RSI Security

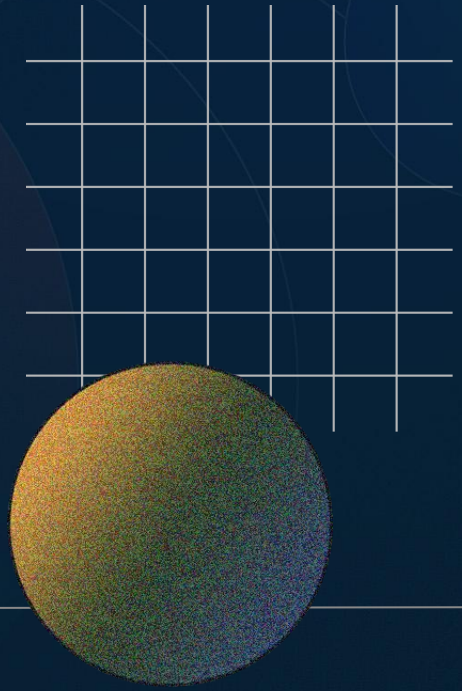
Rethinking Your Cybersecurity

Mohan Shamachar
Director of Information Security & Compliance

Agenda

1 **About RSI Security**

2 **PCI DSS Overview**



3 **PCI DSS 4.0**
Goals
What's New?
Assessor, Merchant and Service Provider To Dos

4 **Q/A**

About RSI Security

- vCISO & Advisory Services
- Compliance Assessments
- Risk Assessments
- Maturity Assessments
- Incident Response
- MSSP

- PCI DSS
- HITRUST
- HIPAA
- SOC 2
- NIST CSF, NIST 800-171
- Privacy
- CIS

What is PCI DSS?

Payment Card Industry Data Security Standard

- Technical and operational requirements designated to protect ***account data***.
- PCI Security Standards Council (PCI SSC)
  - Founded in 2006 by Payment Card Brands - American Express, Discover, JCB International, Mastercard and Visa Inc; Maintain, Evolve and Promote PCI standards.

Applicability:

- Entities with CDE where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted
- Entities with environments that can impact the security of the CDE
- Entities that are responsible for the protection of *account data*

PCI DSS 4.0

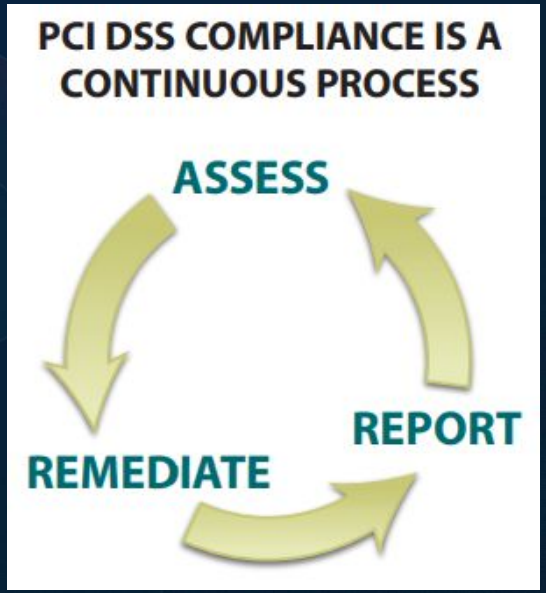

Goals for PCI DSS v4.0
Continue to Meet the Security Needs of the Payment Industry
Promote Security as Continuous Process
Add Flexibility for Different Methodologies
Enhance Validation Methods

