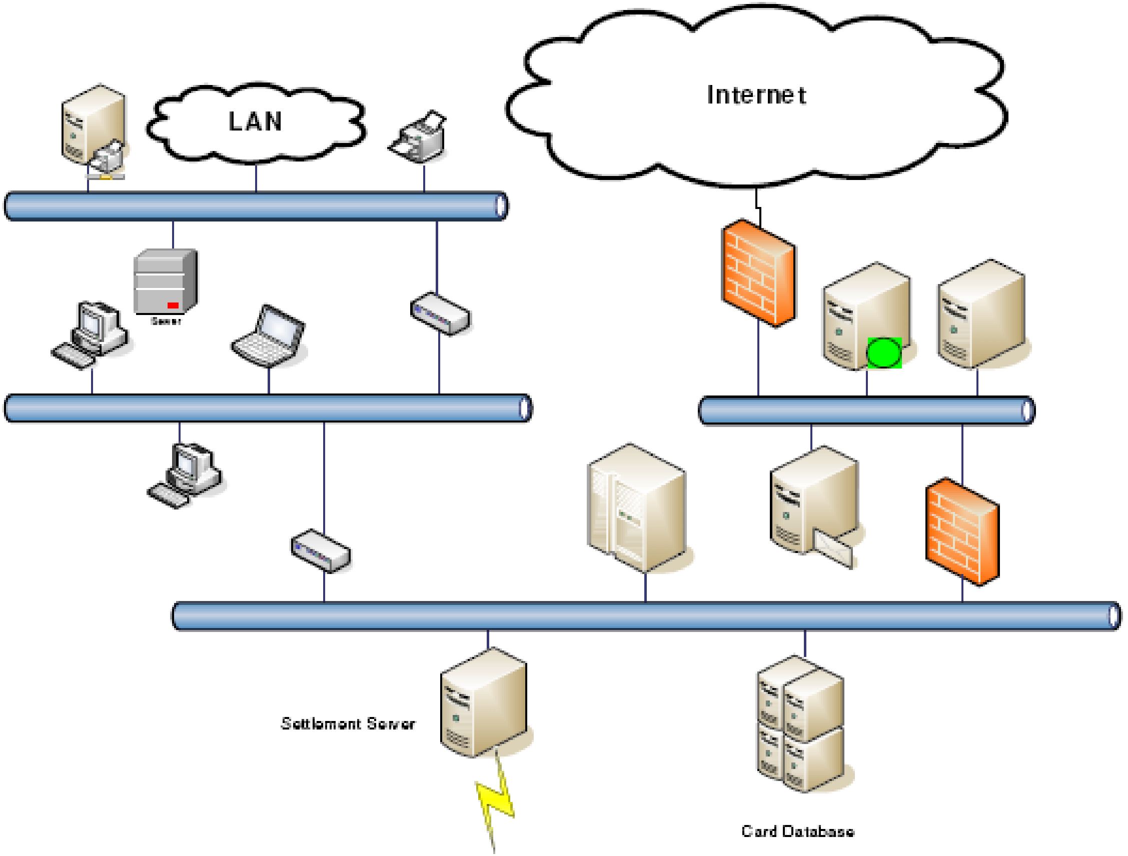
- Vendor software doesn’t follow PCI guidelines
  - Instant issue systems store SAD
  - Vendor software stores clear-text PAN

Exercise - Segment Your Network

- What is in-scope here?

- ➢ NOTHING
- ➢ Firewalls
- ➢ Servers
- ➢ PCs
- ➢ Everything

- Why?

