PKWARE

pkware.com

What's Next After Achieving PCI DSS Compliance

Building a Sustainable Strategy

2021

Contents

What is PCI DSS?

First launched in September 2006, the Payment Card Industry Data Security Standard (PCI DSS) has become the leading set of security standards for maintaining a secure environment for all companies—regardless of size or number of transactions—that accept, process, store, or transmit credit card information. PCI DSS is administered and managed by the Payment Card Industry Security Standards Council, an independent body created by major payment card brands Visa, MasterCard, American Express, Discover, and JCB.

Compliance within PCI DSS is comprised of four distinct levels with varying degrees of validation requirements. Merchants are assigned a level based specifically on their volume of payment card transactions over a 12-month span. If at any time, a merchant suffers a breach resulting in compromised account data, they may find themselves moved to a higher level with stricter validation requirements.

> "PCI compliance is the beginning of security, not the end."

Merchant Level	Criteria	Validation Requirements
1	■ 6M+ payment card transactions per year ■ Any merchant that Visa or Mastercard determines should meet Level 1 requirements to minimize risk to the system	■ Annual Report on Compliance by Qualified Security Assessor or Internal Security Assessor ■ Quarterly network scan by Approved Scan Vendor ■ Attestation of Compliance form
2	■ 1 – 6M payment card transactions per year	■ Self-Assessment Questionnaire ■ Quarterly network scans by Approved Scanning Vendor ■ Attestation of Compliance form ■ Quarterly PCI scan may be required
3	■ 20,000 – 1M ecommerce transactions per year	■ Self-Assessment Questionnaire ■ Quarterly network scans by Approved Scanning Vendor ■ Attestation of Compliance form
4	■ >20,000 ecommerce transactions per year or all merchants processing up to 1M payment card transactions per year	■ Self-Assessment Questionnaire ■ Quarterly network scans by Approved Scanning Vendor

Any organization that accepts credit, debit, or pre-paid cards under the American Express, Discover, MasterCard, Visa, and Discover brands must maintain PCI DSS compliance. Those who do not store card data may find that compliance is easier to achieve, due to the inherent risks of storing sensitive data. Conversely, those who do need to store data—such as for recurring billing—will find the self-assessment bar set very high, and they may need a Qualified Security Assessor (QSA) to run an audit and verify all the necessary controls are in place for meeting PCI DSS specifications regardless of their merchant level.

The ongoing pursuit of PCI compliance is supported by annual assessments. These annual assessments are a required component for every Merchant Level of PCI compliance, and for good reason: One study found that only about a third of companies are still compliant one year after their initial validation. Non-compliant merchants run a higher risk of breach, audit, fines, and damage to brand reputation.

It may be noted, then, that PCI compliance is the beginning of security, not the end.

The Benefits of Reducing the Scope in PCI DSS Audits

PCI DSS compliance audits will examine an organization's systems and cardholder data environments to identify vulnerabilities with the overarching goal of preventing data from being compromised. Audits are also valuable to organizations that have already suffered a data breach, as they will include a roadmap that can help avoid future incidence.

A QSA will begin by examining the business' security infrastructure, including policies, procedures, networks, and systems. Audited environments may include any device, component, network, or application that stores, processes, or transmits cardholder data. Following the examination, the company will receive a risk assessment that includes the foundation for improving data security.

Improving data security standards can reduce the scope (what is being assessed) of the overall audit, but it's also possible to reduce the scope prior to the audit, saving money and making PCI compliance assessments easier and less painful.

Organizations can help reduce the scope of audit by applying redaction (irreversible data protection), masking (reversible data protection), and/or encryption (reversible data protection) to cardholder data. Not only does this protect the data and meet PCI DSS standards, it also ensures data is protected before it hits any machine inside or outside of the organization, thereby removing it from the audit scope.

