PBMares℠

CPAs and Consultants

PCI Security Standards Council®

QUALIFIED SECURITY ASSESSOR™

PCI DSS Compliance Services

A targeted route to PCI compliance — tailored for your budget and specific needs.

It's our mission to help companies strengthen cyber-resilience by mitigating the risk of cyber threats and PCI DSS non-compliance to protect your financial, operational, and legal well-being.

What Is PCI DSS Compliance?

All entities that store, process, and/or transmit cardholder data (CHD) must achieve and demonstrate data security compliance with the Payment Card Industry Data Security Standards, collectively referred to as PCI DSS. Additionally, merchants who accept or process payment cards must also comply with PCI DSS.

In our digital age, lax security can enable criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems. Minimizing financial fraud and improving transaction security strengthens trust between your organization and the customers you serve when accepting, processing, storing, and transmitting CHD.

In addition to protecting your business from losing customers, PCI DSS compliance also protects against brand erosion, litigation and financial penalties.

PCI DSS compliance involves:

- Adhering to protection of CHD
- Demonstrating compliance through periodic scanning and reporting
- Obtaining validation from a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV)

The exact PCI DSS compliance requirements vary based on the number of credit card transactions you process annually, as well as the specific requirements of the major payment card brands or acquirers. However, with more than 350 potential control requirements to address, demonstrating PCI DSS compliance can quickly become an onerous process.

PBMares PCI DSS Compliance Services

As an authorized QSA, PBMares will help your organization achieve and demonstrate PCI DSS compliance under the current framework version 3.2.1. Our team can also help your organization transition from version 3.2.1 to version 4.0 and address emerging threats and technologies with innovative solutions.

With our team's expert guidance, strengthen your overall security posture, promote security as a continuous process, and tackle every one of your PCI DSS compliance needs:

ROCs

A PCI Report on Compliance (ROC) is issued by a QSA and provides details about your organization's security posture, environment, systems, and protection of cardholder data. The ROC is developed through an onsite assessment and evaluation of controls using a standardized template provided to all QSAs.

By engaging an authorized QSA, you receive best practice recommendations to properly represent your status on PCI compliance by closing compliance gaps and remediating identified deficiencies.

SAQs

Ideal for small merchants and service providers that are not required to submit a report on compliance, a PCI Self-Assessment Questionnaire (SAQ) is designed as a self-validation tool to assess security of CHD. There are nine types of SAQs. Which SAQ is right for your organization? The answer depends on how you accept payment cards.

There are two components to the SAQ. The first is filling out the set of questions within the SAQ, enabling you to understand how well your current security posture aligns with relevant PCI requirements. The second is obtaining an appropriate Attestation of Compliance that you are eligible to have performed by a QSA.

Even though a SAQ is a self-assessment, many organizations look to PBMares for expert guidance to ensure the assessment is conducted properly.

AOCs

The PCI Attestation of Compliance (AOC) reports your organization's PCI DSS compliance status and attests to the fact that you're using best practices to protect the security of CHD.

Just like the SAQ, there are several versions of the AOC. Which one is right for your organization depends on which SAQ was applicable. Our experienced team of professionals at PBMares can simplify this process for you and as an authorized QSA, release an AOC.

Penetration Testing

PCI DSS penetration testing is an assessment designed to identify and address vulnerabilities in network infrastructure and applications from outside and inside your network environment.

You can engage PBMares for penetration testing in any area — from cloud computing, firewalls, and web applications to mobile devices and network security. We'll make recommendations to address identified vulnerabilities using PCI compliance best practices.

Vulnerability Scanning

PCI DSS requires two independent vulnerability scanning methods — internal and external. The scans evaluate your network from different perspectives. PBMares can identify and address vulnerabilities and provide prioritized expert recommendations for managing and remediating those vulnerabilities through an authorized ASV.

Gap Analysis

A PCI DSS Gap Analysis is performed by a QSA and highlights discrepancies between your cardholder data environment (CDE) and the latest version of PCI DSS. The result is a detailed list of systems, networks, and applicable PCI DSS controls that require attention.

When PBMares performs this analysis for you, you'll have a concise snapshot of your PCI DSS compliance and a cost-effective and prioritized remediation plan. Plus, you will thoroughly understand your PCI DSS audit readiness and be able to proactively address any gaps or deficiencies.

Employee Education and Cybersecurity Training

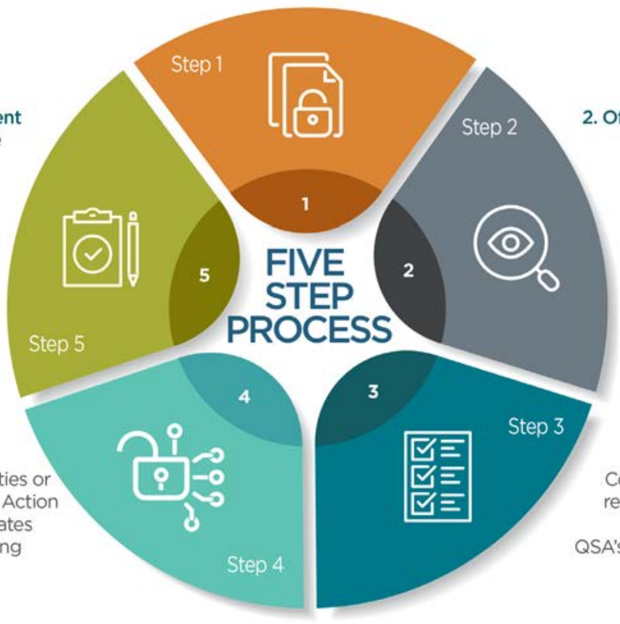
PBMares provides training to increase employee awareness of PCI DSS requirements, so employees can take appropriate action to protect your organization and your customers' cardholder data. Employees walk away with a clear understanding of best practices for identifying, addressing, and mitigating cybersecurity risks.