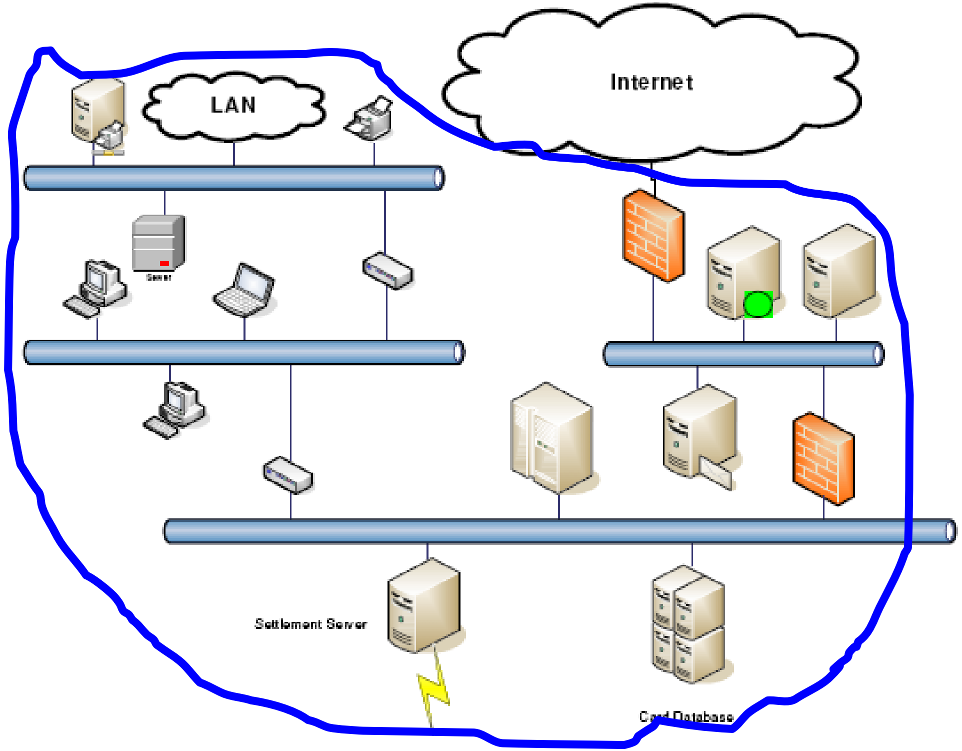


Exercise - Segment Your Network

- What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

- Why?

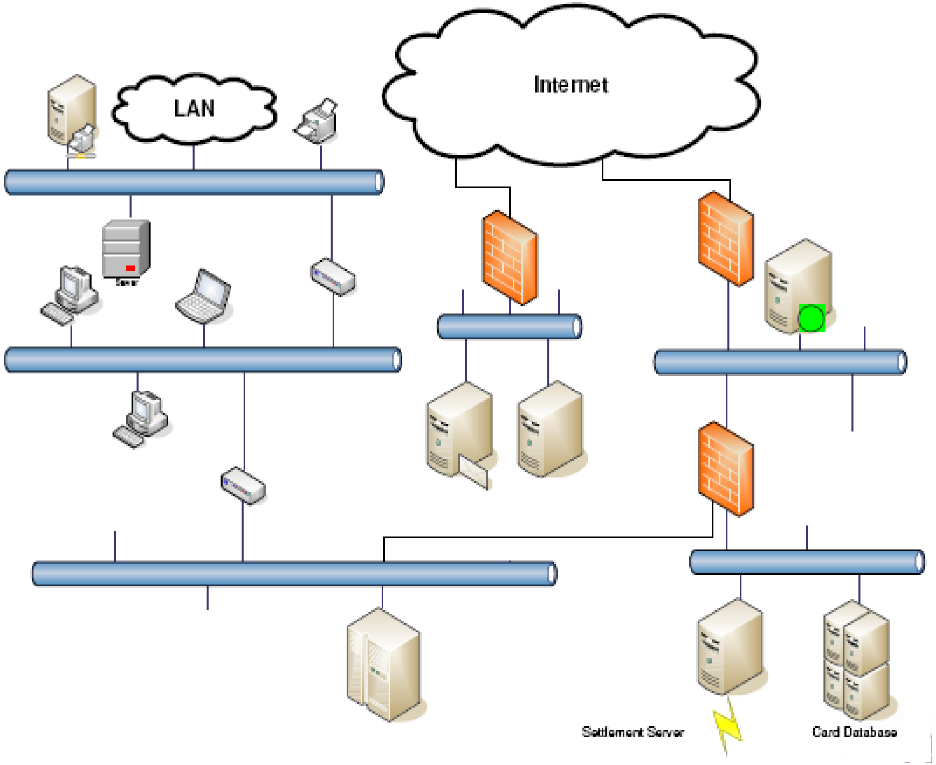


Segment Your Network

What is in-scope here?