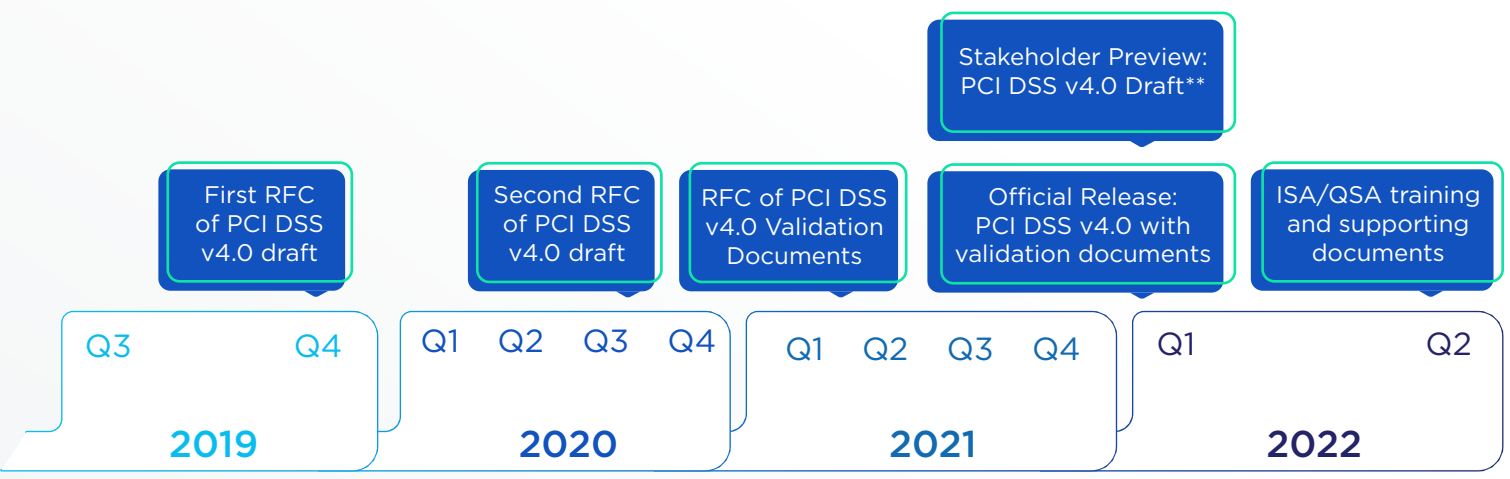
Changing with the Times: PCI DSS 4.0

The long-awaited Payment Card Industry Data Security Standards (PCI DSS) version 4.0 is the first major change to PCI DSS since the end of 2013. With how rapidly technology progresses, the PCI DSS standards also needed to change in order to keep up with the rapidly evolving payment ecosystem. This latest 4.0 update is expected to release in early 2022. The current mandate, PCI DSS 3.2.1, is projected to be retired in Q1 of 2024, at which point version 4.0 will become the mandatory standard.

Experts agree that version 4.0 is expected to require far more stringent security on the part of credit card processing organizations, while allowing greater discretion and freedom as to how implementations for meeting these stricter expectations can be customized.

The overall intent of PCI DSS has always been to protect cardholder payment data and, once 4.0 is effective, to better secure modern data technology—including cloud environments. Version 4.0 is also positioned to more forcefully mitigate against rampant data breaches that have been consistently compromising card holder private and personal data.

PCI DSS v4.0 Development Timeline*



Review and Incorporate RFC Feedback

***All dates based on current projections and subject to change**

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

Key Priorities and Goals for PCI DSS v4.0

The goals of PCI DSS version 4.0 include a focus on persistent, end-to-end personal data protection for processing payments in modern data environments. According to the PCI Security Standards Council, "PCI DSS is being updated to address stakeholder feedback and to support a range of environments, technologies, and methodologies for achieving security."

Some things about PCI DSS are not changing. This includes the 12 core categories of requirements, which are likely to remain the same in PCI DSS 4.0 as they are in version 3.2.1.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	■ Install and maintain a firewall configuration to protect cardholder data ■ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	■ Protect stored cardholder data ■ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	■ Use and regularly update anti-virus software or programs ■ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	■ Restrict access to cardholder data by business need-to-know ■ Assign a unique ID to each person with computer access ■ Restrict physical access to cardholder data

Goals	PCI DSS Requirements
Regularly Monitor and Test Networks	■ Track and monitor all access to network resources and cardholder data ■ Regularly test security systems and processes
Maintain an Information Security Policy	■ Maintain a policy that addresses information security for employees and contractors

The PCI Security Standards Council (SSC) continually evaluates how the payments industry operates and searches for ways to improve it. Businesses are constantly challenged to manage the development, storage, dissemination, and security of cardholder data. Thus, PCI SSC works on new updates—such as version 4.0—to help businesses improve their practice in those areas and increase data security.

