



PCI Compliance For Credit Unions

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

CLA – A Professional Services Firm


- A professional services firm with three distinct business lines
 - Audit
 - Tax
 - Outsourcing
 - Wealth Advisory
 - Digital Transformation
- More than 8,500 professionals
- Offices coast to coast
- Serve more than 1,500 financial institutions



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

- Top Firm for Credit Unions

CLA is recognized as the #1 auditor of credit unions in the country by Callahan & Associates.



WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

 703-825-2168 | [CLAconnect.com](https://www.CLAconnect.com)

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

Cyber Security Services

Information Security offered as specialized service offering for over 25 years

- Largest Credit Union Service Practice*
- Penetration Testing and Vulnerability Assessment
 - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (GLBA, FFIEC, CIS, etc...)
- **PCI-DSS Readiness and Compliance Assessments**
- Incident response and forensics
- Independent security consulting
- Internal audit support
- **At last count... CLA was one of only 12 firms in the nation with all three of these designations/affiliations/capabilities**



*Callahan and Associates 2021 Guide to Credit Union CPA Auditors.





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.

C:\whoami

- “Professional Student”
- Science Teacher / Self Taught Computer Guy
- IT Consultant - Project Manager – IT Staff/Help Desk - Hacker
- Assistant Scout Master (Boy Scouts)



Exercise

- 5 Minute exercise...
- Think about how/where your Credit Union stores, processes, or transmits credit card information
- Think in terms of the steps/stages followed
 - Examples:
 - ♣ Accept payment information over the phone
 - ♣ Members make payments online
 - ♣ Receive payment information in the mail
 - ♣ Member statements are sent/stored/reviewed by member services reps
- End Goal is to understand “where the card data lives”



PCI - DSS Overview

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

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

Before PCI DSS

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



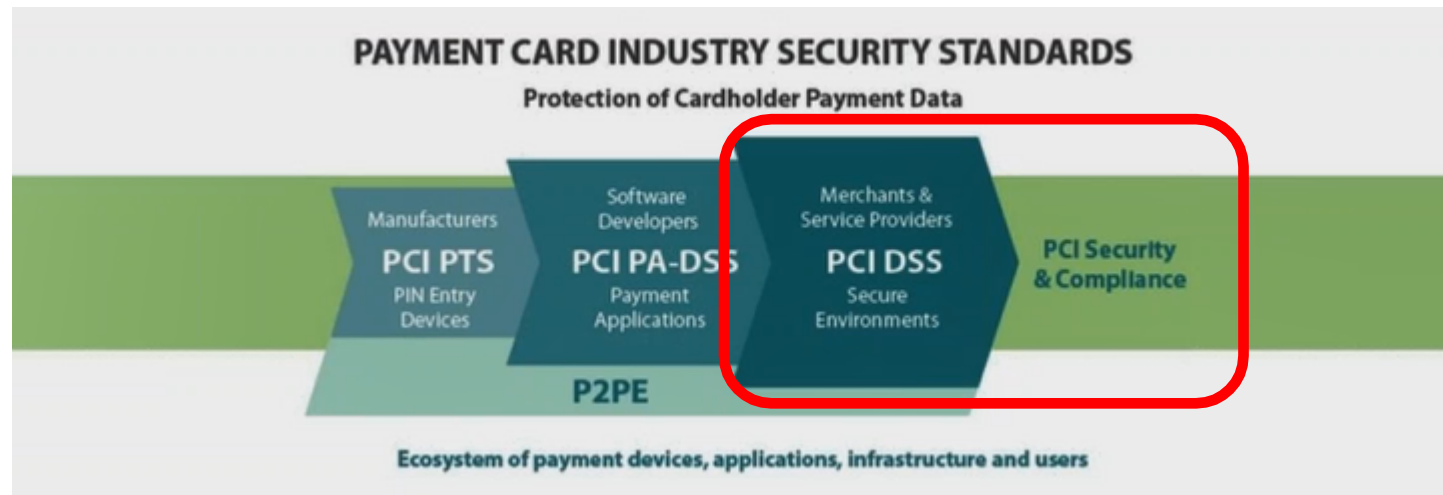
Merchants and processors who accepted multiple brands of cards needed to have a separate compliance program for each.

- 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



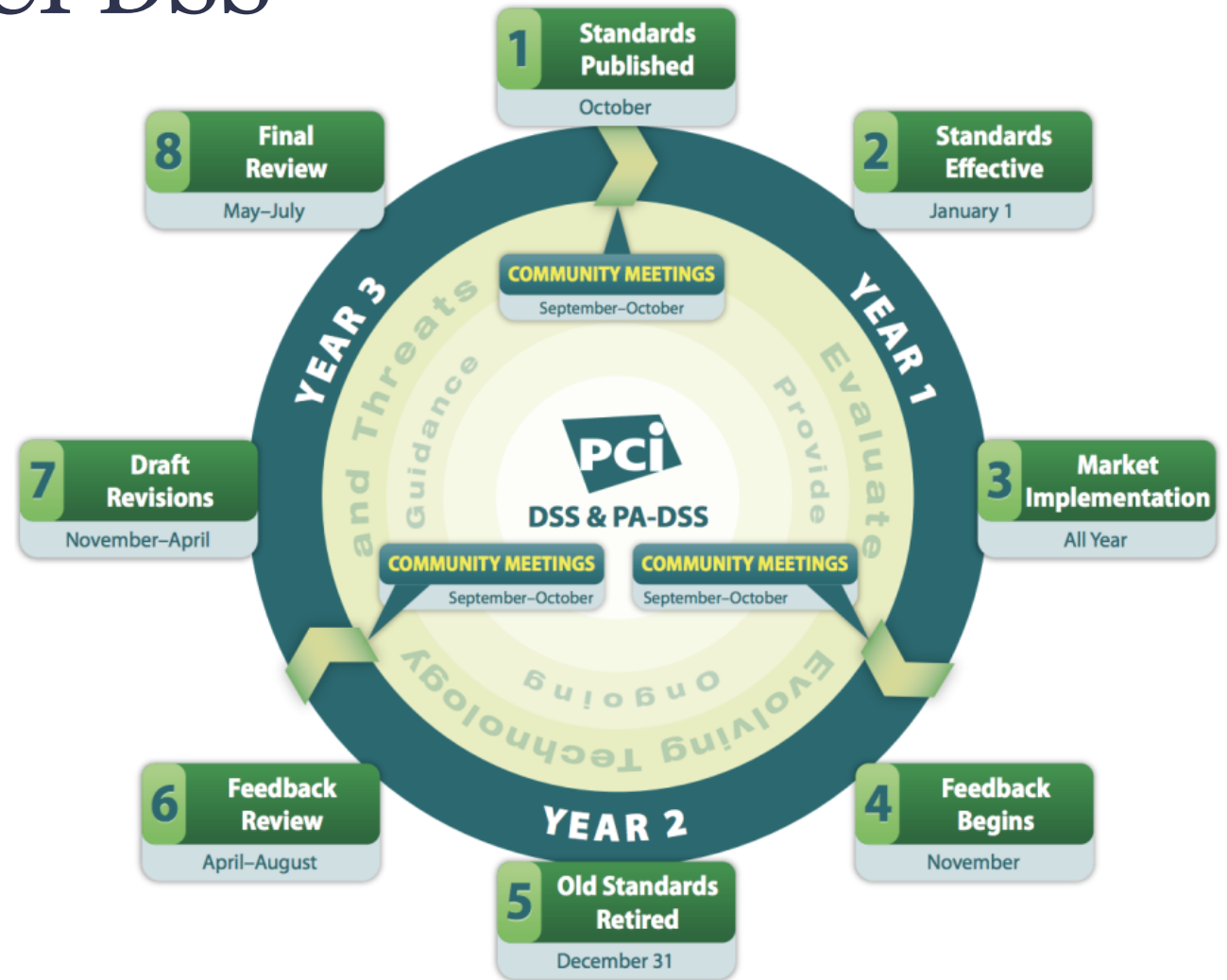
The PCI Security Standards

- **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.



