We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Modern Cyber Risks & PCI Readiness

October 2026

©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

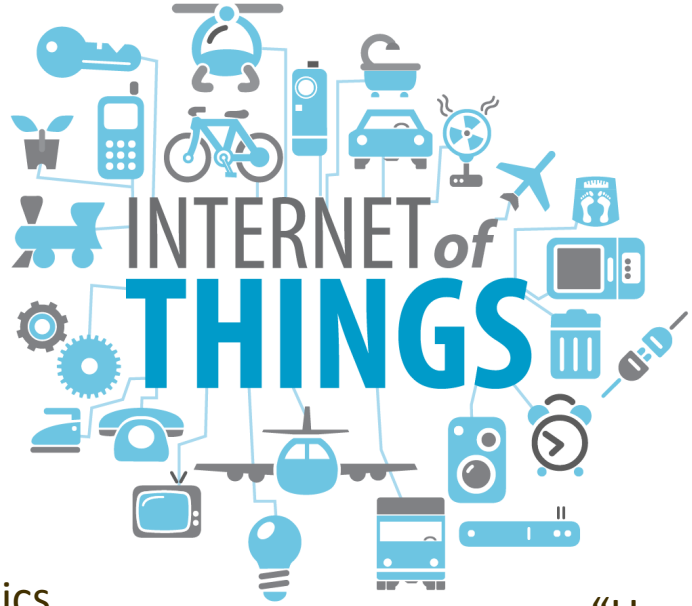
The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen 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.

©2026 CliftonLarsonAllen LLP

Raise Your Hand if You Work for a Tech Company

- Security Cameras
- Motion Sensors
- Logistics/GPS Tracking
- Print Vendors
- Smart (TV) Displays
- HVAC
- Digital Assistance
- Enterprise Data Processing
- Cloud Applications & Analytics
- Hosted Application Processing
- AI…



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

Apple Watch or FitBit

“Hey Siri, what’s my balance?”

Stand up if….

©2026 CliftonLarsonAllen LLP

Sun Tzu: “*Know Your Enemy*”
BSA Motto: ”Be Prepared”

The Current Threat Landscape



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Cybercrime and Black-Market Economies

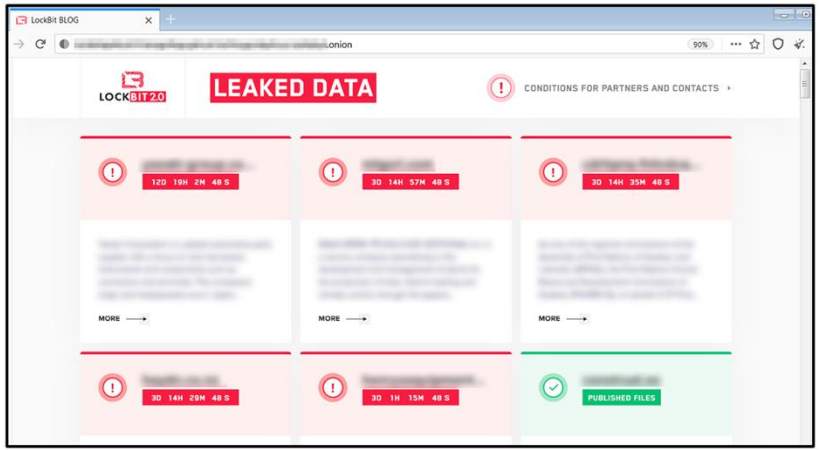
- Black market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)

- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Log-in Credentials
    - ePHI, PII, PFI, account profiles, etc.
    - Credit card information
  - Ransomware, interference w/ operations and extortion

- Monetization of access…

They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Data exfiltration
5. Ransomware
6. Extortion to avoid breach disclosure



©2026 CliftonLarsonAllen LLP

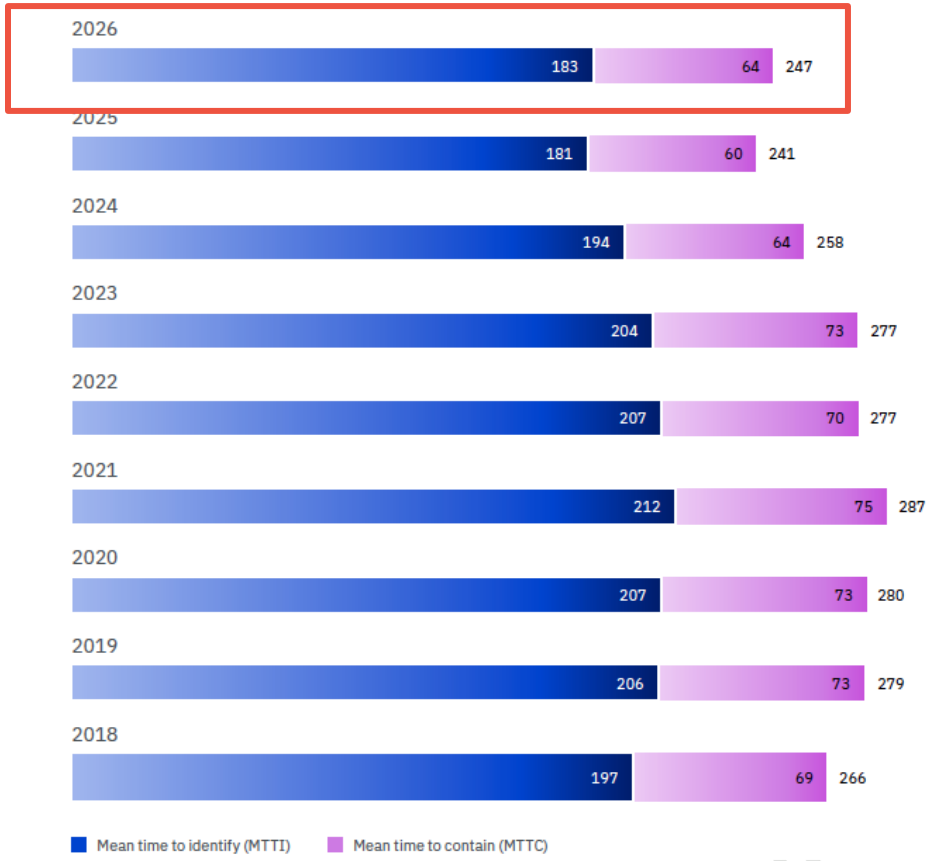
IBM - Average Days to Identify and Contain a Data Breach

Global average is

247 days

- 183 days to identify a breach
- 64 days to contain the attack

What are the bad actors doing for 183 days?



Source: IBM Security Cost of a Data Breach Report 20265

©2026 CliftonLarsonAllen LLP

IBM - Cost of a Data Breach

Average cost in 2025 is $6.29 M

(up from $4.4M)