Flexibility and enhanced security are key to the most recent updates in PCI DSS 4.0:

- Reinforcing security as a continuous process addresses evolving risks and threats to payment data
- Requirements and validation options are redesigned to focus on security objectives to support organizations using different and custom methodologies to meet the intent of PCI DSS requirements

PCI DSS 4.0 is also anticipated to provide new guidance and considerations for specific newer technologies—modern cloud data environments and intelligent, AI-assisted encryption—via an Appendix to 4.0 clarifying the roles and expectations for cloud providers.

Four overarching security objectives represent a palpable shift in data security focus of 4.0:

1. Ensure the standard continues to meet the security needs of the payments industry
2. Add flexibility and support of additional methodologies to achieve security
3. Promote security as a continuous process
4. Enhance validation methods and procedures

Combined with the new customized validation approach, companies will now have more flexibility in not only modifying implementation features, but also in meeting requirement intent. Those who choose to follow a customized implementation must document that the intent of the requirement is met. External assessors will verify the effectiveness of custom implementations both by reviewing associated documentation and testing each control.

Three Steps to Adhering to PCI DSS

Becoming compliant with PCI DSS can be a complicated journey, and leveraging the assistance of an external consultant or third-party auditor is a wise move. Whether you have the internal resources to run your adherence campaign, or leverage outside expertise, the journey to PCI DSS compliance can be boiled down to three steps:

1. **Assess:** Perform an audit to identify the cardholder data the organization is responsible for, inventory IT assets and business processes involved in payment card processing and analyze for vulnerabilities.

2. **Remediate:** Fix any vulnerabilities uncovered in the assessment stage. If the organization is storing unnecessary cardholder data, take steps to properly dispose of it. For businesses that need to retain cardholder data, consider leveraging an external qualified body for storage, or investigate proper remediation techniques, such as redaction and/or encryption.

3. **Report:** Assemble and submit any applicable require remediation records and compliance reports.

Building Ongoing Compliance Capabilities

As stated earlier, PCI DSS compliance is the beginning of security, not the end. Compliance must be an ongoing endeavor; focusing solely on the annual assessment may create a false sense of security. It's important then to stay on top of compliance efforts, even leveraging consultants to run quarterly scans so nothing surprising is found during your annual review.

Automated compliance solutions can play a crucial part in maintaining compliance both for and between annual reviews. Simplified compliance and reporting is a must for keeping business moving at the speed of buyers.

Here are some top considerations to keep in mind when considering building out an automated PCI DSS compliance setup:

Flexibility

PCI DSS guidelines specifically outline requirements for security controls. Compensating controls are currently only allowed as exceptions when the rigid requirements are proven to be impractical. However, the upcoming version 4.0 will allow customized validation that is effective for the business, markets, and customers. Customized implementations must be designed to meet the intent behind PCI DSS 4.0 Security Controls. All customized implementations will need to be approved by a QSA.

The Council and standards recognize that companies often may arrive at solutions and implementations that are new, innovative, or unique, and achieve all the intent of the objective using their own security controls. Now these same organizations are provided the flexibility to design and execute on a custom set of effective capabilities and controls that fit the business while protecting cardholders' personal data.

Security

PCI DSS continues to set a high bar for strong security standards: Cardholder data must be protected whether it is stored as structured, unstructured, or semi-structured data across the enterprise, from databases to endpoints.

While the safe, secure processing, transmission, and storage of cardholder private data remains the overarching purpose of PCI DSS standards, even stronger requirements and security standards will likely be in place when version 4.0 is released. Included in the stricter requirements are approaches to securing cloud-based data and serverless workloads.

Encryption

The earlier and more broadly organizations can discover and encrypt personal data, the stronger their security becomes. According to PCI requirements 3.4 and 3.2, stored Primary Account Numbers (PAN) must be rendered unreadable. Organizations must protect cardholder data during transfer and storage, both while data is at rest and in motion.