Lifecycle Changes to PCI DSS

- Current version is 3.2.1 (May 2018)
- Version 4 is out and entities have until March 2024...



- *****[.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf](https://pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf)

PCI DSS Requirements

“The Digital Dozen”

Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel



Cardholder Data (CHD)

The PCI DSS defines CHD to be:

At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following:
cardholder name, expiration date and/or service code.”

- **PAN** – Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
- **Service Code** – Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
- **SAD** – Acronym for “sensitive authentication data.” Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.



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, ***including any connected system components.***

- **Store** – when cardholder data is inactive or at rest (e.g., located on electronic media, 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...*



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 Credit Union?



PCI Merchant Levels

Merchant Level	Merchant Definition	Compliance
Level 1	More than 6 million V/MC transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 2	1,000,000 – 5,999,999 V/MC transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 3	20,000 – 1,000,000 V/MC e-commerce transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 4	Less than 20,000 e-commerce V/MC transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing



PCI Service Provider Levels

Service Provider Level	Service Provider Definition	Compliance
Level 1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year.	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing
Level 2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year.	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing

Compliance and Certification

Every organization that stores, processes, or transmits credit card data needs to comply with all DSS standards. This includes Service Providers and Issuers.

Depending on the type and size of the organization you must (may need to?) annually attest compliance 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 all FI's and Issuers must be PCI compliant.

- [*****usa.visa.com/partner-with-us/pci-dss-compliance-information.html](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.

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

PCI Security Standards Council

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?	<ul style="list-style-type: none">Review documented process.Interview personnel.Examine network configurations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none">Review current network diagram.Examine network configurations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a process to ensure the diagram is kept current?	<ul style="list-style-type: none">Interview responsible personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	<ul style="list-style-type: none">Review current dataflow diagram.Examine network configurations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a process to ensure the diagram is kept current?	<ul style="list-style-type: none">Interview personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



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 service providers and 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 AOC

6. Findings and Observations							
Build and Maintain a Secure Network and Systems							
Requirement 1: Install and maintain a firewall configuration to protect cardholder data							
PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			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:	Identify the document(s) reviewed to verify procedures define the formal processes for:						
• Network connections, and	• Testing and approval of all network connections.	Art-1_XXX Information Security Policy 1.90.pdf, (page 23 and 78)					
• Changes to firewall and router configurations.	• 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 XXX XXX - 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 XXX XXX - 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





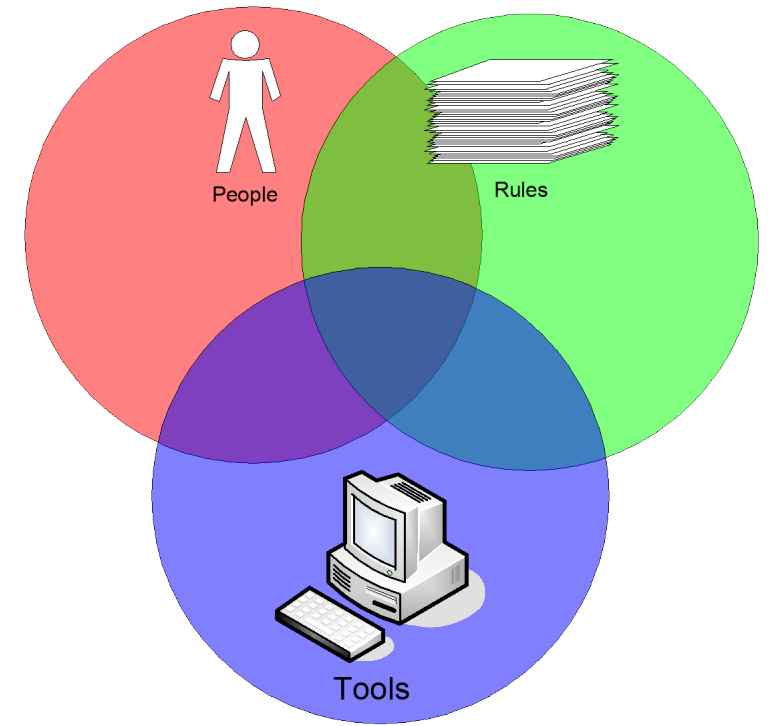
PCI - DSS The Framework

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

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?
- ❏ PCI is all about **“Daily Business as Usual”**
- ❏ Standards based operations from a governance or compliance framework:
 - GLBA, FFIEC, (State Laws?)----- *Regulatory*
 - **PCI – DSS**, CMMC ----- **Contractual**
 - CIS Critical Controls, NIST ----- *Operational standards*



Overview – PCI DSS – “Digital Dozen”

Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel

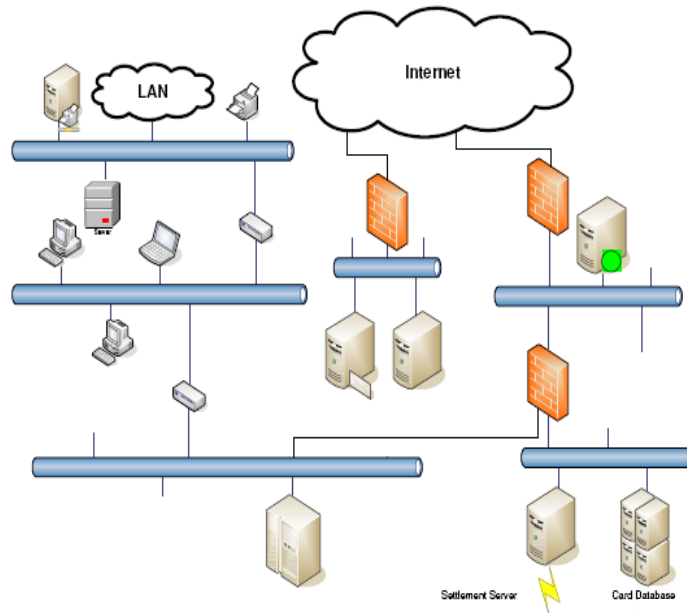
Six Goals and Twelve Requirements

- ~ 140 Controls
 - Three elements to each control
- ◇ 420 “things to address”



PCI DSS – Build & Maintain a Secure Network

	Goals	PCI DSS Requirements
1	Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters



Default password lists:

- *****.phenoelit-us.org/
- *****.cirt.net/passwords
- ***.google.com
 - ▢ “default password”

People
Processes
Technology



PCI DSS – Protect Cardholder Data

	Goals	PCI DSS Requirements
2	Protect Cardholder Data	3. Protect stored cardholder data
		4. Encrypt transmission of cardholder data across open, public networks

- Minimize storage
 - Implement data retention and disposal policies
 - Do NOT store sensitive authentication data
 - Mask displayed PAN
 - Render PAN unreadable where stored
 - Protect cryptographic keys
- **ADDITION: NEVER send unprotected PAN by end user messaging (email, chat, IM, etc...)**

Encryption does not take a data source out of scope

PCI DSS – Maintain Vulnerability Mgmt Program

	Goals	PCI DSS Requirements
3	Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
		6. Develop and maintain secure systems and applications

- “Use anti-virus...”
- Secure software development and change control...
- Secure build checklists:
 - CIS offers vendor-neutral hardening resources
*****.cisecurity.org/
 - Microsoft Security Checklists
*****.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true
*****technet.microsoft.com/en-us/library/dd366061.aspx
 - PA-DSS “certified” applications will have an Implementation Guide

There is overlap between Requirement 6 and Requirement 11.



