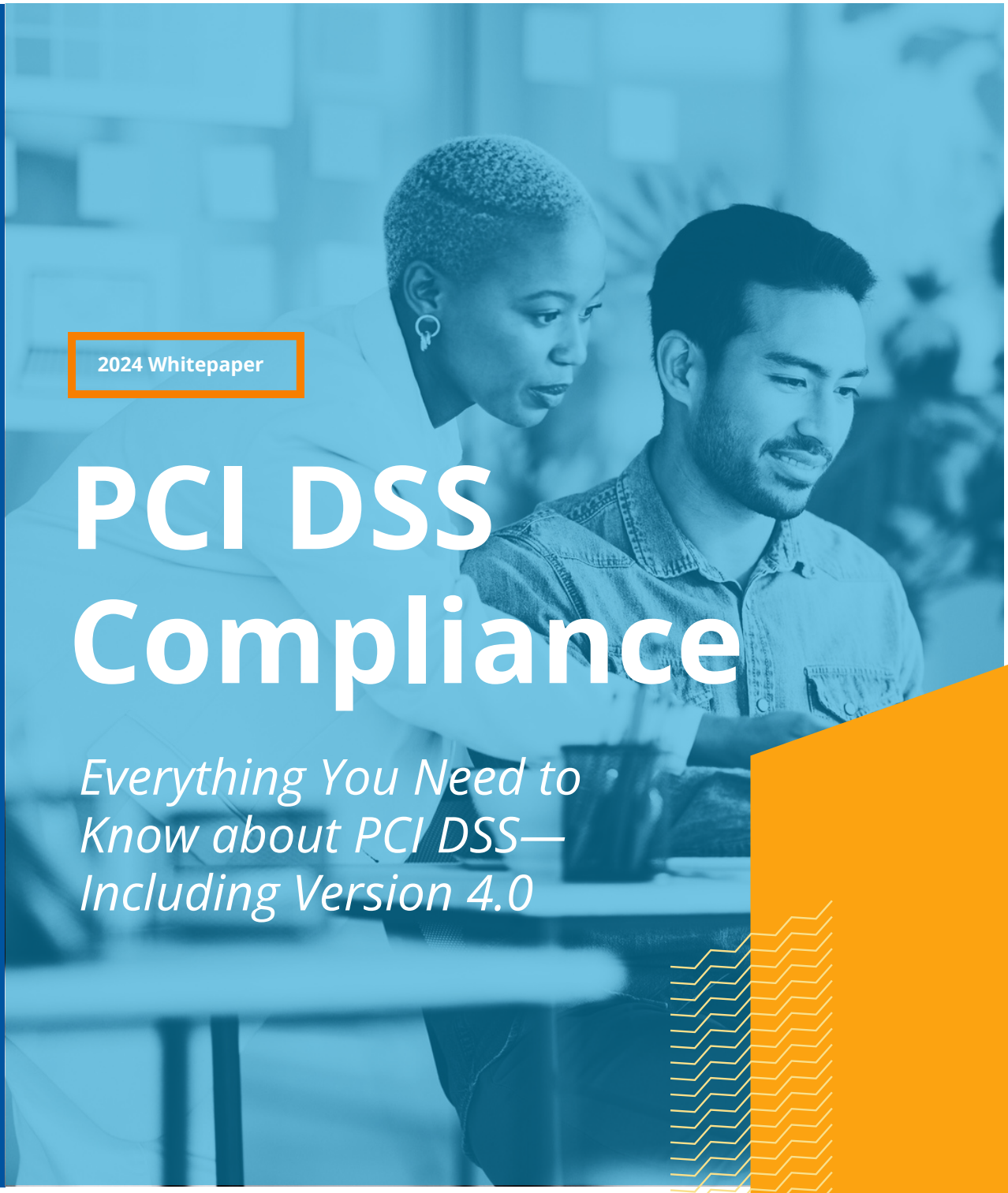
BARR ADVISORY

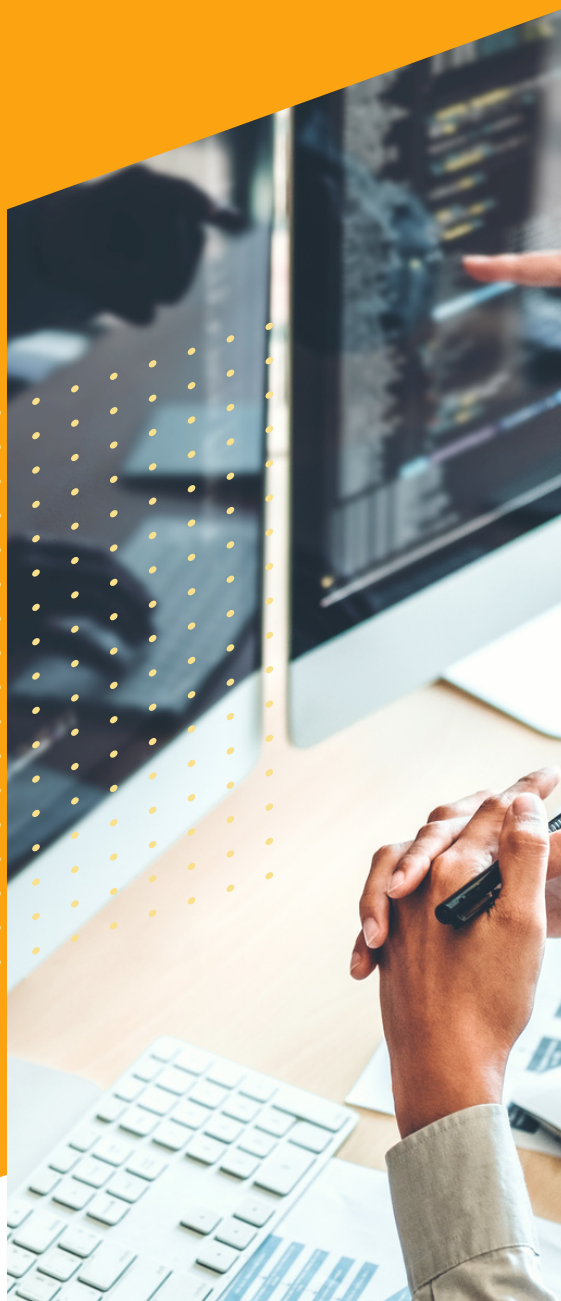


2024 Whitepaper

PCI DSS Compliance

Everything You Need to Know about PCI DSS—Including Version 4.0

Table of Contents



Introduction

In today's business world, it only takes the tap of a card or click of a button to process customer payments—and with any type of financial transaction lies the opportunity for cardholder data theft. No matter the size of your organization, if you store, process, or transmit credit card information, you'll want to comply with the Payment Card Industry Data Security Standard (PCI DSS) in order to avoid hefty fines and most importantly, keep your customer's data secure.

What is PCI DSS?

PCI DSS is a set of security standards established to safeguard payment card information and prevent unauthorized access. Developed by major credit card companies, including Visa, Mastercard, and American Express, the standard aims to create a secure environment for processing, storing, and transmitting cardholder data.

PCI DSS compliance involves three main components:

- Handling customer credit card data securely from start to finish. More specifically, making sure that sensitive card details are collected and transmitted appropriately.
- Storing data securely as outlined by the 12 security domains of the PCI DSS standard such as encryption, ongoing monitoring, and security testing of access to cardholder data.
- Validating that required security controls are in place on an annual basis. This can include security questionnaires, external vulnerability scanning services, and third-party audits.

"For organizations that process payment card transactions, PCI DSS is an essential piece of a holistic compliance program."

Cameron Kline, PCI Qualified Security Assessor (QSA)

Key Principles of PCI DSS

PCI DSS is a framework which serves as a baseline of protection for consumers.

Principles of PCI DSS

PCI DSS includes six major principles which can be further expanded to cover the 12 requirements.

Build and maintain a secure network:
- Installation and maintenance of a firewall to protect cardholder data.
- Configuration of system passwords and security parameters.

