Security program documentation establishes a foundation needed for organizations to effectively define and communicate control requirements. While critical to the success of a security program, keeping up with documentation requirements can be challenging for any organization. Whether you are just starting to develop a security program, or making continuous improvements to an established security program, this documentation checklist for PCI DSS will help ensure that your organization maintains the appropriate documentation to support a successful security program. While this list may not be all inclusive for all organizations, you will likely need to account for these documents in some manner to achieve your compliance goals.

PCI DSS is comprised of 12 standard control families for all organizations required to be compliant, plus 3 additional control groups that are based of applicability of individual organizations. Each of the following sections contain the topics that should be addressed for each control family, followed by the recommended documentation that should be used to address them.

PART I: SECURE NETWORKS, DEVICES, AND INFORMATION SYSTEMS

1. FIREWALL CONFIGURATIONS

Topics addressed by documentation for this control family should include:

1.1. Firewall Management Policy and Procedure
1.2. Firewall, Router, and Switch Configuration Standards
1.3. Network Connections and Firewall, Router, and Switch Changes
1.4. Network Diagrams
1.5. Data Flow Diagrams
1.6. Firewall Placements
1.7. Roles and Responsibilities
1.8. Services, Protocols, and Services
1.9. Rule Set Reviews
1.10. Restricting Access to Untrusted Networks
1.11. Inbound and Outbound Traffic Restrictions
1.12. Synchronized Configuration Files
1.13. Perimeter Firewalls
1.14. Restricting Public Access to Cardholder Data
1.15. DMZ Implementation

1.16. Anti-Spoofing Measures
1.17. Outbound Traffic Containing Cardholder Data
1.18. Established Network Connections
1.19. Internal Network Zone
1.20. Private IP Addresses and Routing Information
1.21. Firewall Functionality for Portable Computing Devices

Recommended documentation includes:

- [ ] **Firewall Configuration Policy**
- [ ] **Firewall Configuration Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Firewall, router, and switch configuration standards
- [ ] Network diagrams
- [ ] Data flow diagrams
- [ ] Firewall management roles and responsibilities matrix
- [ ] Evidence of rule set reviews
- [ ] Private IP address and routing information

2. SECURE BASELINE CONFIGURATIONS

Topics addressed by documentation for this control family should include:

2.1. Secure Baseline Configuration Policy and Procedure
2.2. Vendor-Supplied Default Accounts and Passwords
2.3. Baseline Configuration Standards
2.4. Encrypted Administrative Access
2.5. System Component Inventory
2.6. Protected Hosting Environments (for hosting providers)

Recommended documentation includes:

- [ ] **Secure Baseline Configurations Policy**

- [ ] **Secure Baseline Configurations Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Baseline Configuration Standards
- [ ] System component inventory

PART II: PROTECTING CARDHOLDER DATA

3. STORED CARDHOLDER DATA

Topics addressed by documentation for this control family should include:

3.1. Stored Cardholder Data Protection Policy and Procedure
3.2. Data Retention Requirements
3.3. Sensitive Authentication Data
3.4. Masking Primary Account Numbers
3.5. Storing Primary Account Numbers
3.6. Encryption Key Protection
3.7. Key Management Processes

Recommended documentation includes:

- [ ] **Stored Cardholder Data Protection Policy**
- [ ] **Stored Cardholder Data Protection Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Data retention schedule
- [ ] Key custodian acknowledgement

4. DATA TRANSMISSION

Topics addressed by documentation for this control family should include:

4.1. Data Transmission Policy and Procedure

4.2. Transmitting Data Over Open Networks
4.3. Restricting the Use of End User Messaging

Recommended documentation includes:

- [ ] **Data Transmission Policy**
- [ ] **Data Transmission Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Encryption configuration settings for wireless networking

PART III: VULNERABILITY MANAGEMENT PROGRAM

5. MALWARE PROTECTION

Topics addressed by documentation for this control family should include:

5.1. Malware Protection Policy and Procedure
5.2. Antivirus Software Deployment
5.3. Maintaining Antivirus Mechanisms
5.4. Antivirus Software Configurations

Recommended documentation includes:

- [ ] **Malware Protection Policy**
- [ ] **Malware Protection Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Inventory of information assets in the cardholder data environment
- [ ] System-generated report listing asset with anti-malware software installed
- [ ] Anti-malware software configuration documentation