Version 4.0 aims to expand security with best practices and insight on fully protecting network transmissions. Encryption will thus hold a broader applicability on trusted networks.

Monitoring

Technology continues to grow rapidly, and with it, more opportunity for security threats if not properly addressed. Early feedback for version 4.0 included a desire for monitoring requirements to consider technology advancements. Pluggable options for information systems will help organizations comply with faster deployment.

Authentication

The latest version of PCI DSS includes a sharper focus on NIST multifactor authentication (MFA)/Password Guidance, with stronger authentication standards to logins for accessing payment and control processes. This is another opportunity for organizations to customize their compliance with regulatory requirements through unique pluggable authentication standards.

MFA will become a standard requirement for cardholder processing.

DESV Requirements

Designated Entities are determined by an Acquirer or Payment Brand, and are organizations that require additional validation to existing PCI DSS requirements. If your organization has been designated as such, you will be subject to additional validation procedures along with increased validation and scoping considerations. These are known as a Designated Entities Supplemental Validation (DESV).

While DESV is not required for non-Designated Entities, all organizations should consider following DESV as a best practice. There is also a strong possibility that version 4.0 will make DESV a mandated compliance requirement for all organizations.

Update Discovery and Protection for PCI DSS Compliance Validation with PKWARE

No matter what PCI DSS 4.0 merchant level your business falls under, if you don't know where all your cardholder and other sensitive data is across the enterprise, you cannot confirm compliance during a QSA's assessment for Compliance Level 1, nor in the Self-Assessment Questionnaire (SAQ) used by Levels 2 – 4.

With PK Discovery, part of the PK Protect suite of data protection and security products, you can automatically dig deep to find every place that cardholder data is stored, whether that's a file system, database, cloud repository, or even endpoint device like laptop or mobile. This exhaustive inventory makes it easier for a QSA to determine or an SAQ to prove maintained compliance.

Aligning with both the current version 3.2.1 and the upcoming 4.0 involves multiple requirements for storing and using data. PK Encryption, another segment of the PK Protect suite, includes multiple options for precise data protection to promote meeting PCI requirements while maximizing the business value of IT assets. Encryption options include file, email, element-level, format preserving, and transparent data encryption with all operations audited to a central location to ensure and prove compliance.

Often, organizations need to remove sensitive information from data while still preserving the value of the original data. PK Masking provides the ideal solution for this data protection demand. Extensive data masking protection options include character-level, custom value, format preserving, redaction, and more, along with customizable options for unique use cases. Control sensitive data with consistent masking across multiple and even disparate data stores. PK Masking can create production-quality DBMS copies so that entire data sets can be leveraged for accurate and meaningful insight without compromising sensitive information. And, with no linkage between original and masked data, there remains no possibility of retrieving the original data from masked values.

By applying persistent data-level protection to PCI data, PKWARE's automated data redaction technology can remove credit card numbers and other sensitive data from files and emails, leaving other contents unchanged. This redaction takes the files out of scope for PCI requirements, ensuring that cardholder data will not be exposed in the event of theft or breach. Bear in mind that it's up to every individual QSA to determine what is in or out of scope, additional technology notwithstanding. PK Protect is accurate in reducing the scope, though some QSAs may still ultimately decide to require additional information.

PK Protect also upholds established validation policies related to which users in what roles can access or process any sensitive personal cardholder data, including supply chain, reseller, and third-party data processors. It can be set to automatically mask sensitive information—such as PANs—in production data sets to safely leverage data for non-production applications such as testing and development. Least privilege access is gained when masked and unmasked data sets are designated to different users. To preserve user workflows and business value of data, users with masked data sets can take advantage of PK Masking's robust masking feature sets to create realistic-looking data sets.

Preparing for PCI DSS starts with being in compliance with the most current version, 3.2.1, then planning for the changes necessary to adapt to new requirements and security testing. PK Protect has proven reliable for PCI DSS compliance and scope reduction year after year by hundreds of global Fortune 1000 companies and organizations.

Establish control of your cardholders' data now and be well positioned to execute on PCI DSS with the help of PKWARE.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

Enterprise Wide Policy Management

The PKWARE Enterprise Manager provide a single point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification and Protection

No other solution has the capability to find, classify and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204