Protect cardholder data:
- Encryption of cardholder data during transmission and storage.
- Implementation of access controls to limit access to sensitive information.

Maintain a vulnerability management program:
- Regular updates of antivirus software and security systems.
- Development and maintenance of secure systems and applications.

Implement strong access control measures:
- Restriction of access to cardholder data to a need-to-know basis.
- Assignment of a unique ID to each person with computer access.

Regular monitoring and testing:
- Continuous monitoring and logging of all access to network resources.
- Regular testing of security systems and processes.

Maintain an information security policy:
- Development and enforcement of a comprehensive security policy.
- Regular education and training for employees on security best practices.

PCI DSS Merchant Levels

PCI DSS was established by the major credit card companies, Visa, Mastercard, Discover, American Express, and JCB. While each company originally established their own merchant levels, recently the brands made it easier to understand which level your organization falls under—no matter which card brands you accept. The general merchant levels are as follows:

- **Level 1:** Merchants processing over 6 million card transactions per year.
- **Level 2:** Merchants processing 1 to 6 million transactions per year.
- **Level 3:** Merchants handling 20,000 to 1 million transactions per year.
- **Level 4:** Merchants handling fewer than 20,000 transactions per year.

PCI DSS 4.0

In 2022, the framework released PCI DSS 4.0—updated from the previous version, PCI DSS 3.2. While the 12 primary PCI DSS requirements will continue to be the core foundation for securing cardholder data under the PCI DSS framework, these requirements have been updated, restructured, and new requirements have been added to offer guidance on how security controls should be used.

Version 4.0 was created by gathering feedback from over 200 organizations. The input from these organizations included the following themes:

- Ensuring the standard continues to meet the security needs of the payments industry;
- Promoting security as a continuous process;
- Enhancing validation methods and procedures; and,
- Adding flexibility and support of additional methodologies to achieve security.

Let's take a look at PCI DSS 4.0 and how the updated version can help your organization maintain a sustainable control environment and strengthen your security program.

Comparing PCI DSS 3.2 with 4.0—What's Changed?

While the 12 primary PCI DSS requirements from the 3.2 version will continue to be the core foundation for securing cardholder data under the PCI DSS framework, these requirements have been updated, restructured, and new requirements have been added to offer guidance on how security controls should be used. Major changes to the requirements include:

- Additional authentication controls, including strict multi-factor authentication (MFA) requirements when accessing the cardholder data environment;
- Updated password requirements, including increasing password length requirements from eight to 12 characters;
- Changing requirements around shared, group, and generic accounts;
- Clearly defined roles and responsibilities needed for each requirement; and,
- New requirements to prevent and detect threats against the payment industry, such as phishing, e-commerce, and skimming attacks.

PCI DSS 4.0

Take a look at some of the other changes from PCI DSS 3.2 to 4.0.

PCI DSS 3.2

- Primarily focuses on prescriptive security controls, offering detailed instructions on what organizations should do to remain compliant.
- Introduces MFA for personnel with non-console administrative access and all remote access to the cardholder data environment.
- Compliance is viewed from a point-in-time assessment.
- Addresses encrypted cardholder data but provides limited guidance on its management when the decryption keys are held separately.
- Outlines requirements for service provider responsibilities.
- Organizations must keep a list of weak or unacceptable cryptographic algorithms.

PCI DSS 4.0

- Emphasizes security outcomes, allowing businesses more flexibility in choosing the best security approaches for their environment.
- Expands on MFA by reinforcing the importance of secure authentication and recognizing the evolving landscape of authentication methods.
- Encourages continuous security and monitoring, highlighting that compliance is an ongoing process, not just an annual audit.
- Offers more precise guidance on managing encrypted data, emphasizing the importance of protecting it even if decryption capabilities are out of reach.
- Extends service provider responsibilities
- Urges organizations to maintain a documented description of the cryptographic architecture.

PCI DSS 4.0

Customized Implementation

Another significant change to PCI DSS is the implementation of a new, customized method for meeting requirements. This customized approach to PCI DSS provides organizations with the flexibility to meet the security objective requirements using new technology and innovative controls.