6. SYSTEM AND APPLICATION SECURITY

Topics addressed by documentation for this control family should include:

6.1. System and Application Security Policy and Procedure
6.2. Vulnerability Information
6.3. Vulnerability Patching
6.4. Internal and External Software Applications
6.5. Change Management
6.6. Common Coding Vulnerabilities
6.7. Public-Facing Web Applications

Recommended documentation includes:

- [ ] **System and Application Security Policy**
- [ ] **System and Application Security Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Vulnerability scanning scheduled
- [ ] Vulnerability remediations schedule
- [ ] Vulnerability patching metrics
- [ ] Evidence of separation between production and non-production environments
- [ ] Separation of duties matrix
- [ ] Change control requests and approval decisions
- [ ] List of public-facing web applications

PART IV: ACCESS MANAGEMENT

7. ACCESS CONTROL

Topics addressed by documentation for this control family should include:

7.1. Access Control Policy and Procedure
7.2. Need to Know Principle
7.3. Access Control for System Components

Recommended documentation includes:

- [ ] **Access Control Policy**
- [ ] **Access Control Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] List of job classifications and roles
- [ ] Access requirements for defined roles
- [ ] Approvals for assigning access privileges and permissions

8. IDENTIFICATION AND AUTHENTICATION

Topics addressed by documentation for this control family should include:

8.1. Identification and Authentication Policy and Procedure
8.2. User Identification Management
8.3. User Authentication Management
8.4. Non-Console Administrative Access
8.5. Password Management
8.6. Shared, Group, and Generic Accounts
8.7. Authentication Mechanisms
8.8. Database Access

Recommended documentation includes:

- [ ] **Identification and Authentication Policy**
- [ ] **Identification and Authentication Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Access revocation records

- [ ] List of all accounts
- [ ] List of all active accounts
- [ ] List of inactive accounts
- [ ] List of third-party accounts
- [ ] List of all personnel
- [ ] List of recently terminated personnel
- [ ] List of recently onboarded personnel
- [ ] Reports of failed logon attempts
- [ ] Password composition, complexity, aging, history, and other configurations
- [ ] Inventory of authentication mechanisms

9. PHYSICAL SECURITY

Topics addressed by documentation for this control family should include:

9.1. Physical Security Policy and Procedure
9.2. Physical Entry Controls
9.3. Distinguishing between Personnel and Visitors
9.4. Physical Access to Sensitive Areas
9.5. Visitor Management
9.6. Physical Security for Media
9.7. Media Distribution
9.8. Media Storage
9.9. Media Destruction
9.10. Devices that Capture Payment Card Data

Recommended documentation includes:

- [ ] **Physical Security Policy**
- [ ] **Physical Security Procedure**

- [ ] Control Evidence Document for each applicable control
- [ ] List of physical entry controls
- [ ] List of names and locations of sensitive areas
- [ ] Evidence of visitor log reviews
- [ ] Media inventory
- [ ] Certificates of destruction for destroyed media
- [ ] Inventory of card interaction devices
- [ ] Card interaction device inspection records
- [ ] Training materials for detecting device tampering or replacement

PART V: NETWORK MONITORING AND TESTING

10. AUDITING AND LOGGING

Topics addressed by documentation for this control family should include:

10.1. Auditing and Logging Policy and Procedure
10.2. System Access Audit Logs
10.3. Event Logging
10.4. Content of Audit Records
10.5. System Clock Synchronization
10.6. Audit Log Protection
10.7. Audit Log Reviews
10.8. Audit Log Retention
10.9. Audit Log Processing Failures

Recommended documentation includes:

- [ ] **Auditing and Logging Policy**

- [ ] **Auditing and Logging Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] List of event types logged and/or audited
- [ ] System access audit logs
- [ ] Event logging reports
- [ ] Evidence of audit log reviews
- [ ] Evidence of response to audit log processing failures

11. SECURITY SYSTEMS AND PROCESS TESTING

Topics addressed by documentation for this control family should include:

11.1. Security Systems and Process Testing Policy and Procedure
11.2. Wireless Access Points
11.3. Vulnerability Scanning
11.4. Penetration Testing
11.5. Intrusion Detection and Prevention Tools
11.6. Change Detection Tools

Recommended documentation includes:

- [ ] **Security Systems and Process Testing Policy**
- [ ] **Security Systems and Process Testing Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Inventory of wireless access points
- [ ] Vulnerability scanning reports
- [ ] External penetration test reports
- [ ] Internal penetration test reports

