

PCI DSS 4.0 CHECKLIST

DRUMMOND



Introduction

PCI compliance is a vital step toward protecting customer financial data, preventing data breaches, and maintaining of market trust. It reduces the risk of costly security incidents and potential legal consequences but also demonstrates a commitment to data security best practices, fostering customer confidence—potentially increasing business opportunities by assuring clients that their sensitive payment information is handled responsibly and securely.
This comprehensive checklist encompasses the 12 requirements and accompanying sub-requirements outlined by the Payment Card Industry Data Security Standard (PCI DSS). We encourage you to review the official PCI DSS documents.

This checklist is NOT an assessment. Its purpose is to help your organization get started on your journey to PCI DSS v4.0 compliance. Drummond's goal is to help your business become compliant across all 300+ security controls within the PCI standards, so you can act to secure the handling, storing and validating of your customer data. Get your free Drummond PCI consultation today and get customized and actionable insights you can use tomorrow.

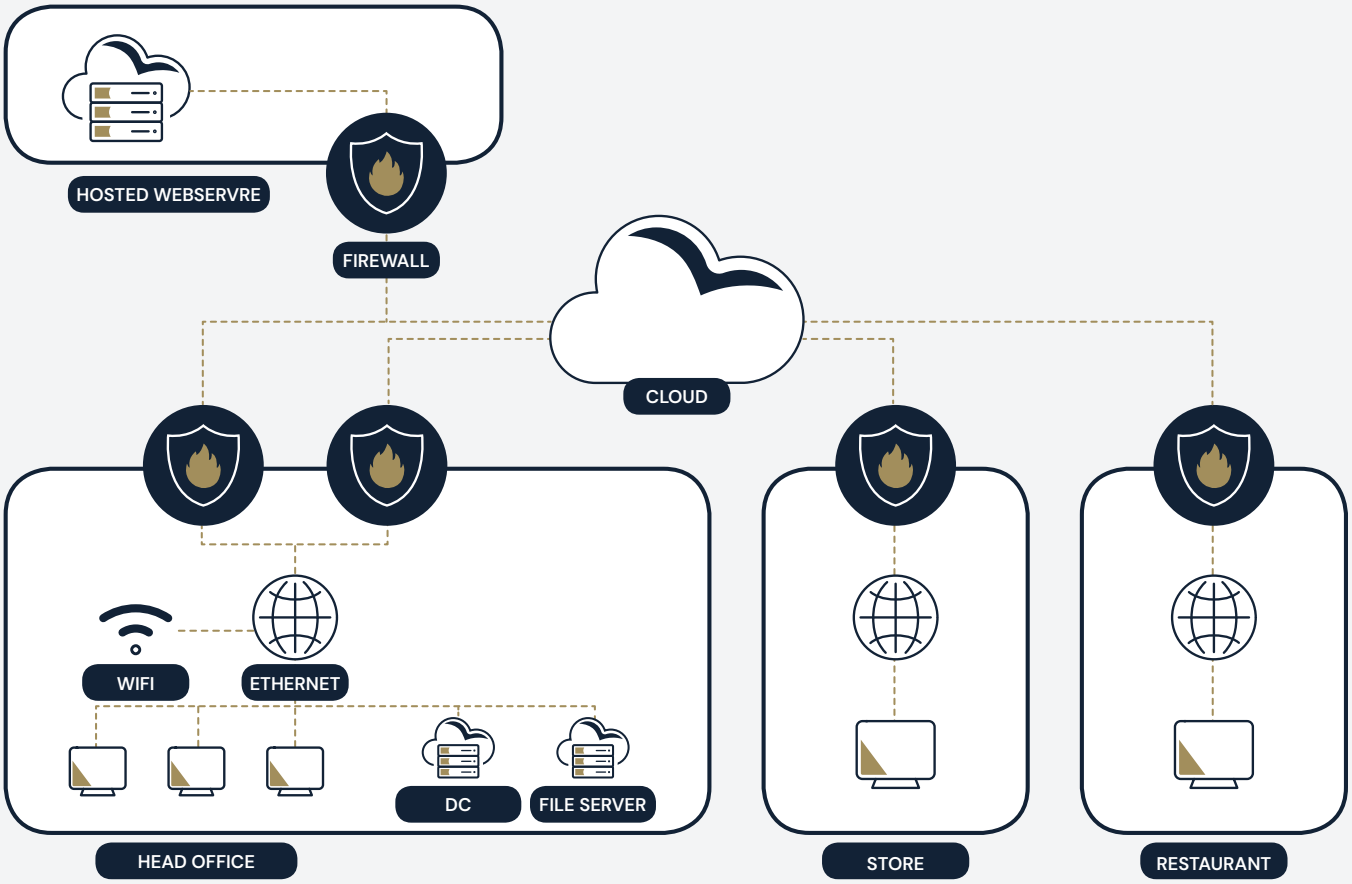
Build and Maintain Secure Networks and Systems