PCI DSS – Implement Strong Access Controls

	Goals	PCI DSS Requirements
4	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

- Principle of minimum access and least privilege
- Unique IDs (◇ NO shared IDs)
- Long/strong passwords, password controls, strong authentication
- Limit and monitor physical access
- Secure storage and tracking of media

Password “rules”
are changing...

PCI DSS – Regularly Monitor and Test Networks

	Goals	PCI DSS Requirements
5	Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
		11. Regularly test security systems and processes

- Process, system, and application logging
- Secure the audit logs
- Review and retain audit logs
- Regular testing:
 - Quarterly*: Wireless testing & Vulnerability scanning
 - Annual*: Penetration testing
- IDS/IPS and
- File integrity monitoring

PCI DSS – Maintain Information Security Policy

	Goals	PCI DSS Requirements
6	Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Section	Control Domain	Section	Control Domain
Section 1	Information Security Program	Section 13	Endpoint Security
Section 2	Risk Management	Section 14	Logging and <u>Alerting</u>
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 Credit Unions

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

Exercise

- Think about how your credit union stores, processes, or transmits credit card information
- Understand who (needs to) interact(s) with CHD
- Think in terms of the steps/stages followed
- End Goal is to understand “where the card data lives”

Exercise

- Do you accept CC payment “in-person”?
- Do you accept CC payment over the phone?
- Do you accept CC payment via a website?
- Do you rely on a 3rd party/vendor to host or manage any of your data systems?
- Do you store or process CC data for your members?
- Do you store or process CC data for someone else?
- Do you have instant issue capabilities?
- Are ATMs “on your network”?



Use of Third-Party Service Providers

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

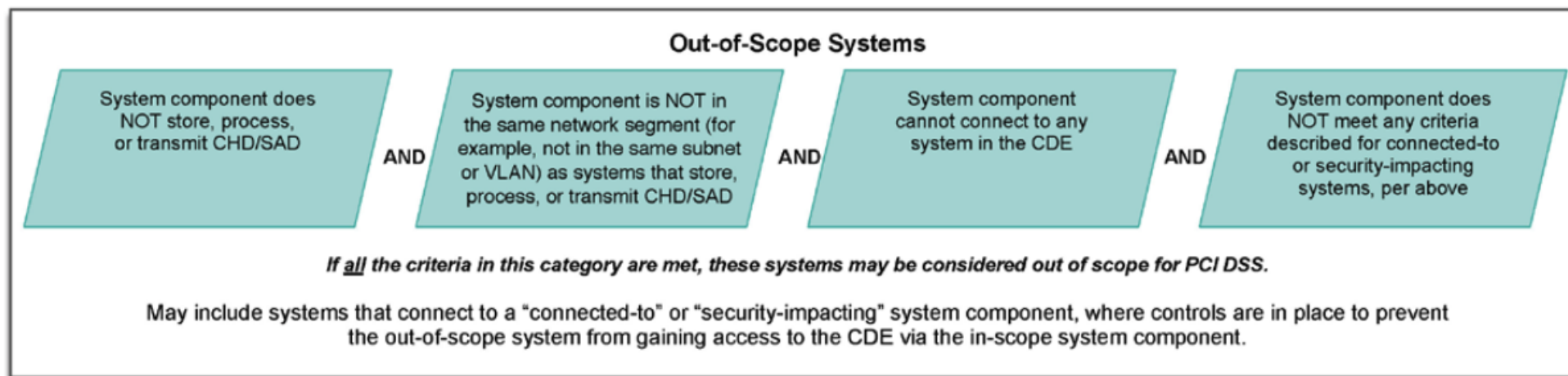
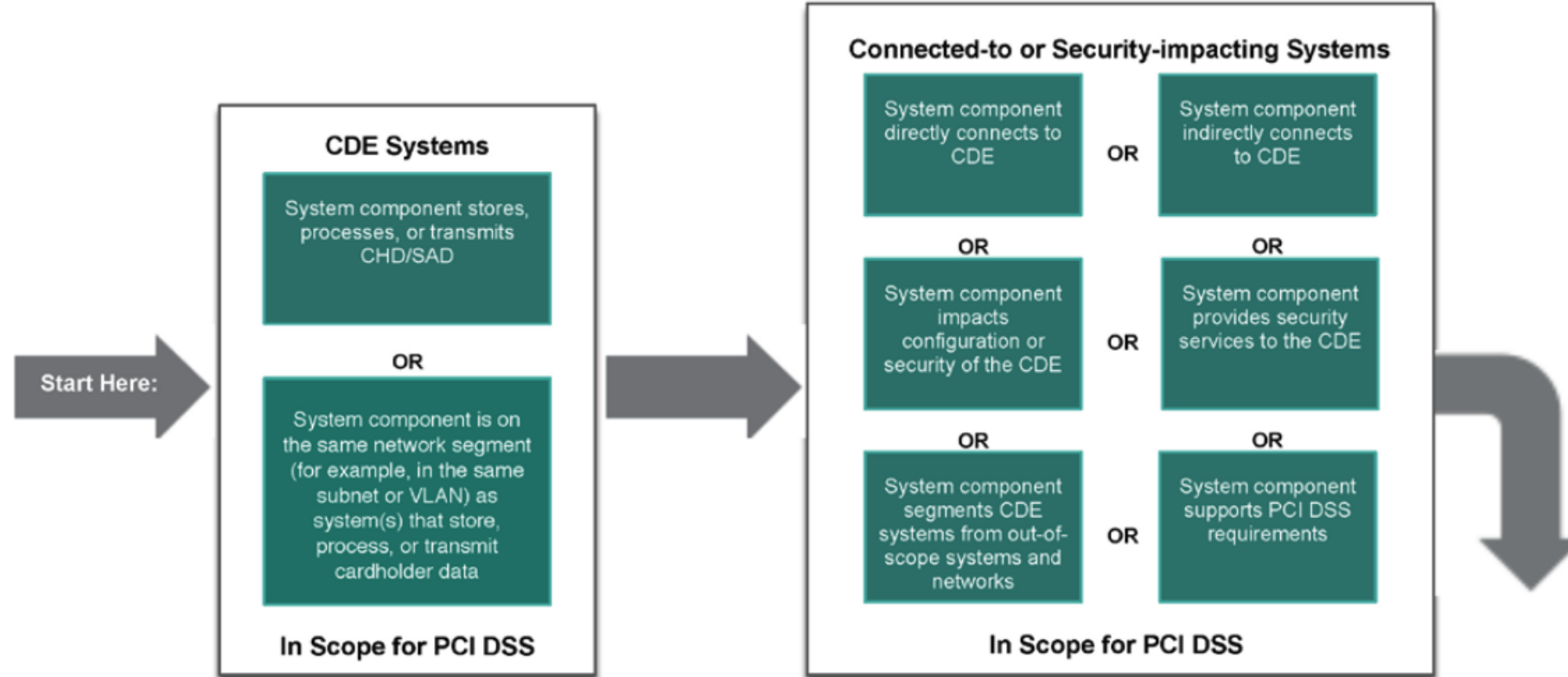