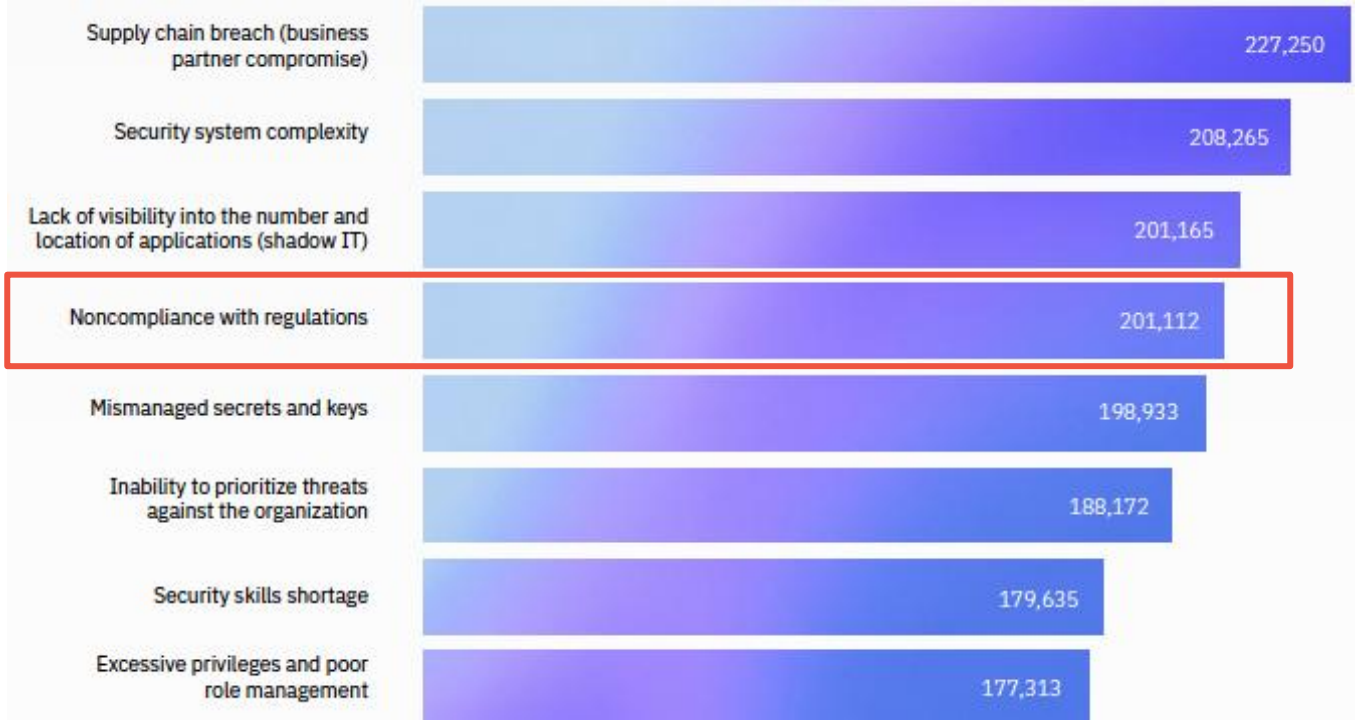




©2026 CliftonLarsonAllen LLP

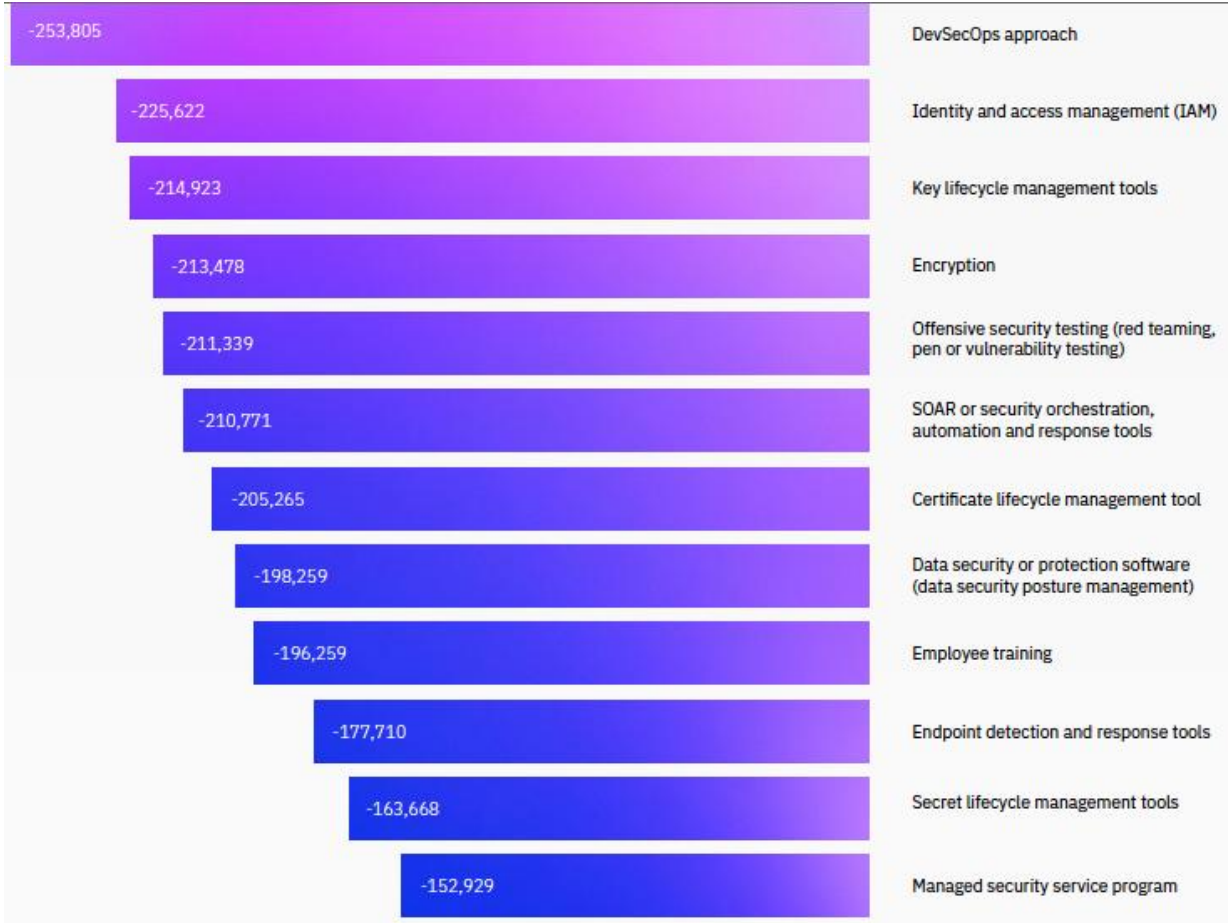
Source: IBM Security Cost of a Data Breach Report 2026

Factors That Make Breaches More Costly



©2026 CliftonLarsonAllen LLP

Source: IBM Security Cost of a Data Breach Report 2026



Mature Operational Factors that Mitigate Breach Impact and Cost

©2026 CliftonLarsonAllen LLP

Source: IBM Security Cost of a Data Breach Report 2026

Polling Question #1

- What is the current average cost of a data breach?

- $1,000,000
- $100/record
- $6.29 M
- Nothing – we don’t pay

©2026 CliftonLarsonAllen LLP

Email (Spear) Phishing

The Starting Point For Most Breaches



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

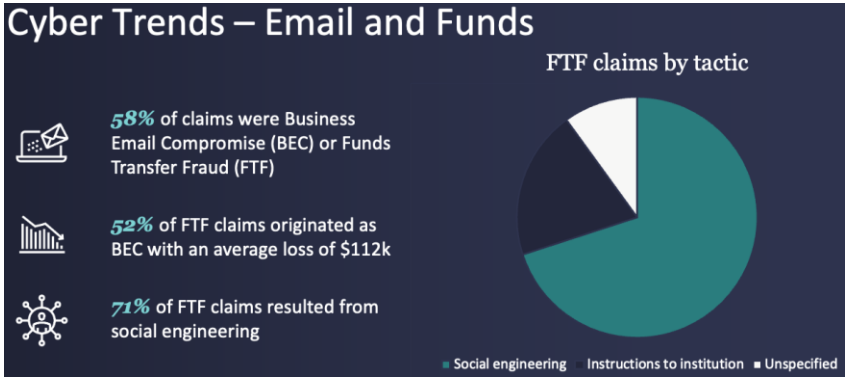
Microsoft Digital Defense Report: Targeting Businesses

Credentialed phishing schemes on the rise – indiscriminately target all inboxes

The volume of phishing attacks is orders of magnitude *greater than all other threats*

Over 700 million phishing emails blocked per week

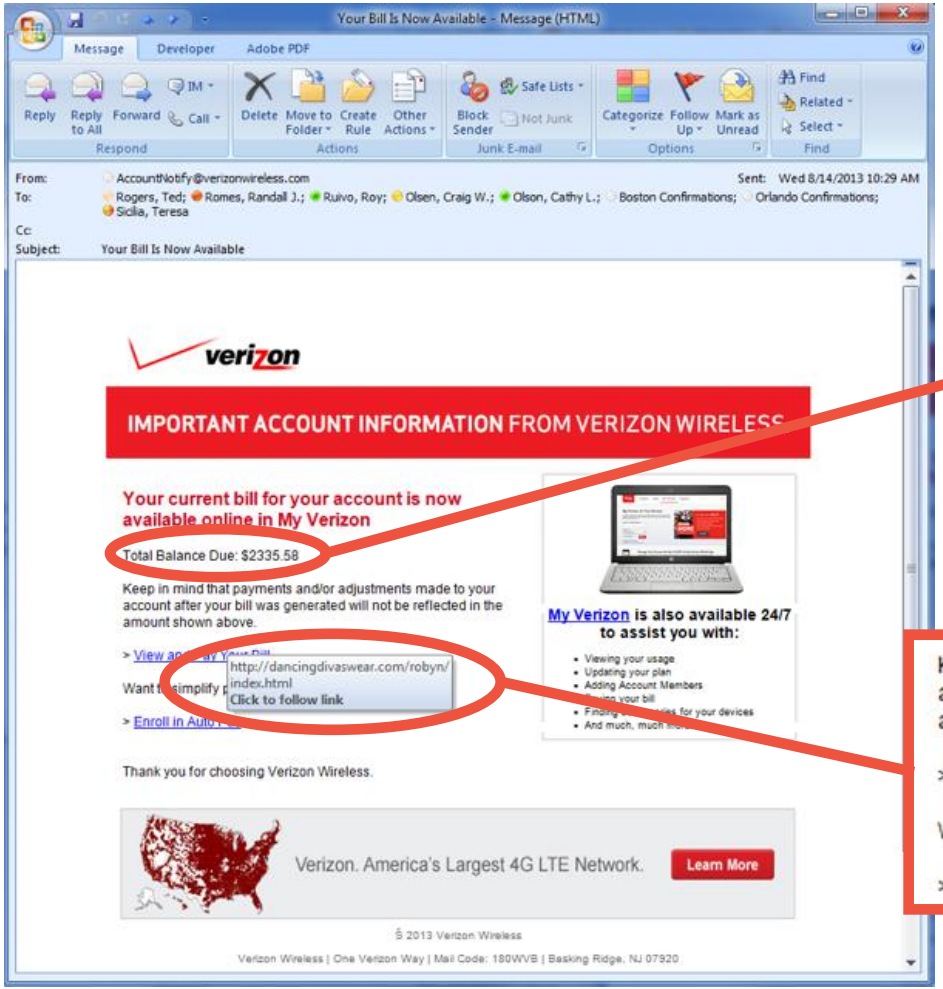
- 1hr 12 m - The median time is takes for an attacker to access your private data if you fall victim to a phishing email
- 1hr 42 m - median time for an attacker to begin moving laterally within your network once a device is compromised



