JOHANSON GROUP

PCI v4.0 Compliance Checklist

Before engaging with a PCI Qualified Security Assessor (QSA), you will want to make sure you have as many items on the following PCI DSS compliance checklist as complete as possible.

This is not comprehensive, but is intended to help identify and address key activities needed to meet each of the 12 PCI DSS requirements.

Scoping

Determine the Scope of Your Cardholder Data Environment (CDE)

- Determine your PCI scope by identifying the people, processes, and technologies that touch or could otherwise impact cardholder data.
- As you're conducting your scoping exercise, you can sort systems into three buckets:
    - **In-scope**: Systems that directly store, process, transmit, or impact the security of cardholder data
    - **Connected to**: Systems not directly involved in processing of cardholder data but are connected to your CDE
    - **Out-of-scope**: Systems that do not directly interact with or connect to your CDE
- Document your scope in a system inventory, cardholder data flow diagram, and network diagram

Step 1

Install and Maintain Network Security Controls

- Isolate cardholder data systems from untrusted networks through network security controls (e.g. firewalls or access control lists). Document the business justification for any enabled port/service
- Review network security control configurations at least every six months

Step 2

Install and Maintain Network Security Controls

- Replace default passwords with strong passwords on every device and system in the CDE
- Harden systems based on industry accepted standards

Step 3

Protect Stored Account Data

- Protect stored cardholder data with appropriate industry-accepted methods, such as strong encryption, non-reversible hashes, or truncation; where possible utilize PCI-compliant third parties to handle and process cardholder data, as this can significantly reduce your scope and compliance responsibilities
- Do not store sensitive authentication data after authorization (even if it's encrypted)
- Create a formal data retention policy for cardholder data storage and retention based on your business, legal, and/or regulatory requirements
- Securely delete cardholder data that exceeds your retention policies at least quarterly

Step 4

Protect Cardholder Data with Strong Cryptography During Transmission Over Public Networks

- Encrypt all in-transit cardholder data using strong cryptography and industry-accepted ciphers
- Maintain an inventory of all certificates and ciphers types used to protect cardholder data

Step 5

Protect All Systems Against Malware

- Employ antivirus and anti-malware software and ensure that logs are kept for at least three months online and one year offline
- Ensure software is regularly updated with the latest versions

Step 6

Deploy and Maintain Secure Systems and Applications

- Secure and keep your systems and applications patched and up-to-date
- Schedule regular maintenance and updates to your systems and applications
- Install critical vendor-supplied security patches for system components and software within one month of release
- Create and maintain applications in accordance with industry-accepted best-practices for secure software development
- For externally-facing sites, deploy and automated technical solution that continually detects and prevents web-based attacks

Step 7

Restrict Access to System Components and Cardholder Data by Business Need to Know

- Define strict roles designed to limit access to cardholder data and systems, document these roles in a formal access control policy

Step 8

Identify Users and Authenticate Access to System Components

- Use a unique user ID for each person that requires access to in-scope systems
- Use strong authentication methods and render all passwords/pass phrases unreadable during transmission and storage using strong cryptography
- Periodically review users and roles to ensure they are granted appropriate access
- Enforce multi-factor authentication for all CDE access

Step 9

Restrict Physical Access to Cardholder Data

- Restrict, monitor, and log all access to any physical facility that stores card holder data and systems
- Perform periodic inventories of physical locations of card holder data
- Where possible outsource physical security and systems hosting to PCI-compliant third parties

Step 10

Log and Monitor All Access to System Components and Cardholder Data

- Generate and securely maintain audit logs for all in-scope PCI components
- Deploy and automated process to review logs and security events for all system components daily to identify anomalies or suspicious activity

Step 11

Test Security of Systems and Networks Regularly

- Conduct internal and external network vulnerability tests at least quarterly and after any significant change to the cardholder data environment
- Create and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or change
- Implement network intrusion detection and/or intrusion prevention solutions
- Deploy a change detection mechanism to alert personnel of unauthorized modifications to critical systems and files

Step 12

Support Information Security with Organizational Policies and Programs

- Develop an information security policy for the company and distribute it to all employees
- Review the information security policy at least annually
- Implement a risk assessment program that is performed at least annually and upon significant changes to the environment
- Implement a formal security awareness program to train all employees on cardholder data security best practices
- Screen employees with access to cardholder data and systems prior to hire via background checks
- Create a formal program to monitor third party PCI DSS compliance status
- Develop an incident response plan and associated response procedures and test the plan at least annually