Applicability

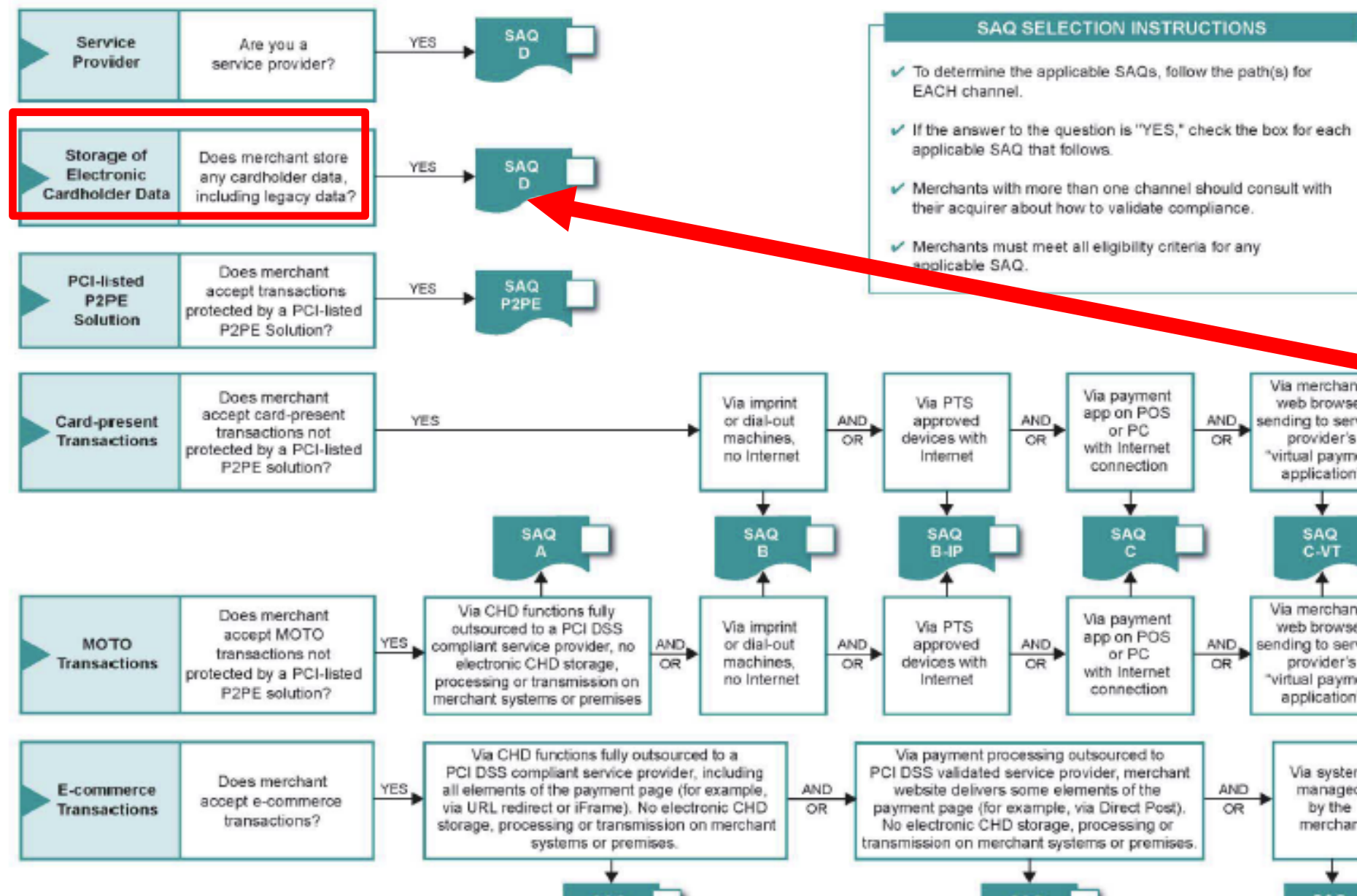
Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
<ul style="list-style-type: none">▪ Primary Account Number (PAN)▪ Cardholder Name▪ Expiration Date▪ Service Code	<ul style="list-style-type: none">▪ Full track data (magnetic-stripe data or equivalent on a chip)▪ CAV2/CVC2/CVV2/CID▪ PINs/PIN blocks

**OK to Store – must be encrypted
in transit and at rest using
Strong Cypher**

**(Generally) NOT OK to Store –
only issuers may store* with
business justification**



Which SAQ Best Applies to My Environment?



You all can probably stop here

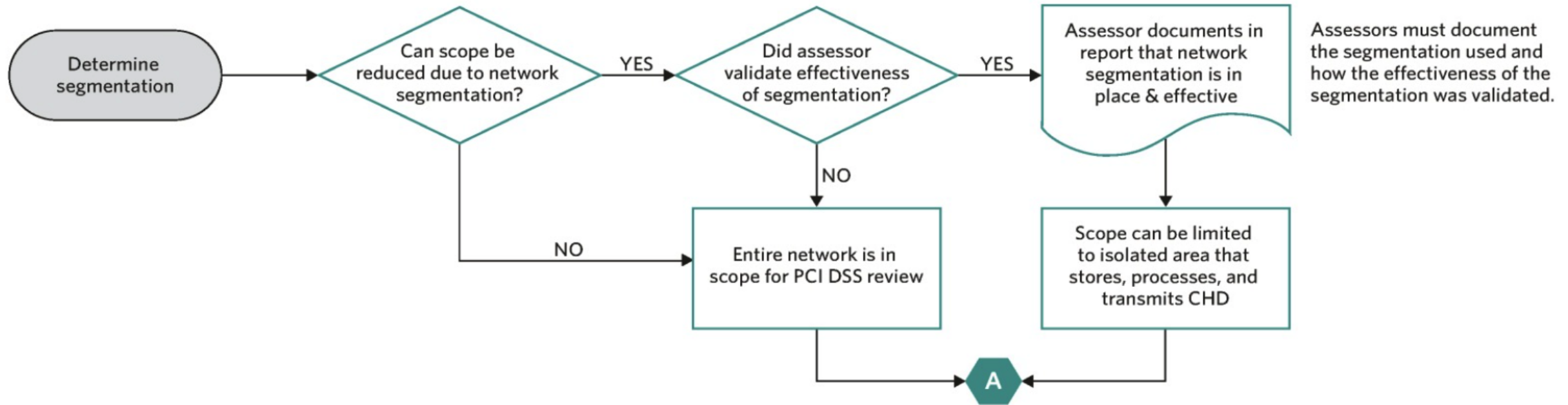
IF you need to report...
It will be either
SAQ-D or a ROC



What is in Scope?