PCI DSS 4.0: Overview

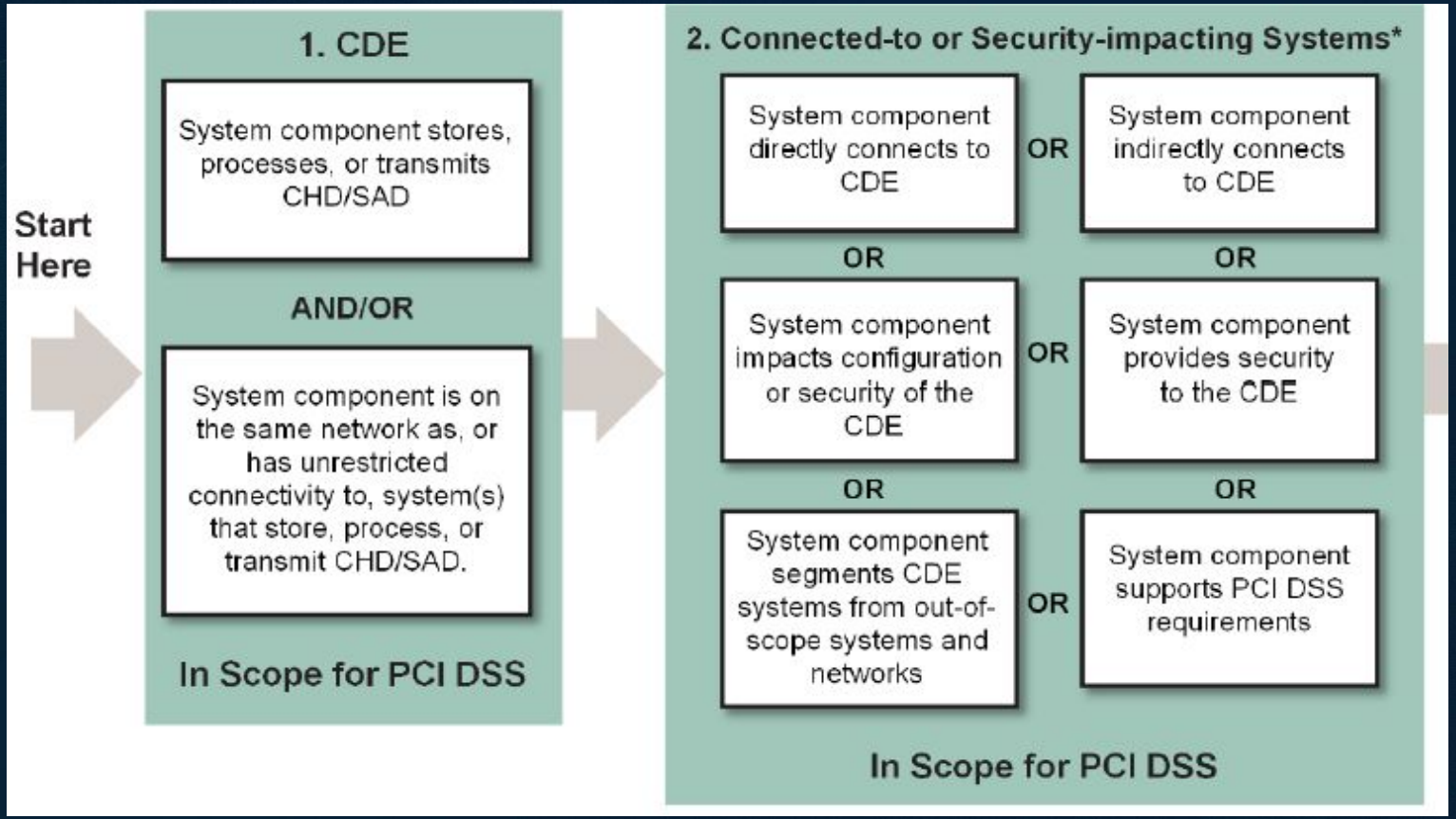
PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography 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 Compliance Process

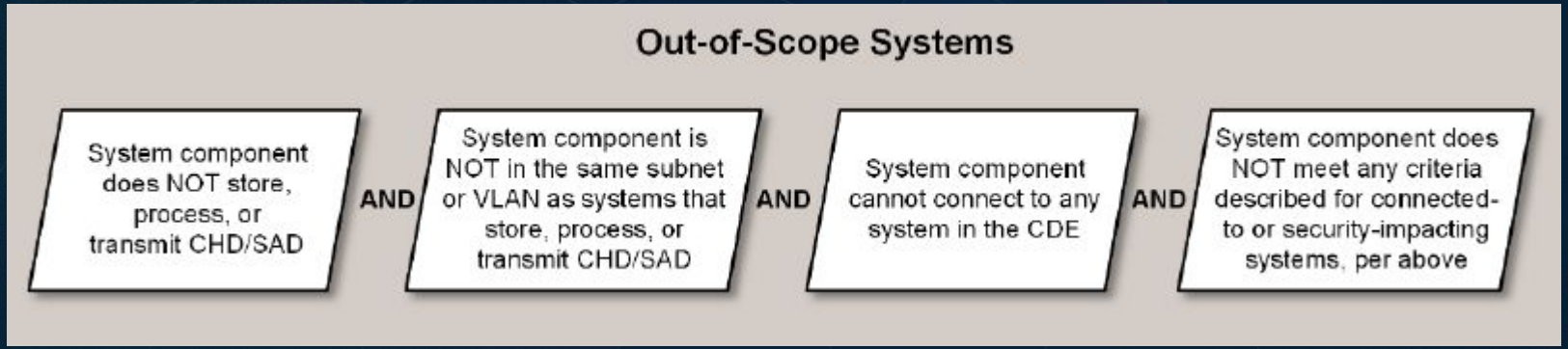
- Assessing
  - Testing and verifying controls in place to protect account data
- Remediating
  - Fix the vulnerabilities
- Reporting
  - Validate compliance and present evidence of data protection controls
- Monitoring & Auto Alerting
  - Constantly monitor access and usage of data, including the logs