Network security controls (NSCs) are firewalls, and other network security technology and policy enforcement points, used to control traffic between different network segments or subnets. While physical firewalls traditionally served this role, NSCs now encompass virtual and cloud-based solutions, software-defined networking, and virtualization/container systems. These controls are vital for safeguarding computer networks and preventing potentially unprotected pathways into sensitive systems, ensuring data security and compliance with PCI DSS requirements.

To Do:

- Ensure all security policies and operational procedures are documented, kept up to date, in use, and are known to all affected parties. (Requirement #1.1.1)
- Examine security policies and operational procedures to verify descriptions of roles and responsibilities for performing activities are documented and assigned. (Requirement #1.1.2)
- Confirm network security controls (NSCs), such as firewalls, VPNs, Sandboxing, Intrusion Prevention Systems (IPS), Anti-spoofing, Encryption and more, are configured, maintained, and reviewed at least once every six months. (Requirement #1.2.1)
- Maintain a network diagram to illustrate connections involving the Cardholder Data Environment (CDE), other networks (including wireless networks), and to ensure that only essential inbound and outbound traffic is permitted in the CDE, while denying all other non-essential traffic. (Requirement #1.2.3)

Example Network Diagram





Protect Account Data

Effective protection methods like encryption, truncation, masking, and hashing are crucial for safeguarding account data. Even if an intruder bypasses other security measures and access encrypted account data, the information remains unreadable without the necessary cryptographic keys, rendering it unusable for the attacker.

To Do:

- Minimize data storage by implementing data retention and disposal policies covering all locations where account data is stored. (Requirement #3.2.)
- Verify Sensitive Authentication Data (SAD), such as verification codes, tracks, PINS, and more, are protected with encryption prior to authorization and are not retained after authorization, even if encrypted. (Requirement #3.3)
- Confirm safeguards protecting cryptographic keys that protect SAD are in place, such as limiting access to the minimum number of custodians needed, ensuring the strength of key-encrypting keys, storing them separately from data-encrypting keys, and maintaining keys securely in the fewest possible locations and forms. (Requirement #3.6)
- Ensure an inventory of the trusted keys and certificates utilized for safeguarding Primary Account Numbers during transmission is maintained. (Requirement #4.2)

Data Storage Do's and Don'ts

DO's	DONT's
Do document the path of payment card information during the transaction workflow.	Don't retain cardholder data unless it serves a necessary purpose.
Do employ robust encryption to render stored cardholder data indecipherable.	Don't keep sensitive authentication data found in the chip or magnetic stripe of payment cards.
Do adhere to PCI DSS regulations, whether verified through self-assessment or external evaluation.	Don't print or display unmasked cardholder data inadequately.
Do submit mandated PCI DSS compliance reports by their deadlines.	Don't store payment card information on unprotected endpoint devices or transmit it via chat, messaging, or similar end-user messaging platforms.
Do verify that third-party payment card processors adhere to applicable PCI DSS requirements.	Don't place servers or payment card system storage devices in locations that lack full security measures.



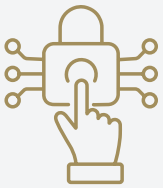
Maintain a Vulnerability Management Program

A cybersecurity vulnerability management program is an organization's systematic approach or process that identifies, assesses, prioritizes, mitigates, and monitors security vulnerabilities in its systems, networks, applications, and infrastructure. This program aims to proactively address weaknesses or flaws that could be exploited by cyber attackers.

Tasks:

- Deploy an anti-malware solution that detects all known types of malware and removes, blocks, or contains all known malware. (Requirement #5.2)
- Configure anti-malware solution(s) to perform periodic and active/real-time scans or perform continuous behavioral analysis of systems and processes. (Requirement #5.3)
- Establish procedures and automated systems to identify and shield personnel from phishing attempts. (Requirement #5.4)
- Confirm custom software is securely developed, adhering to industry standards, PCI DSS requirements, and considering information security throughout the software development lifecycle. (Requirement #6.2)
- Conduct annual training for custom software development personnel encompassing software security relevant to their roles and programming languages, secure software design, coding techniques, and security testing tools for vulnerability detection. (Requirement #6.2)
- Inventory all custom software, along with third-party software components integrated into custom software, and confirm they are properly maintained to streamline vulnerability and patch management. (Requirement #6.2)
- Continually monitor publicly accessible web applications and safeguard them from malicious attacks by an automated technical solution. (Requirement #6.4)

Implement Strong Access Control Measures



Cybersecurity access control measures are mechanisms put in place to manage and regulate access to sensitive information, systems, networks, and resources within an organization's digital environment. These measures aim to ensure that only authorized individuals or entities have the appropriate level of access to specific resources while preventing unauthorized access or misuse.