Source: Coalition 2026 Cyber Claims Report

©2026 CliftonLarsonAllen LLP

Old School Spear Phishing



Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

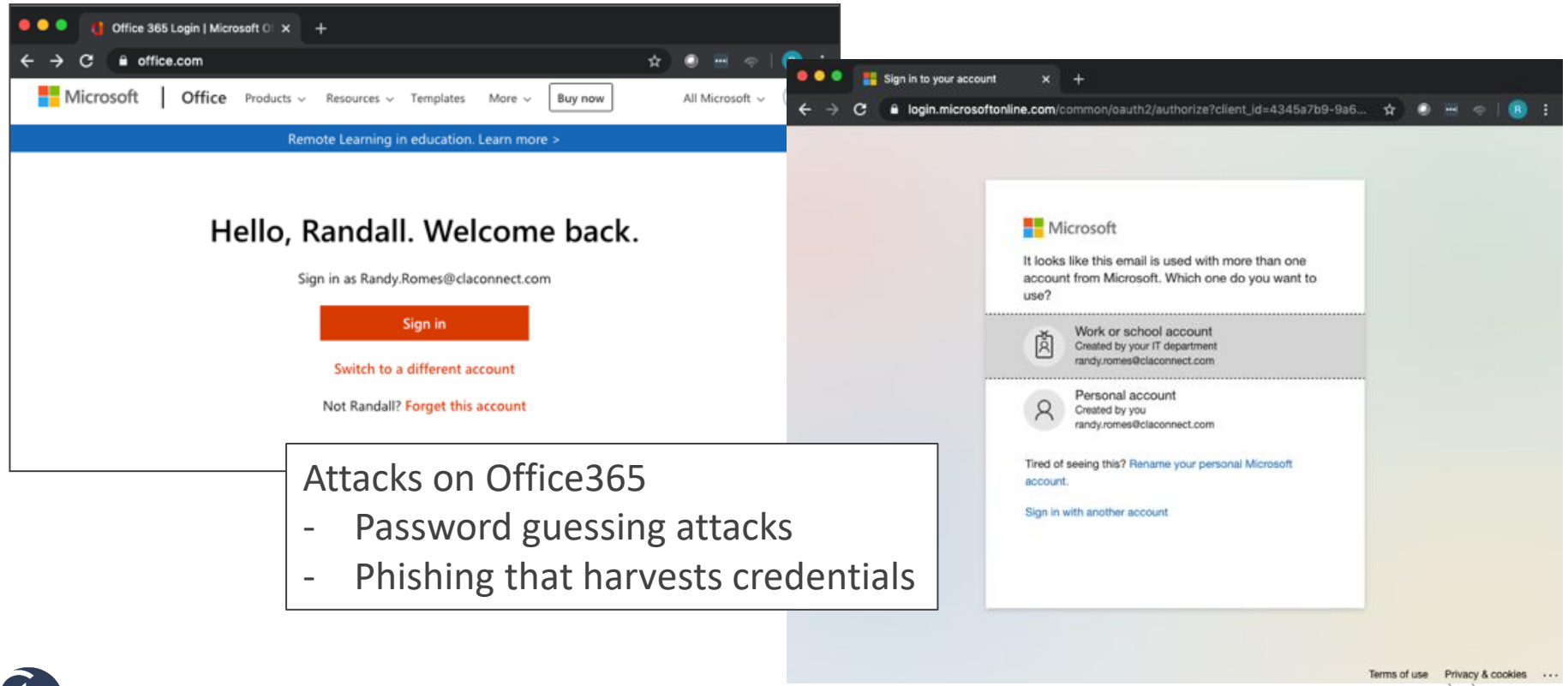
Want to simplify

http://dancingdivaswear.com/robyn/index.html
Click to follow link

> Enroll in Auto Pay

©2026 CliftonLarsonAllen LLP

Credential Harvesting and Password Guessing:



Attacks on Office365

- Password guessing attacks
- Phishing that harvests credentials

©2026 CliftonLarsonAllen LLP

Attacking the Supply Chain and Exposed Services



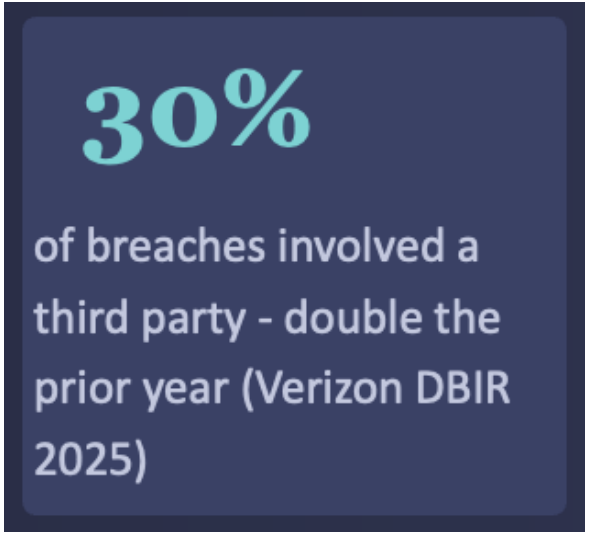
©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Software Vendor/Supply Chain Risk Management

Significant Issues:

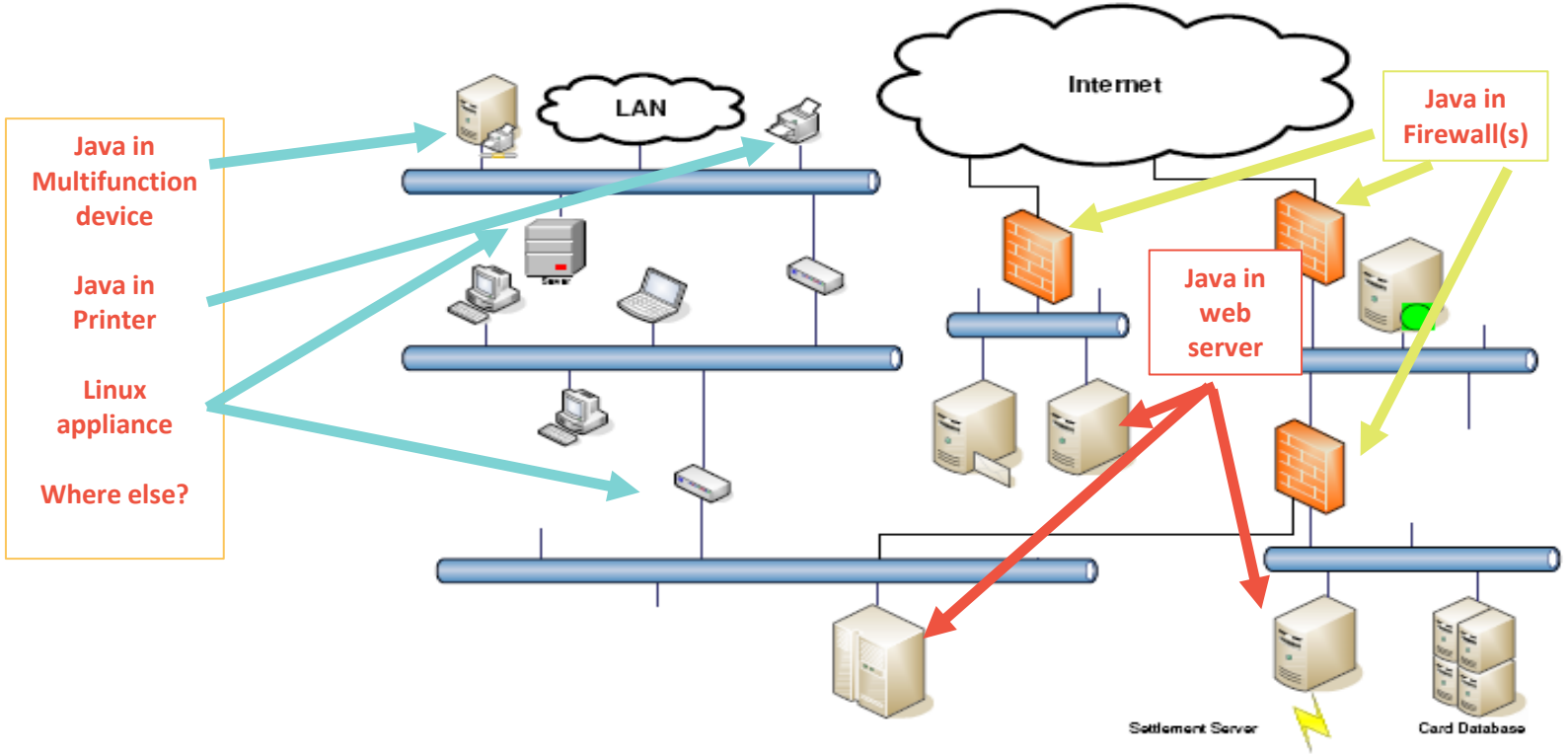
- Common software components with exploitable vulnerabilities.
- Recent examples include
  - “**Log4j**” Java vulnerabilities…
- Attacks on website/webservices/APIs
- Attacks on (web) hosted infrastructure