Scoping: Components In Scope



Scoping: Components Out of Scope



Scoping: Environment with encrypted cardholder Data

- Systems performing encryption, decryption and systems performing key management functions
- Encrypted cardholder data that is not isolated from the encryption and decryption and key management processes
- Encrypted cardholder data that is present on a system or media that also contains the decryption key
- Encrypted cardholder data that is present in the same environment as the decryption key
- Encrypted cardholder data that is accessible to an entity that also has access to the decryption key

Customized Approach

- Meet the stated Customized Approach Objective
- Entity determines and designs the security control
- At least meet or exceed the security provided by the defined requirement
- Require extensive documentation: For each customized control
  - Controls Matrix Template
  - Perform Target Risk Analysis
  - Testing evidence
  - Monitoring and Evidence of effectiveness of each customized control
- Assessor: Create and document testing procedures for each customized control
- Entity's Decision.
  - Acceptable to QSA and/or Acquirer
- Defined, Customized or Combination of assessment allowed for each applicable requirement

Compensating Controls vs Customized Approach

Compensating Control

- Cannot meet the defined requirement as stated due to technical or business constraint
- Risk mitigation via alternative control
- Meet the original intent, above and beyond other PCI DSS requirements

Custom Control

- Strategic implementation choice
- Meet the stated Customized Approach Objective
- Compensating control is not an option

Custom Controls Matrix

- Name of the custom control
- Requirement(s) and Stated Objective(s) met by the control
- Control functions
- Control locations (facilities, systems, applications)
- Control execution: Frequency, schedule, real-time, intervals, #of times
- Control owner: Roles/Personnel
- Control maintenance: Roles/Personnel/Teams
- Description: How the control meets the objectives
- Testing performed and test results
- Target Risk Analysis Result Summary

Roles and Responsibilities

- Control: Document and assign roles and responsibilities for performing the control activities
- Assessment: Examine documentation and Interview personnel
  - Example: Responsible, Accountable, Consulted, Informed (RACI Matrix)

Data Retention Policy and Security: Sensitive Authentication Data (SAD)

[3.2.1, 3.3.2, 3.3.3]

- Control: Address SAD within the data retention and disposal policies, procedures, and processes
- Control: Encrypt SAD stored *prior to authorization*; Issuer Functions
- Assessment: Examine documentation, system records, observe mechanisms and interview personnel;
- Merchant/SP*: SAD should not be retained even if encrypted*

PAN Security at Rest [3.4.1, 3.4.2, 3.5.1]

- Control: PAN is masked
  - Only personnel with a business need can see more than the BIN/last four digits
- Control: When using remote access, prevent copy and/or relocation of PAN
  - Except with authorization and business need
- Control: PAN hashes must be keyed cryptographic hashes with key-management
- Control: Use disk or partition level encryption of PAN on removable media only
  - Non removable media must has additional PAN security controls
- Assessment: Examine docs, roles that need access, hashing methods, logs, crypto architecture, technical controls and Interview personnel
- TPSPs: Prevent the use of the same encryption keys in production and test environments

PAN Security During Transmission

- Control: Confirm certificate is valid, not expired or revoked
- Control: Inventory of trusted keys and certificates
- Assessment: Examine docs, inventory, technical controls and Interview personnel

Anti-phishing [5.4.1]

- Control: Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks
- Assessment: Examine documentation, mechanism, observe processes

Public-Facing/Web App Security [6.4.2, 6.4.3]

- Control: Deploy an automated technical solution to continually detect and prevent web-based attacks
- Control: Authorize, Inventory, Assure integrity of all payment page scripts that are loaded and executed in the consumer's browser
- Assessment: Examine documentation, system configuration settings, inventory records, audit logs, and interview responsible personnel

Access Management [7.2.4, 7.2.5, 7.2.5.1]

- Control: Review and remediate all user accounts and access privileges, including third party/vendor accounts
  - At least once every 6 months; management acknowledgment
- Control: Manage, assign and review all application and system accounts and related access privileges
  - Periodically; Management acknowledgment; least privileges
- Assessment: Examine documentation; examine user, system, application accounts, and config settings; observe logins; interview personnel