Segmentation

To use network segmentation to reduce PCI DSS scope, an entity must isolate systems that store, process, or transmit cardholder data from the rest of the network.

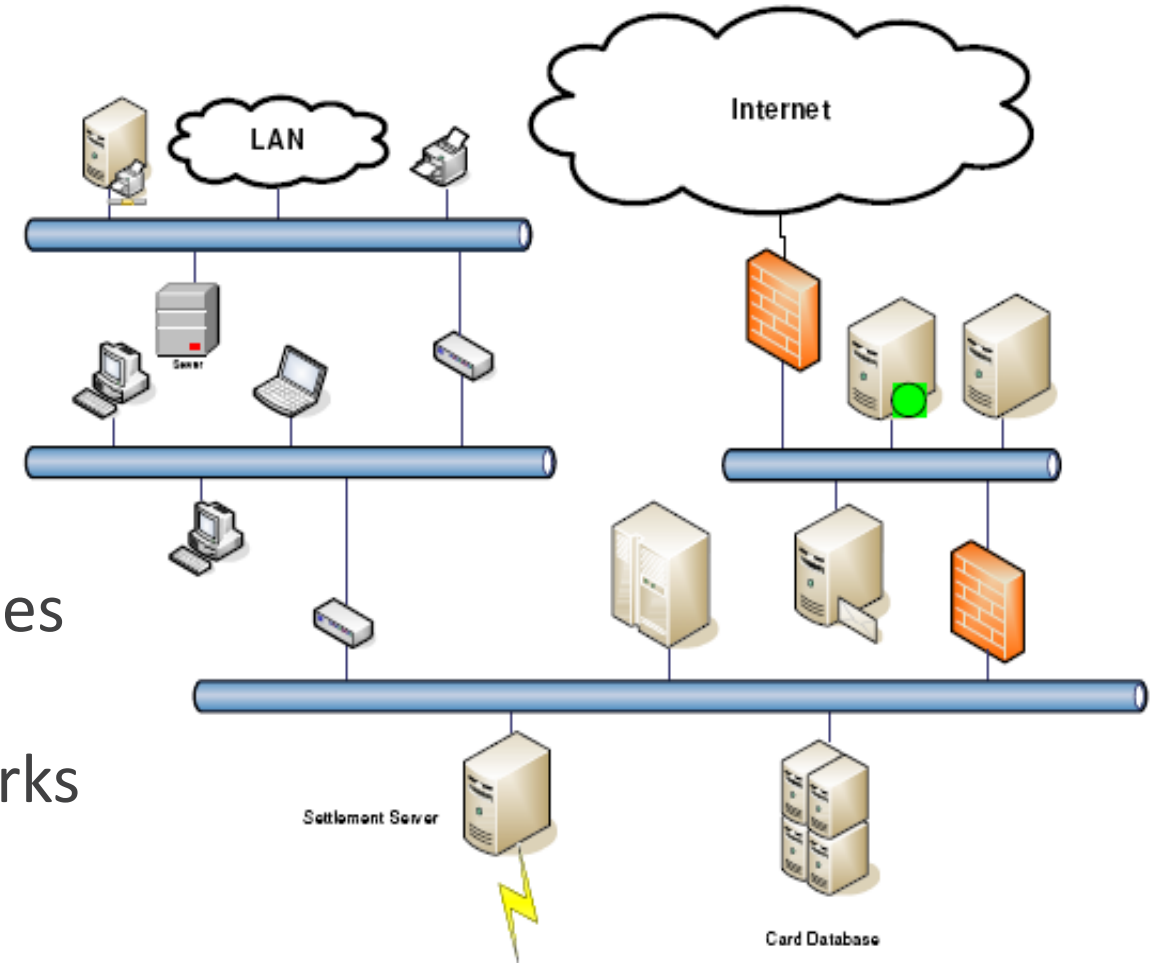


Words and Vocabulary are IMPORTANT:
Segmentation in this context means ISOLATION



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



Most Significant Challenges to PCI Compliance?

8. Identify where card holder data is “stored” – minimize storage
7. Compare current control requirements (FFIEC and GLBA) to PCI – identify overlaps and gaps
6. Vendor/service provider applications do not support PCI compliance
5. Secure application development/compliance
4. Vulnerability management and remediation
3. Secure standard configuration management
2. Network segmentation ↓ you need to think “isolation”
1. Operational maturity:
 - Disciplined adherence to policies and procedures – PCI is daily business as usual
 - Mature documentation of evidence & documented exception management



Common Challenges for Credit Unions

- 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
- Members have old systems
 - Credit Union wants to support legacy (non-compliant) protocols for members with old PCs