This change encourages organizations to adjust their implementation process in a way that fits their unique control environment. During a PCI DSS engagement, a third-party assessor will validate that the customized controls meet the PCI DSS requirements by reviewing an organization's unique documented approach and developing a procedure for validating the controls.

Transitioning from PCI DSS 3.2 to 4.0

Until March 31, 2024, PCI DSS 3.2 will remain active, and additional requirements will be considered best practice until March 31, 2025—meaning there's still time to transition to the 4.0 version.Organizations are not required to validate these new requirements. However, if your organization has implemented controls to meet PCI DSS 4.0, you're encouraged to have them assessed as soon as possible.

BARR associates also encourage you to review the changes in the official PCI DSS 4.0 document from the PCI Security Standards Council (SSC) to fully understand the changes and what steps you need to take to be prepared for and implement version 4.0.

Benefits of PCI DSS

- ✓ Build customer and stakeholder trust
- ✓ Achieve legal compliance
- ✓ Avoid financial loss and legal repercussions
- ✓ Maintain global acceptance

How to Prepare for Your Audit

Our QSA-certified team will walk you through each stage of the engagement process. Here are a few steps you can take ahead of time to ensure your assessment goes smoothly.

Understand Your CDE Segmentation

Understanding your CDE segmentation is often referred to as "requirement zero." To do this, it's helpful to maintain current network diagrams that reflect how data is transmitted, processed, and stored, which will help limit your scope prior to your engagement.

Understand Your Requirements

Are you a service provider or a merchant? Protect yourself from last-minute surprises by identifying any specific requirements that may apply to your organization.

Know Your Transaction Amount

Organizations are held accountable for the number of transactions handled annually. Prepare for your audit by having these numbers readily accessible.

> *At BARR, we're fueled by a passion to help organizations* ***build trust and achieve lasting cyber resilience.***
>
> *Kyle Helles, Partner, Attest Services Leader*

Simplify PCI DSS with BARR

BARR uses our four-phase PCI DSS proven process to help organizations prepare for and successfully achieve compliance seamlessly.

Phase 1: Planning

The planning phase of PCI DSS compliance helps BARR and your organization set expectations for your PCI engagement. After signing your engagement letter, your engagement team will partner with you to complete a scoping assessment, which determines your in-scope system components, determine the timing of your engagement and applicable travel plans, gain a better understanding of your organization's cardholder data environment (CDE), and create all necessary administration files and evidence request documents.

Phase 2: Assessment

At least three months prior to your PCI compliance report date, BARR will hold a kickoff meeting to finalize the engagement plans and ensure you're as prepared as possible. Your organization will then respond to evidence requests that are customized to your unique CDE through BARR's audit portal, and your engagement team conduct the testing and gathering process—including policy reviews, system evidence reviews, interviews, and observations.

Phase 3: Reporting

Depending on your organization's transaction amounts and customer requests, you can choose to perform a self-assessment questionnaire (SAQ) or a report of compliance (RoC). Your organization can complete an SAQ on your own, or you can have a QSA like BARR assist you with the process. If you choose to perform an RoC, BARR will draft the report along with an attestation of compliance (AoC), which will be submitted to the appropriate entities for official attestation. As your trusted partner and a certified QSA, BARR serves as an official reviewer of these reports—and will give you the opportunity to review them—prior to receiving your final deliverable. Depending on the complexity of your CDE, achieving an RoC will take **three to six months** to complete.

Phase 4: Issuance, Debrief, Celebrate

Once your report is issued and your audit is archived, BARR will debrief with your organization, communicating process improvement opportunities (PIOs), action items for continuous management, and a pre-plan for your next engagement. Organizations should conduct PCI DSS engagements at least annually and continuously consider your customers and vendors' requests to determine the appropriate cadence for achieving PCI DSS compliance. BARR will help you celebrate and optimize your accomplishment, ensuring your organization is prepared to achieve future security and compliance goals.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about completing a PCI DSS Assessment with BARR? Contact us today.