CHECKLIST

PCI DSS

Clearly defining scope is one of the most critical steps in a successful PCI DSS assessment. A well-defined scope reduces risk, limits compliance effort, and avoids unnecessary remediation by ensuring that only systems, processes, and people that impact payment card data are included.

PCI DSS scope includes all system components, networks, applications, and personnel that store, process, transmit, or can impact the security of cardholder data (CHD) or sensitive authentication data (SAD).

Independence Notice: Advisory and remediation services are provided separately from any formal PCI DSS assessment activities, in accordance with PCI SSC independence requirements.

Identify Data Types

Identify and document all payment-related and sensitive data handled within the environment, including:

- [ ] Cardholder Data (CHD)
- [ ] Sensitive Authentication Data (SAD)
- [ ] Payment-Related Financial Data
- [ ] Authentication and Access Credentials
- [ ] Logs or Metadata Containing CHD

Understand Data Flows

Document how cardholder data flows through the environment from entry to exit:

- [ ] Identify data entry points
- [ ] Track internal data movement
- [ ] Identify storage locations
- [ ] Identify exit points
- [ ] Include non-obvious data flows
- [ ] Capture data transmission methods

Identify In-Scope System Components

Determine which components are included in PCI DSS scope, such as:

- [ ] Servers, databases, and applications that store, process, or transmit CHD
- [ ] Network devices and security controls (firewall, switches, load balancers)
- [ ] Virtualization platforms, cloud services, and container environments
- [ ] User endpoints and administrative systems with access to the CDE
- [ ] Third-party systems or services that can impact CHD security

Evaluate Segmentation and Scope Reduction

- [ ] If network segmentation is used to reduce scope:
- [ ] Document segmentation controls and boundaries
- [ ] Validate that segmentation is effective and enforced
- [ ] Confirm that out-of-scope systems cannot access the CDE
- [ ] Include segmentation testing results as supporting evidence

Document Scope Decisions

- [ ] Maintain network and data-flow diagrams reflecting current scope
- [ ] Document in-scope and out-of-scope systems with justification
- [ ] Review and update scope documentation:
  - [ ] At least annually
- [ ] After significant changes to the environment

Requirement 1

Install and Maintain Network Security Controls (NSCs)

