WHAT TO KNOW ABOUT PCI DSS V4.0

QUICK REFERENCE GUIDE

OVERVIEW

The Payment Card Industry Data Security Standard (**PCI DSS**) is a set of requirements to ensure that entities properly process, transmit, and store credit card data to maintain a secure environment.

Launched in 2006, PCI DSS is **widely** considered the foundational standard for credit card vendor security, and adherence to these practices is required by all major credit card brands.

PCI DSS contains **twelve requirements** for compliance, each with detailed subcomponents.

PCI DSS standards have **evolved** over time with **periodic updates**. The current operational standard is **v3.2.1**, created in 2018.

In March 2022, PCI DSS **v4.0** was released. Companies can **choose** to comply with v4.0 **immediately**. However, compliance with all v4.0 requirements will not be **mandatory** until **2025**.

As an accredited **Qualified Security Assessor Company** (QSAC) authorized to perform PCI DSS Assessments under v4.0, VENZA can provide a **full suite** of compliance products that have been proven effective for thousands of hospitality organizations.

CONTENT CHANGES

Version 4.0 is a significant change from PCI DSS v3.2.1. It adds dozens of clarifications, additional guidance, and restructuring of content for additional clarity. Importantly, it also adds 64 new requirements.

Ensuring that you are prepared for v4.0 **requires consultation with an expert QSA**. VENZA's Security Team is prepared to assist you with that process.

For **informational purposes**, a few key content changes should be highlighted:

MFA

Requirements for use of multi-factor authentication (MFA) are significantly expanded. MFA will be required for any and all access to the cardholder data environment (CDE).

This may impact prior procedures:

- **Users** – v4.0 mandates that MFA must be used for all users to access the CDE, not just administrators.
- **Location** – the current MFA requirement is for remote, non-console access. This will be expanded to on-site console access as well
- **Each Attempt** – previously, MFA was required only once for remote users to connect to the CDE through a VPN. Now, MFA will be required for every attempt to access the CDE. This means MFA may be required multiple times during remote access (e.g., once when connecting to a network and again when accessing the CDE within the network).

Changes to MFA procedure are currently designed as recommended best practices and will become mandatory requirements in March 2025.

CUSTOMIZED APPROACH

PCI DSS v4.0 adds an additional alternative for merchants and service providers who cannot meet prescriptive controls.

In addition to the previously existing "compensating control" method included in 3.2.1, v4.0 allows a merchant or service provider to document a different control to achieve the objective of the control being customized. This will then be assessed in place of the control that is being substituted. A customized approach does not replace the current compensating controls.

YEARLY DILIGENCE

v4.0 adds new controls for periodic diligence of merchants and service providers. This includes:

- Documenting the in-scope CDE at least every twelve months and upon significant change
- Targeted risk analysis for customized controls at least every twelve months
- Risk analysis for controls that have flexibility for frequency at least every twelve months
- Review of cipher suites and protocols and hardware and software technologies in use at least every twelve months

OTHER CHANGES

v4.0 also contains other changes worth noting:

- **Encryption** – disk-level or partition-level encryption will no longer be acceptable for rendering PAN unreadable
- **Cryptographic Inventories** – an inventory of trusted keys and certificates to protect Primary Account Number (PAN) data during transmission must be maintained
- **Firewalls** – vulnerability scans are no longer an acceptable alternative to web application firewalls for public-facing applications
- **Scanning** – internal vulnerability scans must be performed via authenticated scans

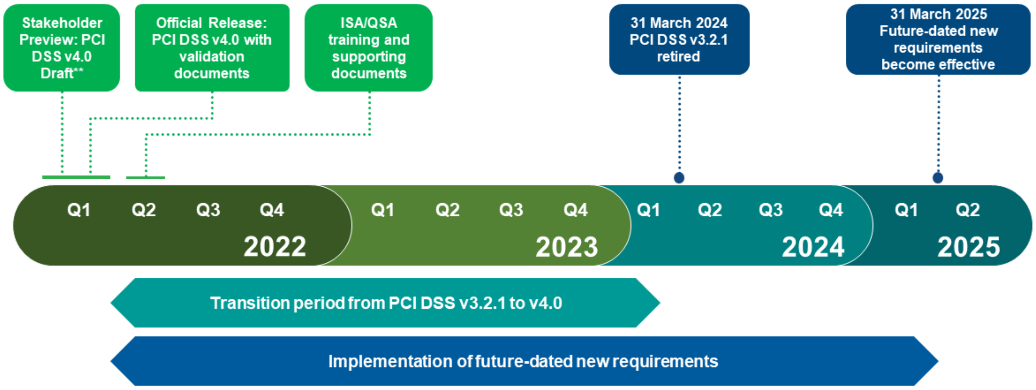
TIMELINE

Compliance with PCI DSS v4.0 is not required immediately. While the PCI Security Standards Council recommends that organizations capable of complying with the new requirements do so now, the implementation of v4.0 occurs in phases with built-in time to adjust systems, processes, and documentation.

There are two main phases to be aware of:

1. **Retirement of v3.2.1** – March 2024. After this date, only v4.0 will be effective. Practically, this means that 13 new requirements included in v4.0 will be immediately mandatory for PCI DSS assessments.

2. **Future-dated requirement deadline** – March 2025. The remaining 51 new requirements become mandatory. After this date, all PCI DSS v4.0 standards must be complied with.


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

(Source: PCI DSS)

ABOUT VENZA

VENZA is a leading provider of security awareness data protection solutions that empower the hospitality industry to mitigate vulnerabilities and ensure compliance. VENZA supports over 2000 hotels globally, keeping guests and their data safe from breaches with 360-degree visibility for proactive management of risks. This allows property managers to focus on guest service and building trust in their brand.

Visit www.VENZAGroup.com or www.CyberTekMSSP.com for additional details.

Contact:

Sales: sales@venzagroup.com

Customer Success: success@venzagroup.com

Disclaimer: In no event shall VENZA Inc. or its subsidiaries be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, consequential, incidental, indirect, economic, or punitive damages, business interruption, loss of business information, or other pecuniary loss) arising out of the use of this document, even if advised of the possibility of such damages.