- [ ] Intrusion detection and prevention reports
- [ ] Change detection reports

PART VI: SECURITY PROGRAM POLICIES AND PROCEDURES

12. SECURITY PROGRAM IMPLEMENTATION AND MANAGEMENT

Topics addressed by documentation for this control family should include:

12.1. Security Program Policy and Procedure
12.2. Risk Assessments
12.3. Acceptable Use Requirements
12.4. Security Program Roles and Responsibilities
12.5. Security Program Management
12.6. Security Awareness Training Program
12.7. Personnel Screening
12.8. Service Provider Due Diligence
12.9. Service Provider Responsibilities
12.10. Incident Response
12.11. Security Program Compliance (for service providers)

Recommended documentation includes:

- [ ] **Security Program Implementation and Management Policy**
- [ ] **Security Program Implementation and Management Procedure**
- [ ] Control Evidence Document for each applicable control
- [ ] Risk assessment
- [ ] Risk assessment results
- [ ] Acceptable use requirements
- [ ] Acceptable use acknowledgements
- [ ] List of authorized devices and personnel

- [ ] Defined ownership and purpose for IT assets
- [ ] Security program roles and responsibilities matrix
- [ ] Executive management roles and responsibilities matrix
- [ ] Security awareness training curriculum
- [ ] Security awareness training materials
- [ ] Security awareness training records
- [ ] Personnel screening criteria and records
- [ ] Inventory of service providers
- [ ] Service provider agreements
- [ ] Onboarding process for service providers
- [ ] Risk ranking results for service providers
- [ ] Due diligence assessment for service providers
- [ ] Due diligence results for service providers
- [ ] Service response security responsibility matrix
- [ ] Incident response plan
- [ ] Incident response test scripts
- [ ] Incident response testing reports
- [ ] Incident response training materials and records
- [ ] Quarterly compliance review documentation

PART VII: ADDITIONAL REQUIREMENTS – BASED ON APPLICABILITY

13. SHARED HOSTING PROVIDER REQUIREMENTS

Topics addressed by documentation for this control family should include:

13.1. Authorized Processing
13.2. Environmental Access Restrictions
13.3. Audit Logging
13.4. Forensic Investigations

Recommended documentation includes:

- [ ] Control Evidence Document for each applicable control
- [ ] Audit logging reports
- [ ] Forensic investigation reports, if applicable

14. USE OF SSL OR EARLY TLS

Topics addressed by documentation for this control family should include:

14.1. Susceptibility to Exploits
14.2. Risk Mitigation and Migration Plans (for service providers)
14.3. Secure Service Offering

Recommended documentation includes:

- [ ] Control Evidence Document for each applicable control
- [ ] Risk mitigation and migration plan

15. SUPPLEMENTAL VALIDATION

Topics addressed by documentation for this control family should include:

15.1. PCI DSS Compliance Program
15.2. PCI DSS Scope
15.3. Incorporating PCI DSS into Normal Business Operations
15.4. Logical Access to Cardholder Data

15.5. Identifying and Responding to Suspicious Events

Recommended documentation includes:

- [ ] Control Evidence Document for each applicable control
- [ ] PCI DSS Compliance Program Plan
- [ ] Compliance program roles and responsibilities matrix
- [ ] Compliance program training and records
- [ ] PCI DSS scope documentation and validation
- [ ] List of security control failures
- [ ] Evidence of hardware and software technology reviews
- [ ] Evidence of logical access to cardholder data reviews
- [ ] Evidence of identifying and responding to suspicious events

About ASCENT: The ASCENT Portal is a secure cloud-based system of record that supports the lifecycle management of security program controls and the resulting continuous compliance for organizations of any size, in any industry. As the single source of security and compliance truth, the ASCENT Portal puts everything you need to comply with security control requirements right at your fingertips. From security assessments and calendar-driven control task reminders to governance documentation and vendor management, ASCENT automates your compliance process, end-to-end, while delivering real-time status and reports all from a single source. Visit ascent-portal.com to schedule a demo focused on making the ASCENT to your security and continuous compliance goals.

Don't become overwhelmed by documentation. If you have a question about security program documentation, you can schedule a free 15-minute consultative discussion by clicking here. You do not need to be an ASCENT Portal customer to take advantage of this no-cost opportunity.