1.1 Define and Understand Processes and Mechanisms

1.1.1 Document and maintain security policies and operational procedures for network security controls.

1.1.2 Assign and communicate roles and responsibilities for NSC management.

1.2 Configure and Maintain Network Security Controls

1.2.1 Establish configuration standards for NSCs.

1.2.2 Manage all NSC changes through a formal change control process.

1.2.3 Maintain accurate network diagrams showing CDE and wireless connections.

1.2.4 Maintain accurate data-flow diagrams for CHD.

1.2.5 Identify, justify, and approve all allowed services, protocols, and ports.

1.2.6 Implement additional security for insecure services where required.

1.2.7 Review NSC configurations at least every six months.

1.2.8 Secure NSC configuration files.

1.3 Restrict Network Access

1.3.1 Restrict inbound traffic to only what is necessary.

1.3.2 Restrict outbound traffic from the CDE.

1.3.3 Place NSCs between wireless networks and the CDE.

1.4 Trusted vs. Untrusted Networks

1.4.1 Implement NSCs at all connections between trusted and untrusted networks.

1.4.2 Restrict inbound traffic from untrusted networks.

1.5 Dual-Homed Devices

1.5.1 Ensure dual-homed devices do not compromise CDE security.

Requirement 2

Apply Secure Configurations to All System Components

2.1 Processes and Roles

2.1.1 Document secure configuration policies.

2.1.2 Assign configuration management responsibilities.

2.2 Secure Configuration Standards

2.2.1 Establish secure configuration standards aligned with industry benchmarks.

2.2.2 Apply standards consistently.

2.2.3 Review standards annually.

2.2.4 Maintain system component inventory.

2.2.5 Enable only required services and ports.

2.3 Default Accounts and Settings

2.3.1 Change vendor default passwords before deployment.

2.3.2 Remove or secure default accounts.

2.4 Configuration Integrity

2.4.1 Verify secure configurations before deployment.

2.4.2 Perform configuration integrity checks regularly.

Requirement 3

Protect Stored Account Data

3.1 Policies and Roles

3.1.1 Document data protection policies.

3.1.2 Assign responsibilities for account data protection.

3.2 Storage Minimization

3.2.1 Retain account data only as needed.

3.2.2 Securely delete data when no longer required.

3.3 Sensitive Authentication Data

3.3.1 Do not store SAD after authorization.

3.4 PAN Protection

3.4.1 Render PAN unreadable using strong cryptography or approved methods.

3.4.2 Mask PAN when displayed.

3.5 Cryptographic Key Management

3.5.1 Protect cryptographic keys from disclosure.

3.5.2 Restrict key access.

3.5.3 Use secure key storage mechanisms.

3.6 Key Lifecycle

3.6.1 Document key lifecycle processes.

3.6.2 Rotate keys periodically and upon compromise.

3.7 Testing

3.7.1 Test key management processes at least annually.

Requirement 4

Protect Cardholder Data During Transmission

4.1 Policies and Roles

4.1.1 Document policies for protecting data in transit.

4.2 Strong Cryptography

4.2.1 Use strong cryptography for transmission over open networks.

4.2.2 Accept only trusted keys and certificates.

4.2.3 Prevent fallback to insecure protocols.

4.3 Sensitive Authentication Data

4.3.1 Never send unprotected SAD via end-user messaging.

Requirement 5

Protect All Systems from Malicious Software

5.1 Policies and Roles

5.1.1 Document malware protection policies.

5.2 Malware Protection

5.2.1 Identify systems at risk.

5.2.2 Deploy anti-malware solutions.

5.2.3 Ensure solutions are active and updated.

5.3 Alternative Controls

5.3.1 Evaluate systems not commonly affected by malware.

5.4 Logging and Alerts

5.4.1 Log and alert on malware events.

Requirement 6

Develop and Maintain Secure Systems and Software

6.1 Policies and Roles

6.1.1 Document secure development policies.

6.2 Vulnerability Management

6.2.1 Identify and rank vulnerabilities.

6.2.2 Remediate vulnerabilities based on risk.

6.3 Secure Development Practices

6.3.1 Train developers annually.

6.3.2 Integrate security throughout the SDLC.

6.3.3 Review custom code prior to release.

6.4 Public-Facing Web Applications

6.4.1 Protect web applications.

6.4.2 Review protections annually.

6.4.3 Detect unauthorized changes to payment page scripts.

Requirement 7

Restrict Access by Business Need to Know

7.1 Policies and Roles

7.1.1 Document access control policies.

7.2 Role-Based Access

7.2.1 Define access needs.

7.2.2 Enforce least privilege.

7.3 Access Reviews

7.3.1 Review access rights at least every six months.

Requirement 8

Identify Users and Authenticate Access

8.1 Policies and Roles

8.1.1 Document authentication policies.

8.2 User Identification

8.2.1 Assign unique IDs.

8.2.2 Disable access for terminated users.

8.3 Authentication

8.3.1 Secure authentication credentials.

8.4 Multi-Factor Authentication

8.4.1 Implement MFA for administrative and remote access.

8.5 Credential Management

8.5.1 Enforce password/passphrase standards.

Requirement 9

Restrict Physical Access to Cardholder Data

9.1 Policies and Roles

9.1.1 Document physical security policies.

9.2 Physical Access Controls

9.2.1 Restrict access to CDE areas.

9.2.2 Log and review physical access.

9.3 Visitor Management

9.3.1 Authorize and escort visitors.

9.4 Media Protection

9.4.1 Secure physical media.

9.4.2 Destroy media securely.

9.5 POI Devices

9.5.1 Maintain POI device inventory.

Requirement 10

Log and Monitor Access

10.1 Policies and Roles

10.1.1 Document logging policies.

10.2 Log Activities

10.2.1 Enable logging of security events.

10.3 Log Protection

10.3.1 Protect logs from modification.

10.4 Log Reviews

10.4.1 Review logs daily.

10.5 Automated Monitoring

10.5.1 Use automated alerting mechanisms.

10.6 Log Collection

10.6.1 Monitor log collection failures.

10.7 Testing

10.7.1 Test logging mechanisms annually.

Requirement 11

Test Security of Systems and Networks

11.1 Policies and Roles

11.1.1 Document testing policies.

11.2 Vulnerability Scanning

11.2.1 Perform internal scans quarterly.

11.2.2 Perform external scans using ASV.

11.3 Penetration Testing

11.3.1 Perform penetration testing annually.

11.4 IDS/IPS

11.4.1 Deploy detection/prevention mechanisms.

11.5 File Integrity Monitoring

11.5.1 Monitor critical files.

11.6 Alerting on Script Changes

11.6.1 Alert personnel when unauthorized payment page script changes occur.

Requirement 12

Support Information Security with Organizational Policies and Programs

12.1 Policies and Roles

12.1.1 Maintain an information security policy.

12.2 Policy Review

12.2.1 Review policies annually.

12.3 Risk Assessment

12.3.1 Perform annual risk assessments.

12.4 Executive Responsibility

12.4.1 Assign executive accountability.

12.5 Security Awareness

12.5.1 Provide training at hire and annually.

12.6 Incident Response

12.6.1 Maintain and test an incident response plan.

12.7 Third-Party Management

12.7.1 Manage service provider security.

12.8 Account Management

12.8.1 Monitor user accounts.

12.9 Documentation

12.9.1 Maintain program documentation.

12.10 Responsibility Acknowledgment

12.10.1 Service providers acknowledge PCI DSS responsibilities.

12.11 Continuous Monitoring

12.11.1 Perform continuous control monitoring.

About RSI Security

RSI Security provides advisory and technical services to support PCI DSS readiness, including scoping assistance, gap assessments, control alignment, documentation development, and compliance program support. Services are delivered through clearly separated advisory and assessment functions to preserve objectivity and maintain assessment independence.

www.rsisecurity.com | (858) 999-3030 | info@rsisecurity.com