Google:
Log4j vulnerabilities



©2026 CliftonLarsonAllen LLP

Java Software and Log4j



©2026 CliftonLarsonAllen LLP

Third-Party Data Breaches - MOVEit

What

SQL injection flaw in MOVEit web application

When

May – November 2023

How

Public webpage was vulnerable to SQL injection, allowing attackers to upload web shell

Impact

- Hackers uploaded web shell to MOVEit servers and exfiltrated data
- Hacker groups demanded payment, and disclosed sensitive data for organizations that did not pay
- Impacted over 2,550 organizations and 66 million individuals

©2026 CliftonLarsonAllen LLP

Operational Stability

Ransomware is not going away…



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Ransomware

- Ransomware bursts on the scene more than ten years ago
- Hollywood Presbyterian decided to pay after ___
- Why did they wait to pay?





©2026 CliftonLarsonAllen LLP

Ransomware

- Interfere with operational up time
  - This costs $

- Extortion:
  - Pay to release data and systems
  - Pay to avoid exposure
  - Threaten those whose data has been stolen

- Be Prepared
  - Have you performed a Ransomware readiness/resilience test…???
  - Can IT operations restore? From bare metal up? In the heat of the moment????
  - Are you confident your hosted vendor is prepared???
    - Case Study to Follow….



Source: Coalition 2026 Cyber Claims Report

©2026 CliftonLarsonAllen LLP

Polling Question #2

- True or False

- State law requires that an organization only pay ransomware demands through covered insurance.

*Florida Statute § 282.3186

©2026 CliftonLarsonAllen LLP

Case Study

BEC, Payment Diversion, and Data Loss

©2026 CliftonLarsonAllen LLP

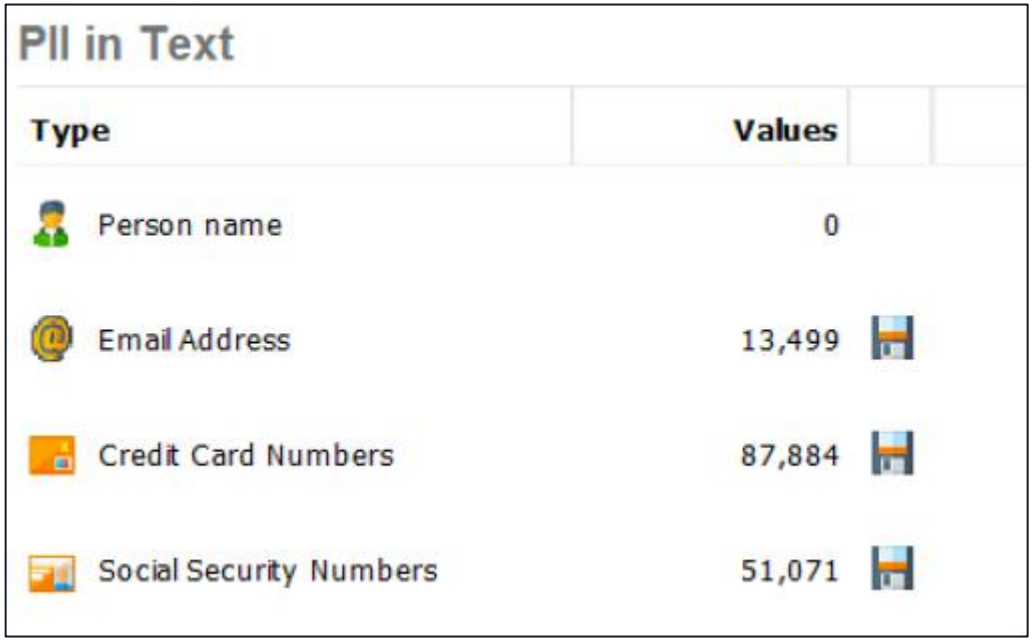
Overview

- Controller sent email to AP to process an invoice
- AP verified the legitimacy, identified request was fraudulent
  - Controller did *NOT* send it
- IT Security team “reviewed”, identified logins from outside the USA, found no other fraudulent emails/payments, and changed password for user
- Four months later, supervisory committee heard about incident and asked for independent investigation
  - Log retention for many systems was default (30 days)

©2026 CliftonLarsonAllen LLP

Analysis

- Analysis of email showed controller had documents with users' social security numbers and credit card numbers



PII in Text

Type	Values
Person name	0
Email Address	13,499
Credit Card Numbers	87,884
Social Security Numbers	51,071

©2026 CliftonLarsonAllen LLP

Standards Based Operations

“People, Rules, and Tools”



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Peace of Mind - It Starts with Policies and Standards

- Security is not a product
  - There is no sliver bullet “solution”
  - Security needs to be an evolving, layered process
- 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 framework**:
  - GLBA, CJIS, HIPAA, NERC/CIP, FERPA --- Regulatory
  - PCI – DSS, CMMC, HITRUST --- Contractual
  - CIS Critical Controls, NIST CSF --- Operational standards

©2026 CliftonLarsonAllen LLP

Standards Based IT and Cyber Operations

CIS Critical Controls – Version 8

- Vendor/Product/Industry agnostic
- 20 years of improvement
- Prioritized
- Scalable

- Check lists, benchmarks, reporting and tracking tools and resources
  - Cloud implementations
  - Operating systems and software
  - Hardware/devices

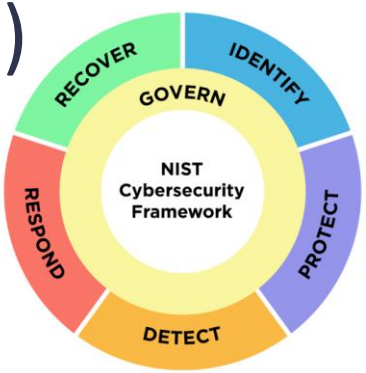
- Includes Maturity Model



©2026 CliftonLarsonAllen LLP

https://www.cisecurity.org/controls/

NIST Cyber Security Frame Work (CSF)



Flexible Risk Management

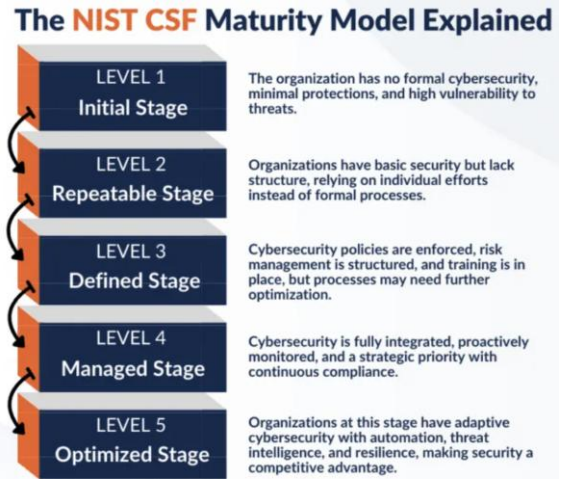
- The NIST Cybersecurity Framework offers a flexible approach tailored to different organizational needs for managing cybersecurity risks.

Core Functions

- Identify – understand assets, data and risks
- Protect – safeguard systems and services
- Detect – discover cybersecurity events quickly
- Respond – take action to contain and mitigate
- Recover – restore capabilities and operations

Incident Management

- Effective incident management is critical, focusing on timely detection and recovery from cybersecurity incidents to minimize impact.



©2026 CliftonLarsonAllen LLP

Polling Question #3

- A cybersecurity maturity framework calls for which of the following:

A. Policies
B. Configured Controls
C. Monitoring and Reporting of Polices and Configured Controls
D. All of the Above

©2026 CliftonLarsonAllen LLP

PCI - DSS Overview

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



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Before PCI DSS

Prior to 2006 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.