To Do:

- Establish an access control model to grant access with the least privileges required to perform a job function. (Requirement #7.3)
- Implement multi-factor authentication (MFA) for all access into the CDE. (Requirement #8.4)
- Review all user accounts and related access privileges, including third-party/vendor accounts, every six months to ensure appropriate access. (Requirement #8.6)
- Assign every user a distinct and individual ID before being granted access to system components or cardholder data. (Requirement #8.6)
- Ensure user access to query repositories of stored cardholder data is tightly controlled with appropriate programs or applications. (Requirement #8.6)
- Remove or disable inactive user accounts within 90 days of inactivity. (Requirement #8.6)
- Document and communicate all authentication policies and procedures, which include guidance on selecting strong authentication factors, protecting these factors, avoiding password reuse, and reporting potential compromises.
- Instruct users to change passwords or passphrases if there is suspicion or evidence of compromise.
- Audit electronic media containing cardholder data on an annual basis. (Requirement #9.4)
- Inventory and audit all Point of Interaction (POI) devices, which includes make and model of device, location of device, device serial number. (Requirement #9.5)
- Train Personnel in POI environments to recognize and respond to potential tampering or substitution of POI devices. (Requirement #9.5)



Regularly Monitor and Test Networks

Effective network testing combines comprehensive audit logging and penetration testing methodologies, which individually offer detailed system records and simulated attacks to identify vulnerabilities and analyze system resilience. These practices, when integrated, create a robust framework for proactive network testing.

To Do:

- Establish audit logs to facilitate the identification of irregularities and questionable actions, and the forensic examination of events. (Requirement #10.2)
- Monitor file integrity of audit logs to guarantee that any alterations to the existing log data trigger alerts. (Requirement #10.3)
- Promptly address any exceptions and anomalies discovered during the review.
- Uphold a record of authorized wireless access points, accompanied by a documented business rationale. (Requirement #11.2)
- Perform internal vulnerability scans at least once every three months. (Requirement #11.3)
- Establish, document, and enforce a defined penetration testing approach. (Requirement #11.4)

Audit Log Examples

- Logs from security events
- Logs from system components handling CHD and/or SAD
- Logs from critical system components
- Logs from servers and system components responsible for security functions, such as network security controls, intrusion detection, and authentication servers.
- (Requirement #10.4)



Maintain an Information Security Policy

A cybersecurity Information Security Policy (ISP) is a foundational document that outlines an organization's approach, guidelines, and rules regarding the protection of its sensitive information, digital assets, and overall cybersecurity posture. This policy serves as a framework to establish and communicate the organization's commitment to security and sets the standards and procedures for safeguarding data and technology resources.

To Do:

- Establish, publish, and maintain an overall information security policy. (Requirement #12.1)
- Create an incident response plan for activation if there is a suspected or confirmed security incident. (Requirement #12.1)
- Annually review the information security policy and adjust as required to align with shifts in business objectives or environmental risks. (Requirement #12.1)
- Conduct a specialized risk assessment for every PCI DSS requirement. This evidence requires approval from senior management and must involve the targeted risk analysis being performed on an annual basis. (Requirement #12.3)
- Record and continuously review cipher suites and protocols employed for cryptography. (Requirement #12.3)
- Annually review hardware and software technologies in use. (Requirement #12.3)
- Document and validate the PCI DSS scope annually and whenever there is a significant alteration to the in-scope environment. (Requirement #12.5)
- Train personnel in security awareness at least once every 12 months or upon hire. (Requirement #12.6)



Conclusion

It is important to note that each organization has unique environments and compliance needs. Compliance professionals should seek guidance from external specialists to devise and execute a thorough PCI compliance strategy customized to those needs.

Want to learn more?

Schedule a FREE, no obligation, consultation with Drummond's PCI Compliance expert.

SCHEDULE NOW.

DRUMMOND

(877) 437-8666
sales@drummondgroup.com
www.drummondgroup.com