User Identification and Authentication: Password Use & Management [8.3.6, 8.3.9]

If password is the ONLY authentication factor (non MFA):

- Control: Minimum password length = 12 (8 if not supported)
  - POS terminal accounts/cashiers, consumers, non-consumer customer accounts excluded
- Control: Change passwords at least once every 90 days OR perform dynamic analysis of account security and determine access at real-time
  - For in-scope systems that are not in the CDE
  - TPSPs: Applicable to customer user access; optional guidance to customers until March, 2025
- Assessment: Examine documentation, config settings and interview personnel

Multifactor Authentication (MFA) [8.4.1, 8.4.2, 8.4.3]

- Control: MFA for all non-console access into the CDE for personnel with administrative access.
  - Best practice for components outside of CDE
- Control: MFA for all access to CDE
- Control: MFA for all remote network access originating from outside the entity's network that could access or impact the CDE
- Assessment: Examine documentation, config settings and Interview personnel

Logging and Monitoring [10.4.1, 10.7.2, 10.7.3]

- Control: Review audit logs at least once daily
- Control: Use automated mechanisms to review audit logs
- Control: Detect, alert and address critical security control failures
  - Network security, IDS/IPS, change detection, physical/logical access, logging, segmentation, log review, testing, anti-malware
- Assessment: Examine documentation, log review mechanisms, detecting and alerting mechanisms, failure/response records

Authenticated Internal Scans [11.4.7]

- Control: Perform authenticated internal scans
- Assessment: Examine documentation, scanning mechanisms, tool configs, interactive login accounts used for scanning

Targeted Risk Analysis (TRA) [12.3.1, 12.3.2]

- Control: Perform targeted risk analysis
  - For controls with flexibility of control activity frequency based on the risk to CDE
  - Systems not known to be at risk from malware
  - Periodic malware scans
  - Periodic review of applications and systems access privileges
  - Periodic password changes
  - Periodic POI device inspections
  - Periodic log reviews for lower-risk system components
  - Addressing lower ranked vulnerabilities
  - Detection and response to payment page tampering/skimming
- Assessment: Examine TRA process and documented TRA.
  - Assets, threats, likelihood/impact, frequency and justification
  - Review TRA at least once annually

Scope review and confirmation [12.5.2, 12.5.3]

- Control: Document and confirm the scope every 12 months and upon significant change
  - Data flows and payment channels
  - Account data locations [CDE change]
    - Data discovery - processing, at rest and in transmission
  - CDE, connected to, and security impacting system components, third party connections/access to CDE
  - Segmentation controls and out-of-scope justification
- Assessment: Examine documented results of scope review
- TPSPs: Every 6 months
- Service Providers: Review the impact to the scope and controls due to change in org. structure; communicated to executive management

Significant Change Criteria

- New hardware, software, or networking equipment added to the CDE
- Replacement or major upgrades of hardware and software in the CDE
- Flow or storage of account data
- CDE boundary and/or assessment scope
- Underlying/supporting CDE infrastructure (directory services, time servers, logging, and monitoring)
- Third-party vendors/service providers (or services provided)

RoC Reporting

Removed

- PCI DSS version number
- Connected entities
- Other business entities
- Wireless summary
- Managed service providers

New

- Remote access activities
- Use of subcontractors
- Overall assessment result
- Storage of Sensitive Authentication Data (SAD)
- Quarterly internal scan results

RoC Reporting

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

PCI DSS Requirement
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note:*** *Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*			<Enter Response Here>	

New: In Place With Remediation [Not in Place before the completion of the assessment]

- Missed ASV scans
- Correct the process to prevent recurrence
- QSA is assured of this correction

Resources

- https://blog.pcisecuritystandards.org/topic/pci-dss-v4-0
- https://www.pcisecuritystandards.org/merchants/
- https://blog.pcisecuritystandards.org/pci-dss-v4-0-a-conversation-with-the-council
- https://www.rsisecurity.com

QUESTIONS?

Guides & Events

BLOG

Our extensive library of security & compliance articles:

blog.rsisecurity.com

RESOURCES

In-depth guides, checklists, whitepapers, and case studies:

rsisecurity.com/resources

EVENTS

Monthly educational webinars:

rsisecurity.com/events

Thank You

ADDRESS: 10531 4S Commons Dr.
Suite 527
San Diego, CA 92127

PHONE: 858-999-3030

EMAIL: info@rsisecurity.com

WEBSITE: rsisecurity.com

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

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
		Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2 [2]	No
		Service Code		
		Expiration Date		
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization as defined in Requirement 3.3.1 [3]	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
		Card verification code		
		PIN/PIN Block		