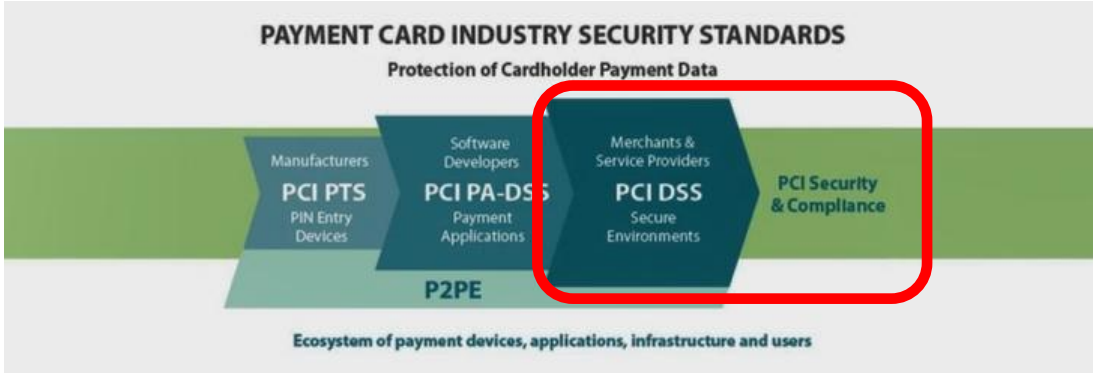
- Visa's Cardholder Information Security Program
- MasterCard's Site Data Protection
- American Express' Data Security Operating Policy
- Discover's Information Security and Compliance
- JCB's Data Security Program



©2026 CliftonLarsonAllen LLP

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 6 goals and 12 detailed requirements that ensure maximum payment card security.



©2026 CliftonLarsonAllen LLP

Lifecycle Changes to PCI DSS

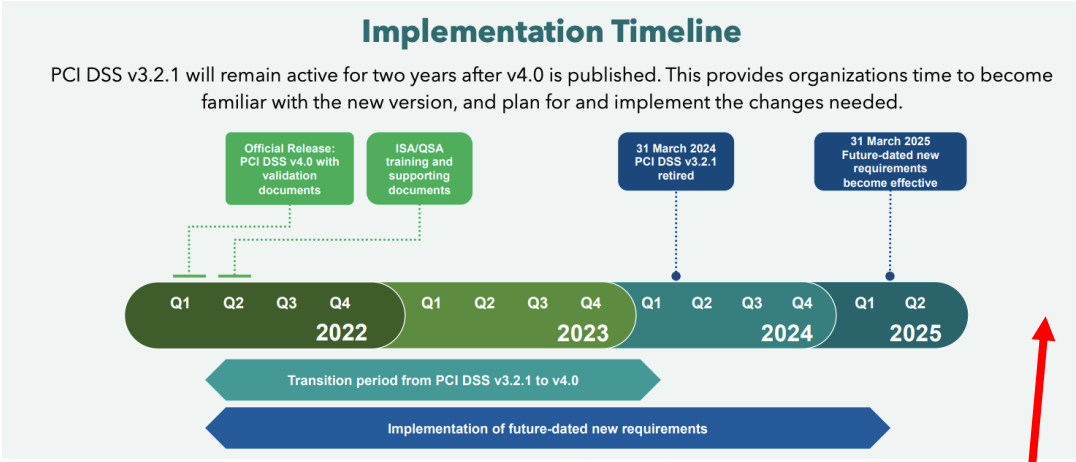
Version 4 released in Q1 of 2022

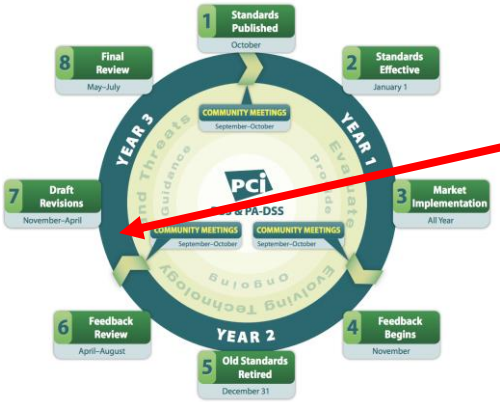
Version 3.2.1 “expired” March 31, 2024

- Version 4 required
- Some controls were best practice for now, with “future dated” requirement

Compliance with Version 4.0.1 is now the standard (April 1, 2025)

- Previous “future dated” controls are now required





https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf

©2026 CliftonLarsonAllen LLP

PCI DSS Compliance

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.

This is a contractual obligation.

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

VISA:

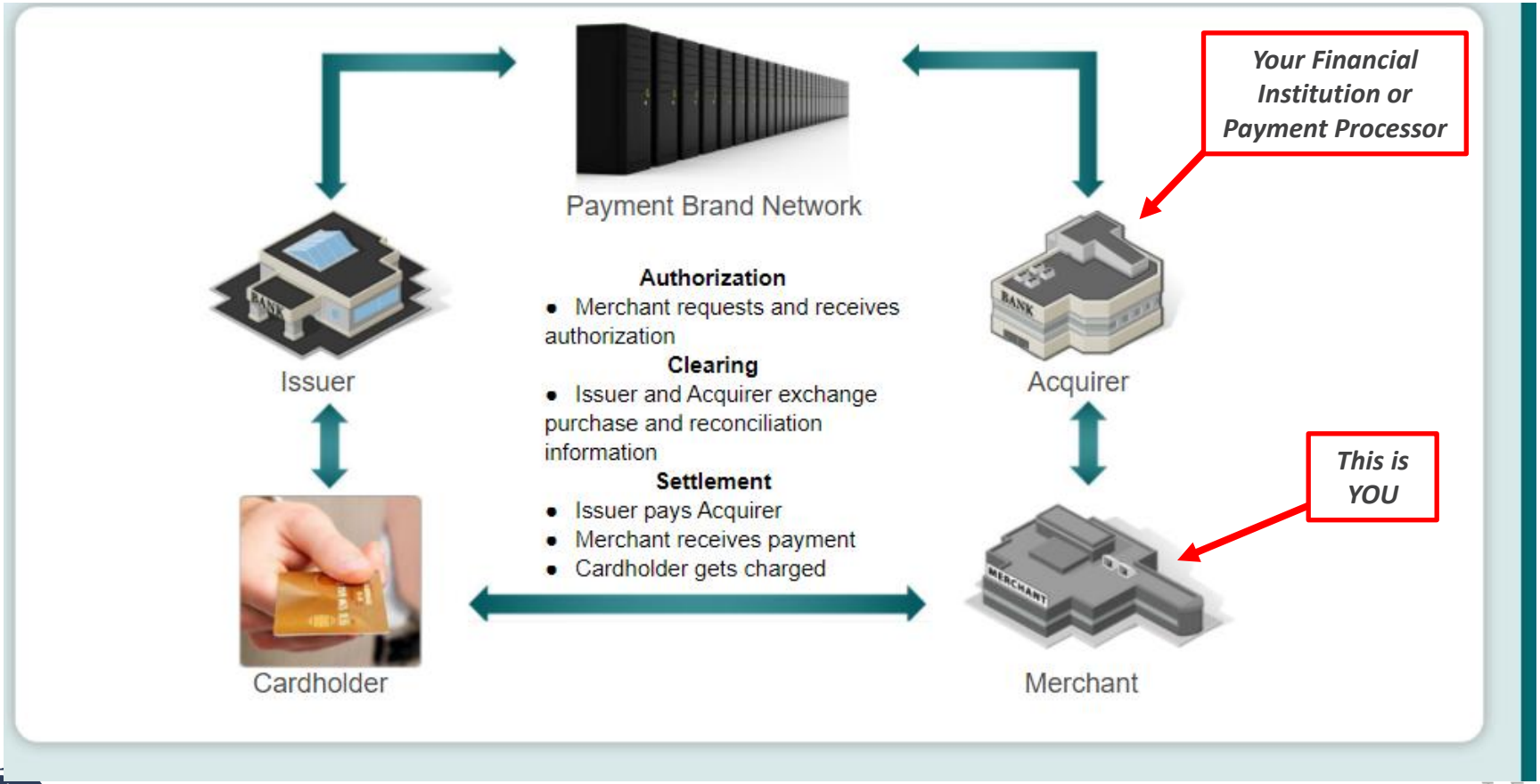
- https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html
- Payment Card Industry Data Security Standard (PCI DSS) compliance is required of all entities that store, process, or transmit Visa cardholder data, including financial institutions, merchants and service providers…

MasterCard:

- Mastercard Document Cover 8.5x11
- Compliance with the PCI DSS is required for all issuers and acquirers…

©2026 CliftonLarsonAllen LLP

Payment Industry Terminology



©2026 CliftonLarsonAllen LLP

From: [redacted]
Date: Monday, November 6, 2023 at 10:05 AM
To: [redacted]
Subject: [EXT EMAIL] Action Required: Validate compliance by January 5

[redacted]

Submit required compliance documentation by January 5

Dear Customer,

[redacted]., a [redacted] 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 [redacted] requesting validation?