Our Process

ACHIEVING PCI DSS COMPLIANCE

PCI DSS compliance efforts follow yearly and quarterly cycles. Each cycle can be broken into a 5-step process.

1. Preparation
Determine PCI asset scope and PCI compliance level, complete applicable SAQ, conduct initial scanning for potential vulnerabilities, and fix any current violations.



2. Official Testing & Evaluation
Undergo third-party QSA assessment, such as RoCs, AoCs, or compliance scans.

3. Form Submission
Complete and submit the required forms along with the third-party QSA's validation documentation.

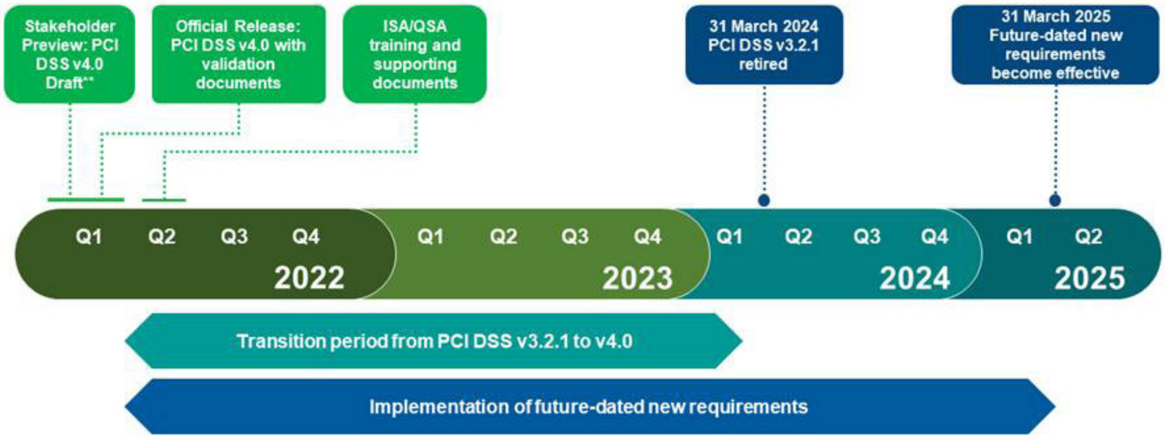
4. Remediation
Remediate any vulnerabilities or violations according to the Action Plans and completion dates specified in the reporting documentation.

5. Ongoing Management
Maintain compliance efforts between reporting periods.

PBMares Can Help You Transition to PCI DSS v4.0

On March 31, 2022, the PCI Security Standards Council released the long-awaited PCI DSS version 4.0, establishing a new baseline of technical and operational standards for protecting account data. PCI DSS version 4.0 replaces PCI DSS version 3.2.1 to better address emerging threats and technologies and provide innovative ways to combat new threats. As of March 31, 2024, version 3.2.1 will be retired and version 4.0 will be the only active version of the standard. The transition period is meant to allow organizations time to grasp the changes in version 4.0 and apply the necessary adjustments. PCI DSS version 3.2.1 will be operational for two years, with a transition period spanning March 31, 2022 to March 31, 2024. PBMares supports organizations in the transition to meeting PCI DSS version 4.0 compliance.

PCI DSS v4.0 Implementation Timeline*


Stakeholder Preview: PCI DSS v4.0 Draft**
Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025 Future-dated new requirements become effective
Q1 Q2 Q3 Q4 2022
Q1 Q2 Q3 Q4 2023
Q1 Q2 Q3 Q4 2024
Q1 Q2 2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

Source: PCISecurityStandards.org

Your PCI DSS Team

With experience advising leaders of large global organizations as well as smaller merchants and service providers, Antonina McAvoy leads the PBMares PCI DSS practice.

For more than a decade, we've been working with boards and upper management to prepare against high-profile cyber-attacks and shore up digital trust. At PBMares, it's our mission to help companies strengthen cyber-resilience by mitigating the risk of cyber threats and PCI DSS non-compliance to protect the financial, operational, and legal well-being of our clients.

How Much Will an Audit Cost?

No matter which PCI DSS compliance service you need, you're focused on keeping CHD safe while also managing a compliance budget. That's why our pricing is driven by the scope of the engagement.

Once we understand what services you need and which deliverables you're expecting, we'll scope your cyber environment. From there, we'll provide a fee estimate.

One thing to know about working with PBMares is that we keep overhead low and minimize scope creep. For you, this means fewer scope/fee expansions as well as fees that are commensurate with the significant value we deliver.

Contact me today to learn more about our pricing process and how our team can help.

Antonina K. McAvoy, CISA, CISM, QSA
Senior Manager, Cybersecurity & Control Risk Services Team Leader

(757) 355-6011
amcavoy@pbmares.com
www.pbmares.com

PBMares℠
CPAs and Consultants

About PBMares

As one of the largest accounting and consulting firms in the United States and a top 100 Accounting Firm as named by *Accounting Today,* PBMares brings a comprehensive approach to client engagements by providing a high level of expertise and experience in tax strategy, audit services, consulting, cybersecurity, investment banking and wealth management.

www.pbmares.com

OFFICE LOCATIONS

MARYLAND
Baltimore
Rockville

NORTH CAROLINA
Morehead City
New Bern

VIRGINIA
Fairfax
Fredericksburg
Harrisonburg
Newport News
Norfolk
Richmond
Warrenton
Williamsburg