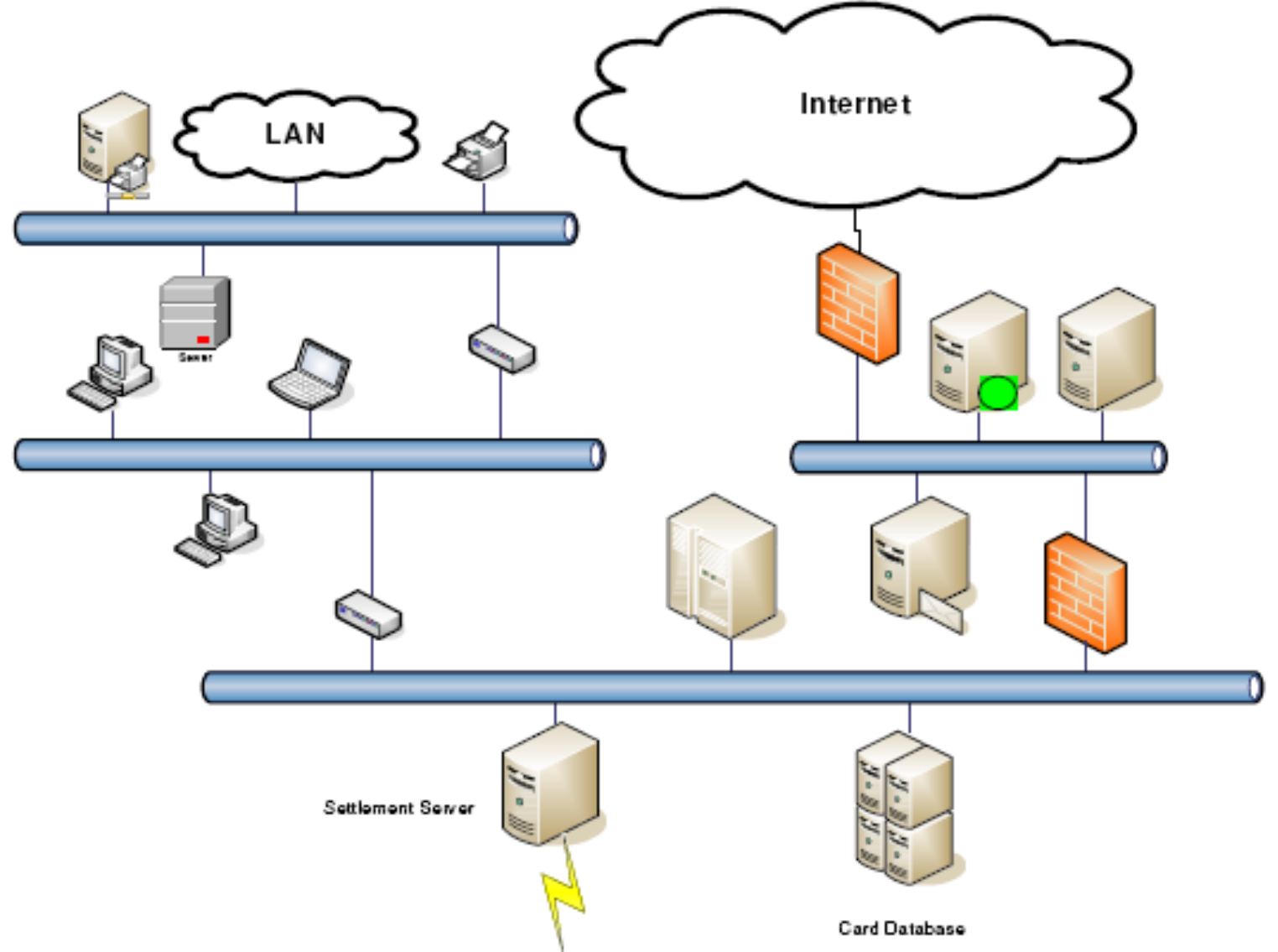


Common Challenges for Credit Unions

- Isolation/segmentation is difficult
 - Everything talks with the core
- Card data is received over the phone
 - Service center records phone calls
 - Phone calls contain PAN data
 - Voice over IP (touches everything... is integrated to everything...)
- This makes all systems on the network in scope

Exercise - Segment Your Network

- What is in-scope here?
 - NOTHING
 - Firewalls
 - Servers
 - PCs
 - Everything
- Why?

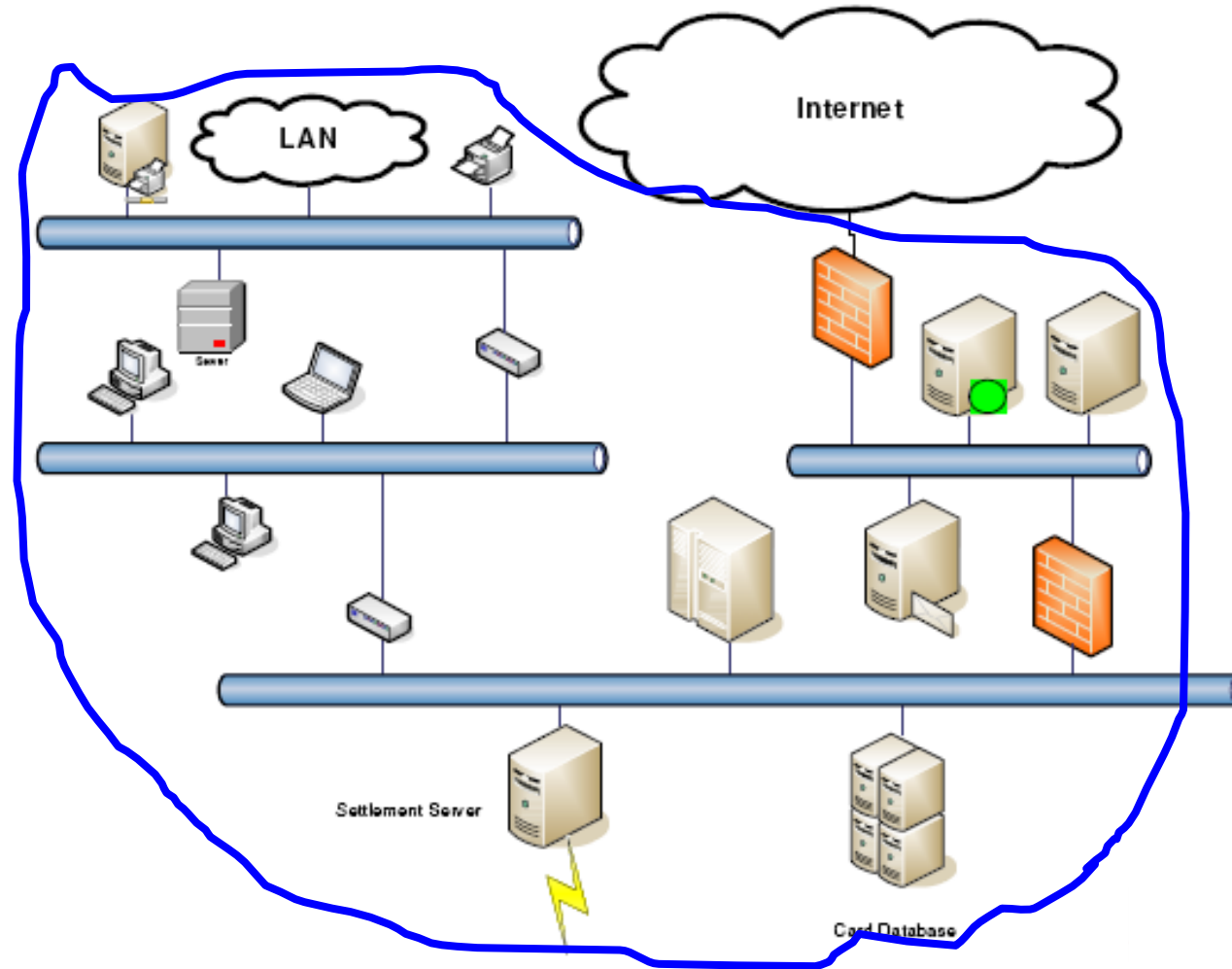


Exercise - Segment Your Network

- What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

- Why?