Visa® and Mastercard® operating rules and your processing agreement with [redacted] 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 [redacted] 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 [redacted]. More details are provided below.

Email the corresponding PCI DSS Attestation of Compliance (AOC) validation document to [redacted]tPCICompliance@[redacted].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 [redacted].

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 t[redacted]**, 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 t[redacted].

Am I required to complete the assessment form [redacted] provides a PCI-compliant payments solution to my organization?

Yes. The AOC validation document is required even [redacted] provides a PCI-compliant payment solution for you. Card brands may assess non-compliance fees if you cannot validate your PCI compliance. [redacted] 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

Fines and Fees for Non-Compliance



- Payment brands or acquirers may, at their discretion fine an entity $5,000 to $100,000 per month for non-compliance
- Banks can terminate the merchant's relationship or increase their transaction fees

©2026 CliftonLarsonAllen LLP

Polling Question #4

- Who can levy fines against an organization if they are not compliant with the PCI DSS?

A. Customers
B. Federal Government
C. Application Solution Provider
D. Acquirer (eg. merchant bank)

©2026 CliftonLarsonAllen LLP

PCI - DSS
The Framework



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

Overview – PCI DSS – “Digital Dozen”

Six Goals & Twelve Requirements

- Approximately 140 Controls

- A cadence of 3 for each “control”
  1. Policies/Standards/Procedures
  2. People assigned responsibility
  3. Evidence of control

→ 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

©2026 CliftonLarsonAllen LLP

Card Holder Data (CHD)

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of cardholder data and/or sensitive authentication data. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data—for example, entities that outsource payment operations or management of their cardholder data environment (CDE) [1]. Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

©2026 CliftonLarsonAllen LLP

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 Card Holder Data (CHD) is inactive or at rest (e.g., Core system, application system or database, stored backups, system component memory, log files, paper, etc…)
- **Process** – when Card Holder Data (CHD) is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed, etc…)
- **Transmit** – when Card Holder Data (CHD) is being transferred from one location to another (e.g., data in motion)



©2026 CliftonLarsonAllen LLP

Understanding the Cardholder Data Environment



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

How and Where Do You Start?



Each (annual) cycle must begin with scope confirmation.

(eg. a Discovery Exercise):

1. **Which People, Processes, and Technology** interact with card holder data or can affect the security of card holder data?
2. ***How*** is card holder data **Stored, Processed, or Transmitted**?
   - *Interviews and tool-based discovery…*

These two steps are important to:

- Define your Cardholder Data Environment (CDE).
- Understand the controls that are in scope.

MUST Do This FIRST

©2026 CliftonLarsonAllen LLP

Understand People and Processes

- How do we accept CC payment “in-person”?
- How do we accept CC payment over the phone?
- How do we accept CC payment via a website?
- How do we store, process or transmit CC data?
- How do we store, process or transmit CC data for someone else?
- Where do we have instant issue capabilities?
- What (vendor) applications do we use that store, process, or transmit CC info?
- How do you rely on a vendor (TPSP) to host or manage any of your systems?

©2026 CliftonLarsonAllen LLP

Use of Third-Party Service Providers (TPSP)

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

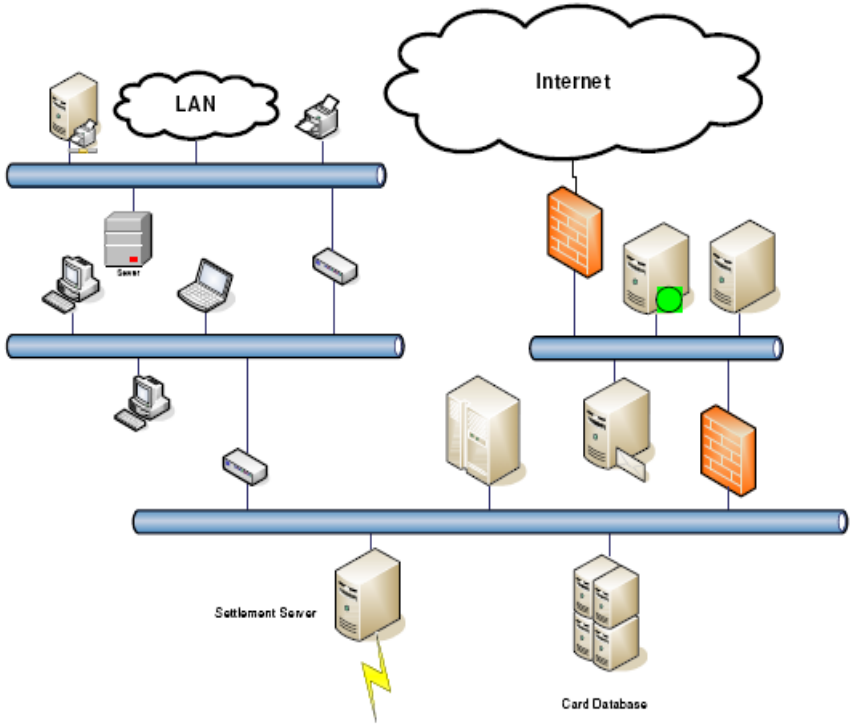
- If a third-party stores, process, or transmits CHD on your behalf they are in scope for your assessment
  - Third-parties may provide an Attestation of Compliance (AOC) which must be reviewed during your assessment
  - If they do not have their own PCI compliance report to share, then they need to be assessed as part of your assessment

- You need a Service Provider Responsibility Matrix – this defines which of the in-scope controls they are responsible for

©2026 CliftonLarsonAllen LLP

Understand Where People and Process Interact with Technology

- Develop data inventory – Document CHD/data flow (diagrams)
  - Applications and systems/servers
  - Third Party Service Providers
- Understand which systems/applications are linked (interfaces) – how does this all interact with cloud hosted services?
- Who is mining data and for what purposes?
- Understand how the back up system works?



©2026 CliftonLarsonAllen LLP

How to Determine System Scope

CDE

System component stores, processes, or transmits CHD/SAD

AND/OR

System is on the same network as, or has unrestricted connectivity to system(s) that store, process, or transmit CHD/SAD

Connected-to or Security-Impacting

System component directly connects to the CDE

OR

System component indirectly connects to the CDE

OR

OR

System component impacts configuration or security of the CDE

OR

System component provides security to the CDE

OR

OR

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

OR

System component provides security to the CDE

Out of Scope

System component does not store, processes, or transmit CHD/SAD

AND

System component is not in the same subnet or VLAN as systems that store, process, or transmit CHD/SAD.

AND

System component cannot connect to any component in the CDE

AND

System component does not meet any criteria described for connected-to or security-impacting systems

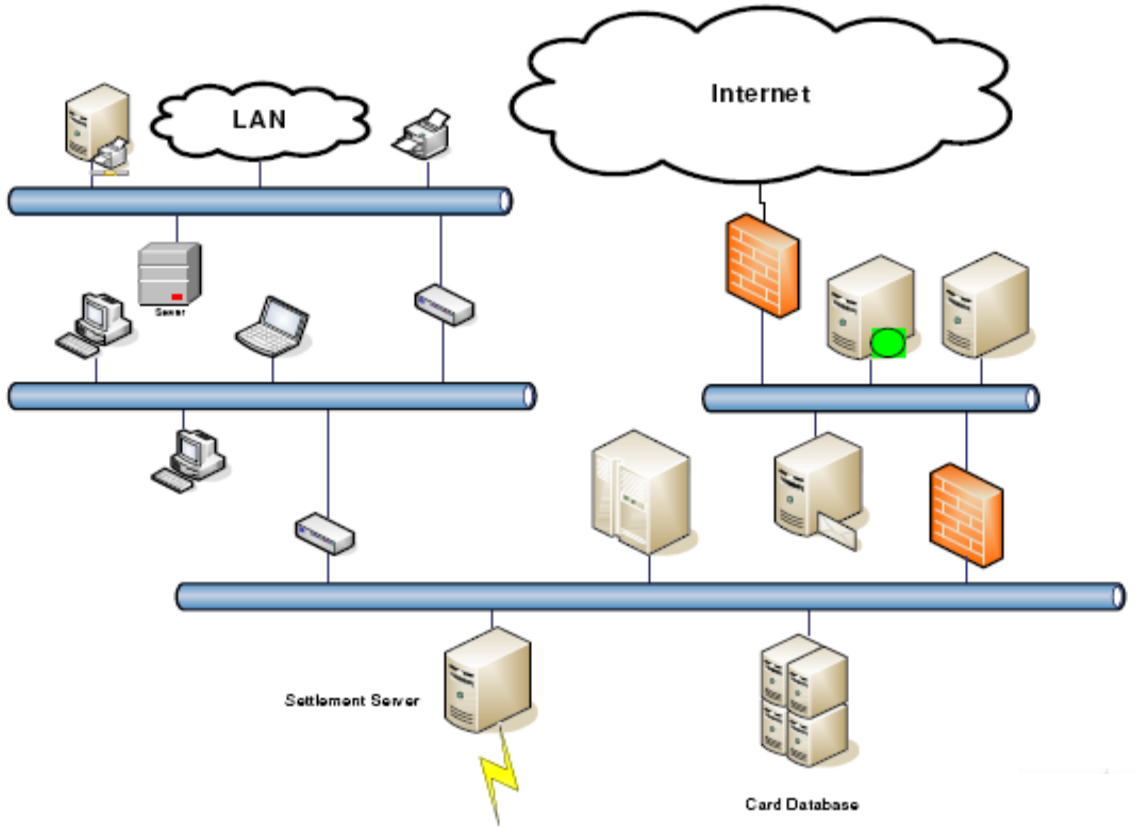
©2026 CliftonLarsonAllen LLP

Exercise - Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

- Why?