- ➢NOTHING
- ➢Firewalls
- ➢Servers
- ➢PCs
- ➢Everything

Why?

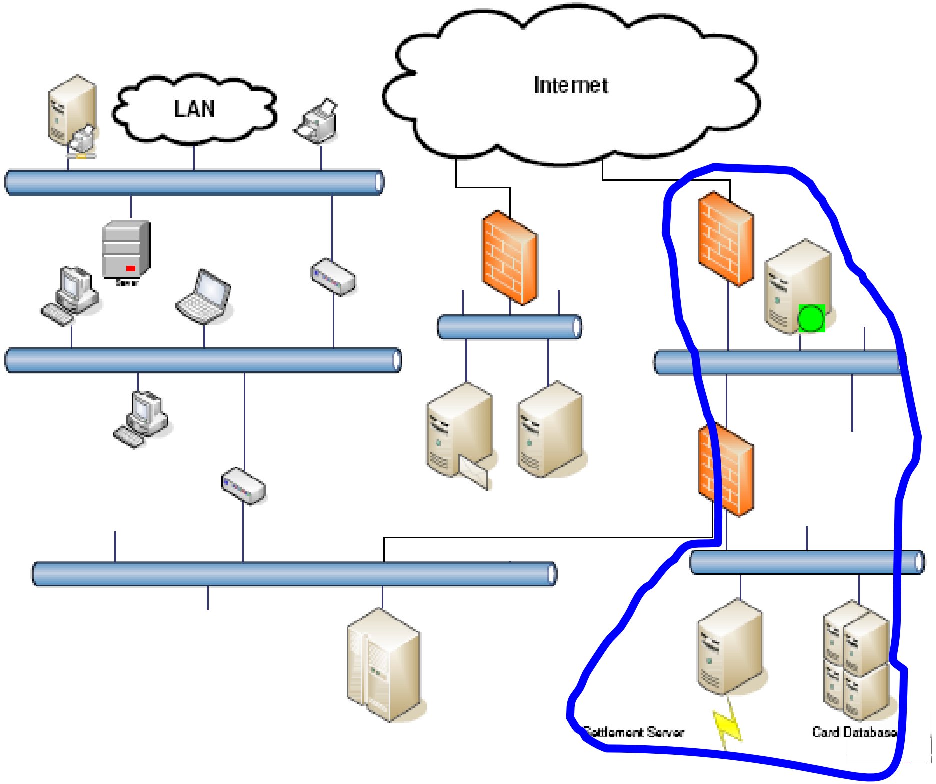


Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?



Summary

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Summarize

1. Financial Institutions need to be PCI compliant
    - Contractual obligation
    - Report as an Issuer
2. There are no “PCI Police” looking for you
3. Some examiners are starting to ask about compliance status
4. Financial Institutions could also be Merchant or Service Provider

Summarize

5. The Financial Institution likely is not compliant right now
6. Start the process
   - ○ Complete a Readiness Assessment
   - ○ Map your controls
   - ○ Utilized Prioritized Approach
   - ○ Identify where card data lives and how it flows through environment
   - ○ Update policies and processes to address PCI requirements
   - ○ Make progress, even if you can’t get all the way there right now…
   - ○ Implement PCI controls into Daily Business as Usual

Questions

Thank You!

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA
Principal, Cybersecurity
612-397-3114
randy.romes@CLAconnect.com

John Moeller, CISSP, CISA
Principal, Cybersecurity
319-558-0282
john.moeller@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Resources

- PCI Website: PCISecurityStandards.org

  Document library

  https://www.pcisecuritystandards.org/document_library

  DSS

  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1632414383382

  Prioritized approach (description and tool)

  https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1632414383404

  https://www.pcisecuritystandards.org/documents/Prioritized-Approach-Tool-v3_2_1.xlsx?agreement=true&time=1632414383408

- CIS – Audit Scripts Mapping Tool

  https://www.auditscripts.com/download/2742/