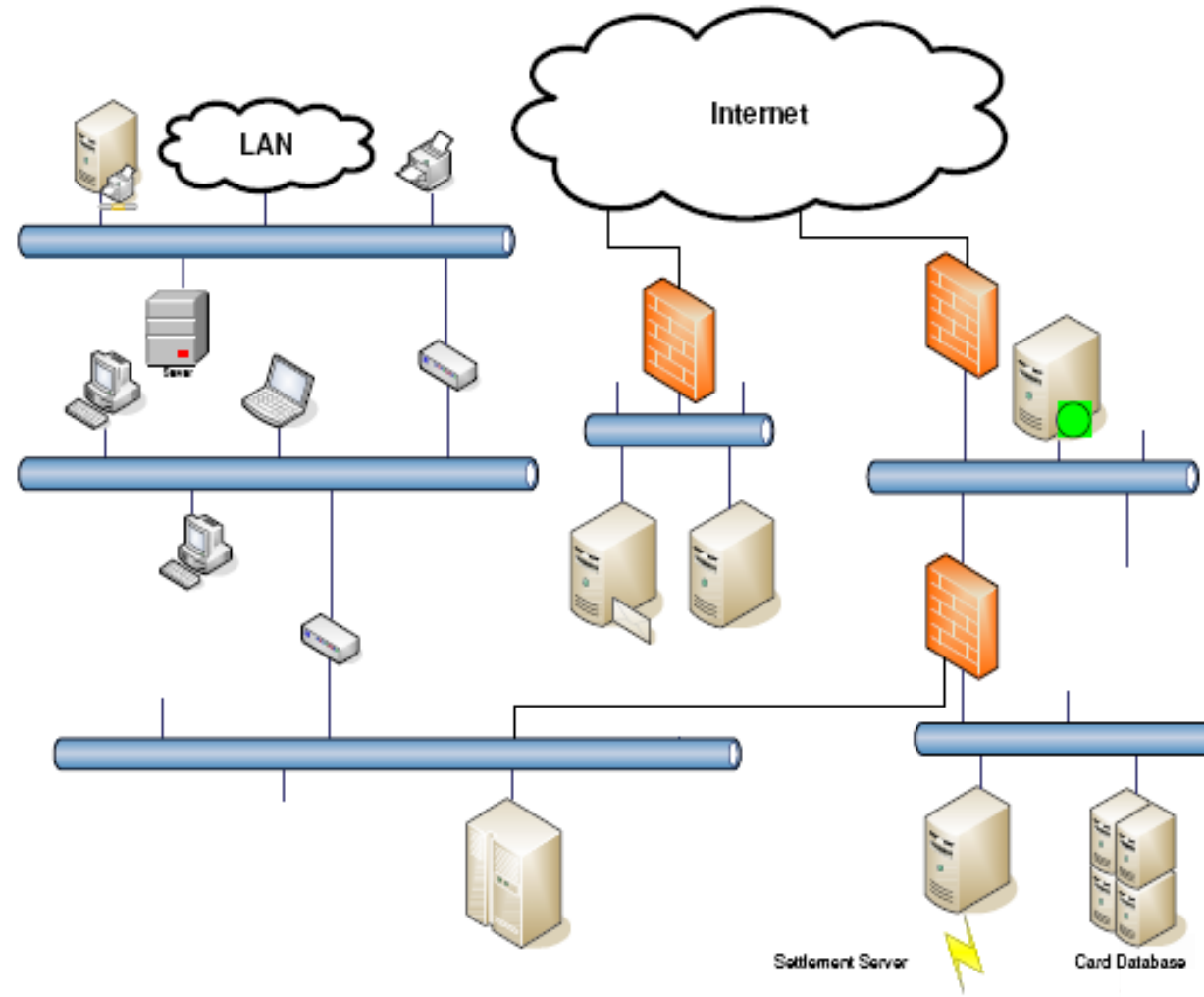


Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?

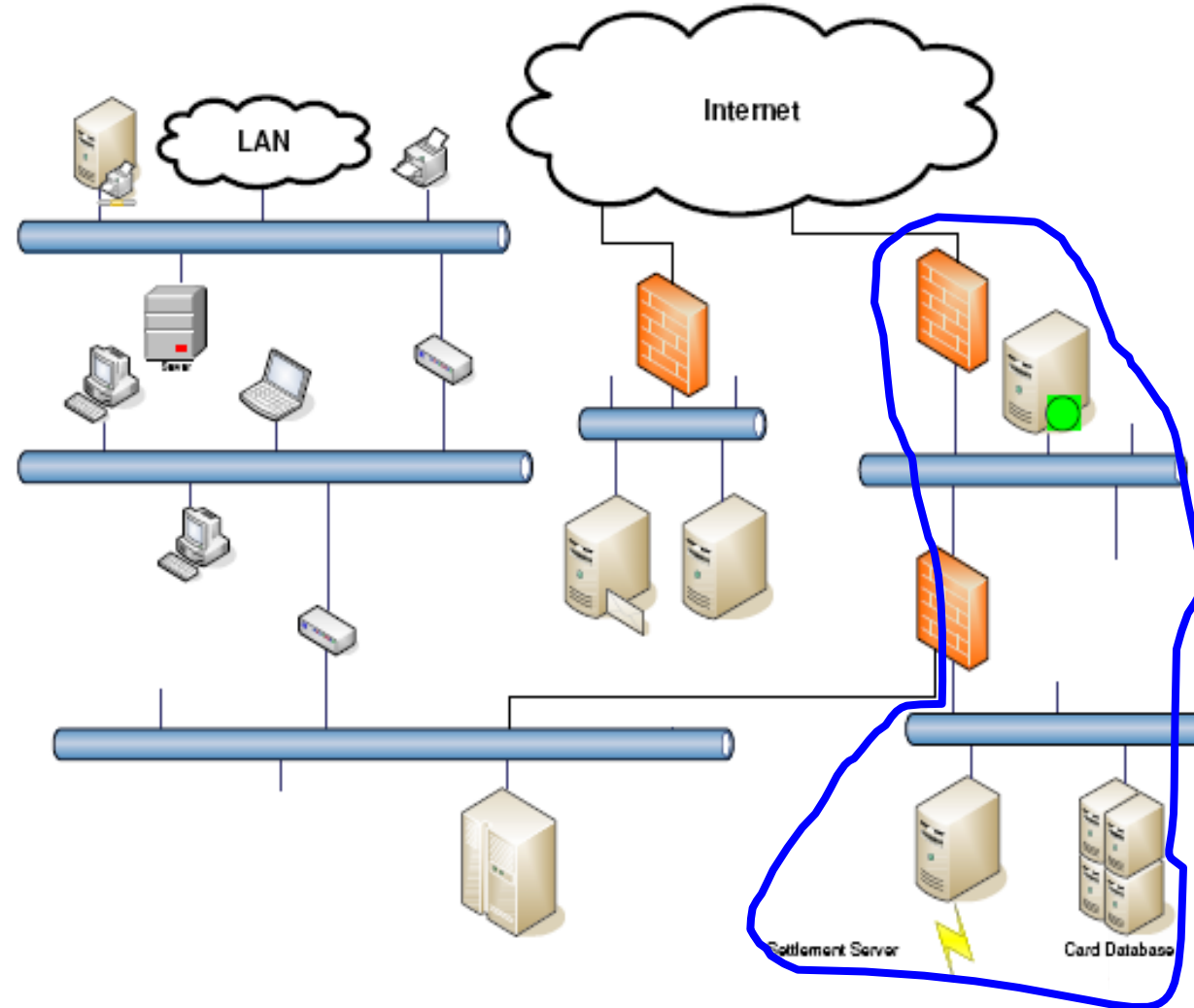


Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?