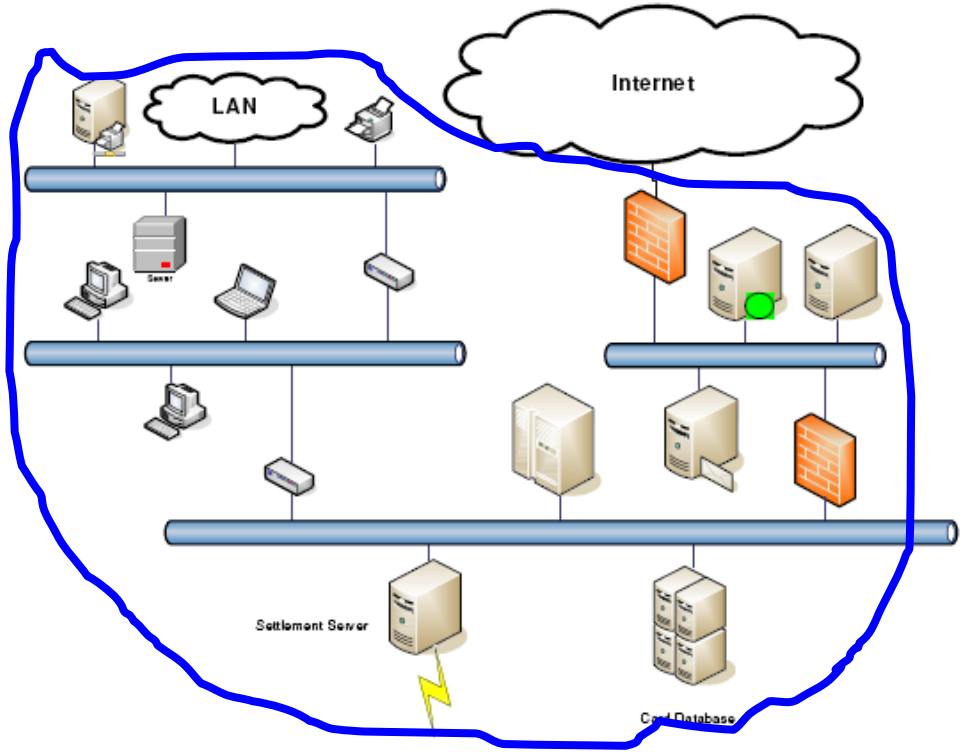
©2026 CliftonLarsonAllen LLP

Exercise - Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

- Why?



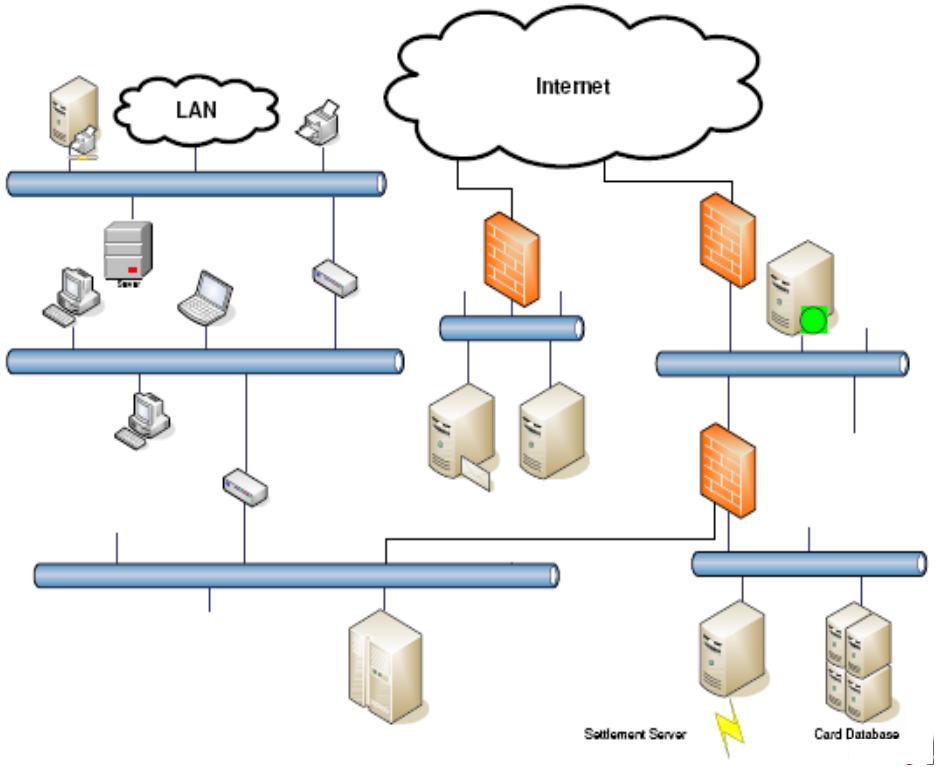
©2026 CliftonLarsonAllen LLP

Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?



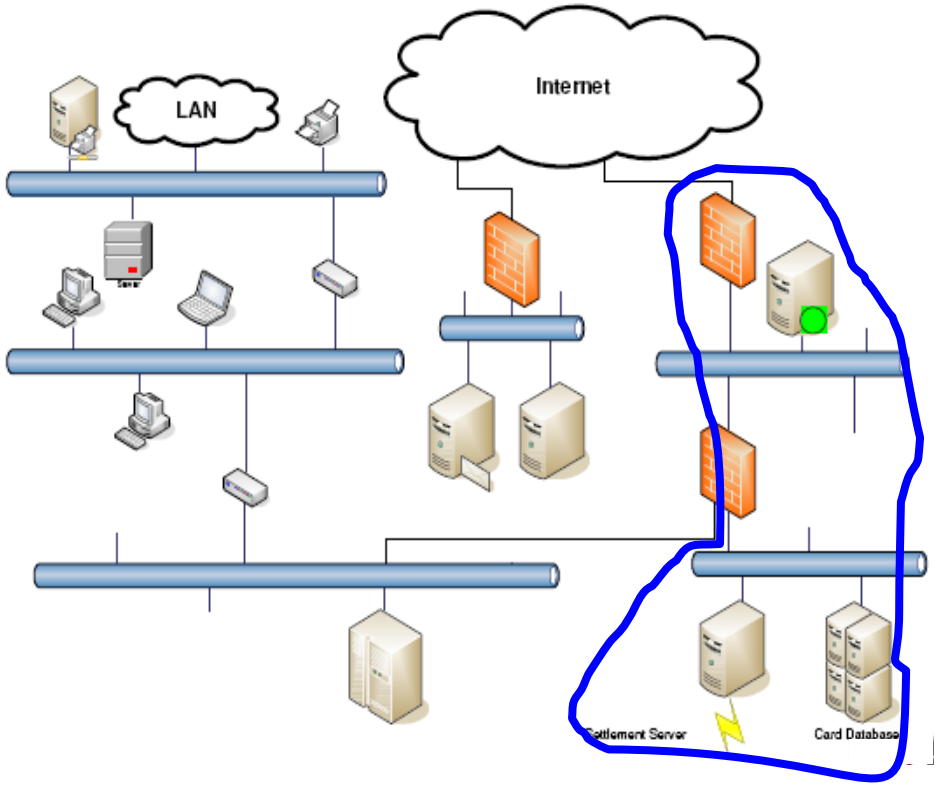
©2026 CliftonLarsonAllen LLP

Segment Your Network

What is in-scope here?

- NOTHING
- Firewalls
- Servers
- PCs
- Everything

Why?



©2026 CliftonLarsonAllen LLP

Polling Question #5

- Which of the following are part of the scope of the Cardholder Data Environment (CDE)?