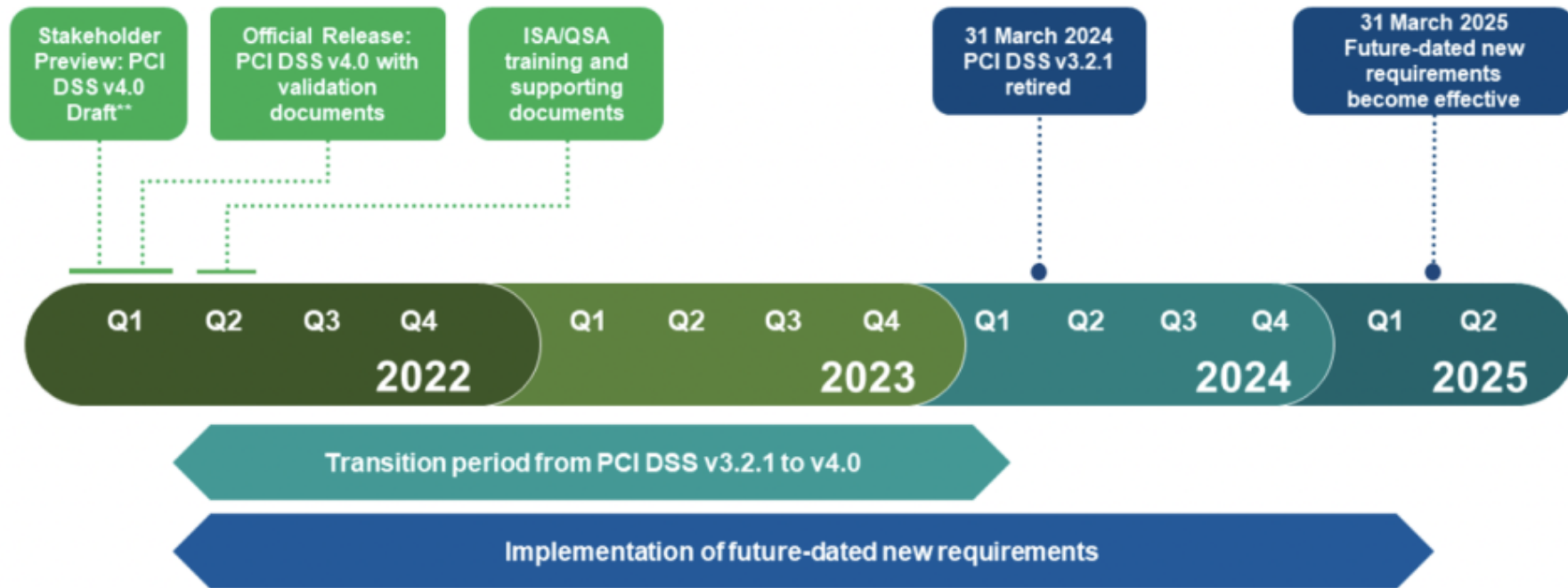
What Is New with Version 4

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

Lifecycle Changes to PCI DSS

PCI DSS v4.0 Implementation Timeline*



* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

- *****blog.pcisecuritystandards.org/countdown-to-pci-dss-v4.0



The Customized Approach

PCI DSS 4.0 keeps the existing prescriptive method for compliance and introduces a new Customized Approach option for meeting a requirement. Customized Approach allows customers to leverage novel technologies and innovations to meet a control objective that may not necessarily meet the defined requirement approach. This is intended to give organizations more flexibility as long as they can show their custom solution meets the objective of the PCI DSS requirement.

The new Customized Approach validation method provides a more mature model from what was previously referred to as Compensating Controls. It requires more vetting and review, including control matrix documentation, and a targeted risk analysis to ensure the assessed entity has fully addressed all associated risks and to confirm the intent of the control objectives are being met.

Outside of the changes to the reporting format and validation methods, there are a good number of changes to the requirements themselves as well. There are a total of 64 changed or new requirements in the PCI DSS 4.0 standard. Here are 12 changes you will need to know.



1. Formalized Annual Scoping Exercise – Performance of an annual scoping exercise was something organizations were instructed to execute within the PCI DSS 3.2.1 instructions. The onus however was on the organization being assessed to confirm this exercise was being properly conducted. PCI DSS v4.0 formalizes this requirement which will now be validated by an assessor as one of the new requirements within the standard itself.

2. Updated Authentication Requirements – Password Authentication Requirements now include:

- ◆ Minimum Password Length – 12 characters (previously 7 characters)
- ◆ Minimum Complexity – numeric and alphabetic
- ◆ Lockout Requirements – no more than 10 failed attempts (previously 6 attempts)
- ◆ Minimum Lockout Duration – 30 minutes
- ◆ Password Expiration – 90 days*
- ◆ Password History – Previous 4 Passwords

*PCI DSS v4.0 does provide additional options to satisfy the 90-day expiration requirement. It clarifies the use of MFA and/or performing a real-time dynamic analysis on a user account's security posture based on a **zero-trust** architecture can also be used to meet this control.



3. **Multi-Factor Authentication** – PCI DSS 4.0 adds clarification to requirements for MFA for remote access and access into the cardholder data environment (CDE). If remote access grants access outside the CDE, then an additional MFA control will be required to gain access into the CDE from that network. This is important because the new standard also clarifies that MFA for remote access is also required for networks with access to the CDE (where connected systems exist).
4. **Risk Assessment** – Instead of a single risk assessment process, PCI DSS v4.0 requires organizations to perform targeted risk analysis for all requirements where there is flexibility allowed and that risk analysis must be performed at least annually for each instance. An example of this are controls that are required to be performed “periodically.” The results of this exercise will need to be documented and provided to the assessor for review prior to the PCI assessment.
5. **Ownership, Roles, & Responsibilities** – Organizations must now properly communicate roles, responsibilities, and ownership of all requirement tasks. Responsibilities must be formally documented, assigned, and understood by the owner.



6. **Encryption** – The hashes used to render a primary account number (PAN) unreadable are required to be keyed cryptographic hashes of the entire PAN. Organizations will no longer be allowed to only hash the sensitive parts of the PAN. In addition, disk encryption will no longer be acceptable as the control used to protect PAN at rest, with the exception of PAN stored on removable media.
7. **Anti-virus/Malware** – The anti-virus requirements will have more flexibility for organizations based on targeted risk assessments. There is a new control required to be in place that detects and protects personnel against phishing attacks.
8. **Public-facing web applications** – PCI DSS v4.0 requires deployment of an automated technical solution that continually detects and prevents web-based attacks. This solution must be in front of public-facing web applications and configured to either block web-based attacks or generate an alert that is immediately investigated.



9. **HTTP Headers** – To help curb the impact of **Magecart attacks**, there's a new requirement for a change and tamper-detection mechanism that alerts of any unauthorized modifications to HTTP headers and the contents of payment pages as received by the consumer browser.
10. **Payment page scripts** – Also related to the above, organizations will be required to manage (and use proper controls to ensure the integrity of) all payment page scripts that are loaded and executed in the consumer's browser. This includes scripts being pulled from third-party sites.
11. **Log Requirements** – Only 'Automated Mechanisms' will be allowed for performing audit log review, meaning daily manual reviews will be prohibited. Also, requirements around control failures will now apply to all organizations and not only service providers.
12. **Internal Vulnerability Scanning** – Internal scans must be authenticated unless the device being scanned does not accept credentials. PCI DSS v4.0 also includes controls concerning the protection of authentication credentials.





Summary

WEALTH ADVISORY | OUTSOURCING AUDIT, TAX, AND CONSULTING

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

Summarize

1. Credit Unions 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. Credit Unions could be Issuer, Merchant, Service Provider



Summarize

5. The Credit Union most likely is not compliant right now

6. Start the process

- Complete a Readiness Assessment
- Utilized Prioritized Approach
- Map your controls
- 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...



Questions





Thank You!

Randy Romes CISSP, CRISC, CISA, MPC, PCI-QSA

612-397-3114

Randy.Romes@claconnect.com

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

Resources

- PCI Website: PCISecurityStandards.org

Document library

*****[.pcisecuritystandards.org/document_library](https://pcisecuritystandards.org/document_library)

DSS

*****[.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1632414383382](https://pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1632414383382)

Prioritized approach (description and tool)

*****[.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1632414383404](https://pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1632414383404)

*****[.pcisecuritystandards.org/documents/Prioritized-Approach-Tool-v3_2_1.xlsx?agreement=true&time=1632414383408](https://pcisecuritystandards.org/documents/Prioritized-Approach-Tool-v3_2_1.xlsx?agreement=true&time=1632414383408)

- CIS – Audit Scripts Mapping Tool

*****[.auditscripts.com/download/2742/](https://auditscripts.com/download/2742/)