A. People, Processes, and Technology that interact with CHD
B. Systems and processes that Store, Process, or Transmit CHD
C. Vendors that are involved with A and B above
D. All of the above

* CHD – Card Holder Data

©2026 CliftonLarsonAllen LLP

Common Challenges and Road Blocks

- **PCI is NOT Risk – Based**
- Isolation/segmentation is difficult
  - CHD is in the enterprise application(s)
  - CHD is in secondary systems
- Card data is received over the phone
  - Phone calls/IVR receives PAN – transmitted electronic CHD
  - Service center records phone calls – stored electronic CHD
  - Phone system is Voice over IP
    - touches everything… is integrated to everything…
- Lock Box Services

Think about these:

Finance system
Secondary Enterprise Apps
Phone Systems
Call Center

Departments

Fire and Safety
Parks and Rec
Entertainment Venues
Parking
Public Transit
Utility/Water
Law Enforcement
Courts
Zoning/Permits/Licenses
DMV
Tax

©2026 CliftonLarsonAllen LLP

Common Challenges and Road Blocks

- Applications/systems cannot meet PCI controls…
  - Encryption/File integrity monitoring
  - Different departments use different solutions/different vendors
- Data warehouse and analytics…
  - Reports (PDF, XLSX, etc.) contain PAN
    - Enterprise/vendor software generates reports with PAN data
    - These reports propagate in email and on network file shares
- Vendor software doesn't follow PCI guidelines
  - Vendor software stores clear-text PAN; has hard coded passwords
  - Vendor software is NOT architected to support PCI compliance controls

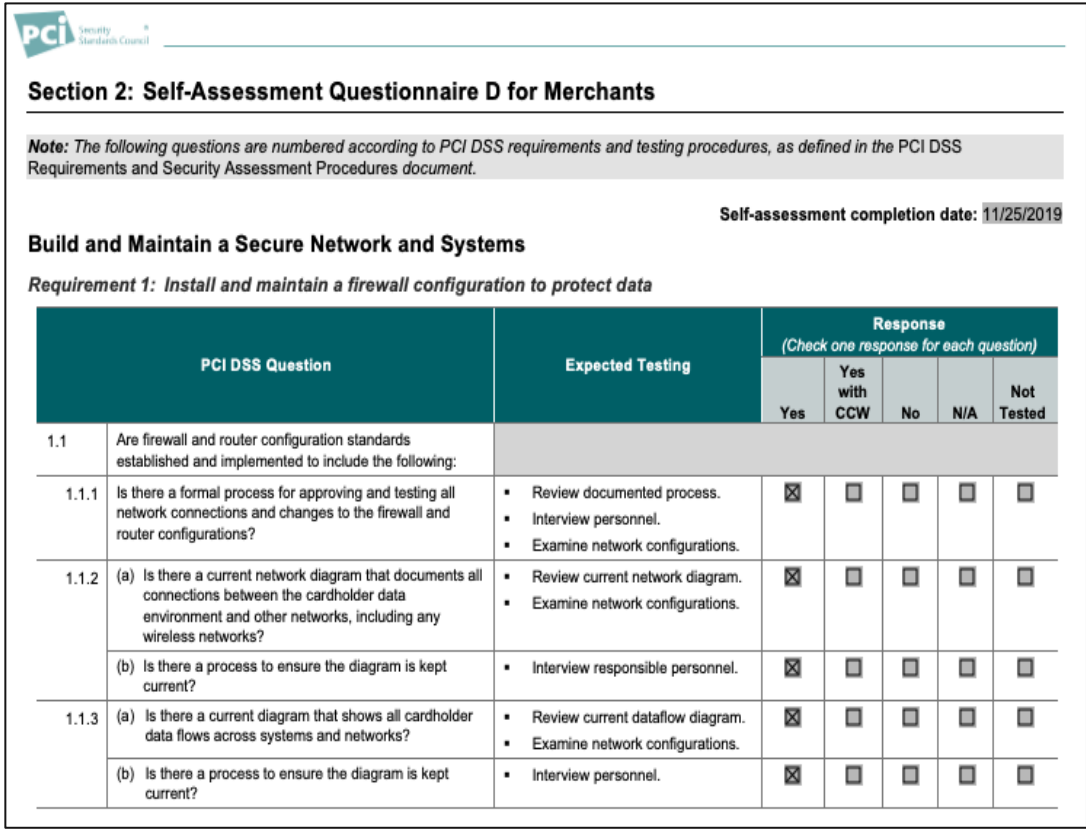
©2026 CliftonLarsonAllen LLP

Self-Assessment Questionnaire (SAQ) – “It’s a Trap!”

The PCI DSS SAQ reporting consists of two components:

1. Questions corresponding to the PCI DSS requirements
   - Minimal to no Narrative

2. Attestation of Compliance
   - A SUMMARY – The organizations certification of eligibility to perform and have performed the appropriate Self-Assessment. The correct Attestation will be packaged with the SAQ selected.



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?	▪ 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.	☒	☐	☐	☐	☐

©2026 CliftonLarsonAllen LLP

PCI DSS Report on Compliance (ROC)

The PCI DSS ROC consists of:

1. ROC is a detailed narrative of controls
   - Appropriate to financial institutions, issuers, service providers, merchants
   - ***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

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: • 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*

©2026 CliftonLarsonAllen LLP

PCI Prioritized Approach Supplement / Guidance

"How do you eat an Elephant?"

One bite at a time…

The SSC has produced guidance and tools to work through a prioritized approach.

Focus on what to do first:

- Address highest risks
- Most "bang for your buck"

The Prioritized Approach to Pursue PCI DSS Compliance

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The following table summarizes the high-level goals of each milestone.

Milestone	Goals
1	**Do not store sensitive authentication data and limit cardholder data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other account data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	**Protect systems and networks and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises and the response processes.
3	**Secure payment applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas are easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning access to your network and cardholder data environment.
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, this milestone targets key protection mechanisms for the stored data.
6	**Complete remaining compliance efforts, and ensure all controls are in place.** This milestone completes PCI DSS requirements and finishes all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



PARTICIPATING ORGANIZATIONS

Merchants, service providers, banks, processors, developers, and point of sale vendors.

https://www.pcisecuritystandards.org/document_library/

©2026 CliftonLarsonAllen LLP

Key Changes in Version 4

- Assigned responsibility (defined in Req 1 – required throughout)
- Enhanced cryptography – full PAN, disk encryption (Req 3)
- New Phishing protection mechanisms (Req 5)
- Public facing websites (Req 6 and Req 11)
- ***Vulnerabilities need to be addressed (Req 6 and Req 11.3.1)***
- Stronger Authentication – MFA, Passwords (Req 8)
- Logging (Req 10)
- Authenticated vulnerability scanning (Req 11)
- Annual scope confirmation (Req 12)
- Targeted Risk Analysis (TRA) – there are 9 of them (Req 12)



©2026 CliftonLarsonAllen LLP

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	5.3.2	Evaluation of systems as "not at risk" to malware
TRA	7.2.5.1	Application and system accounts access reviewed based on TRA frequency _____
TRA	8.6.3	Frequency of change of passwords for application and system accounts
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	11.3.1.1	All other applicable vulnerabilites **are addressed**
TRA	11.6.1	Change and tamper detection for web page payment pages is performed every ____
TRA	12.10.4.1	IR personnel training updated based on TRA

©2026 CliftonLarsonAllen LLP

Polling Question #6

- True or False

- Our organization only has to be PCI DSS compliant if we accept more than 1,000,000 credit card transactions

©2026 CliftonLarsonAllen LLP

Summary



©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

PCI Summary:

1. Understand and define your CDE (every year – this is required)
   A. Identify People and Processes that interact with CHD
   B. Identify Technology that People and Processes interact with
   C. **You MUST do this first – otherwise the rest is done on faulty premise**
2. Organize A and B to determine in-scope controls
3. Confirm your “level” – the number of transactions whose security you can impact (not $ amount)
4. Use #3 to confirm your reporting format (ROC or SAQ)
5. Map current controls to PCI and identify gaps
6. Implement PCI controls into “daily business as usual”
7. Have compliance report ready for when it is needed

©2026 CliftonLarsonAllen LLP

Be Prepared…

Prepare

Operate

Test

- Standards Based Operations and Exception Management
  - Pick a Framework
  - Daily Operational DNA
- Regular/periodic risk assessment:
  - Daily Business as Usual
- Monitor and fine tune:
  - Continuous improvement
  - Ensure security operations tools support IT and Forensic needs
- **Practice and Test**
  - Audit your operations controls (against a framework)
  - Red Team and Purple Team engagements to test and validate preventative controls aligned to logging, monitoring, and alerting
  - Schedule IR Tabletop and Disaster Recovery exercises

©2026 CliftonLarsonAllen LLP

Thank you!

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA
Principal – Cybersecurity
612.397.3114
randy.romes@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

©2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.