FORTRA™

# Five-Step PCI DSS v4.0 Transition Checklist

## An Essential Guide for the Updated PCI Requirements

## Setting the Stage for PCI DSS v4.0

The Payment Card Industry Data Security Standard (PCI DSS) underwent its last update in 2018, and, as we all know, the world has changed a lot since then. The pandemic created an e-commerce boom, ushering in a 43 percent increase in online payments according to U.S. Census data, representing an additional $244.2 billion in e-commerce in 2020 alone.[1]

This spurred the need for an updated set of PCI DSS requirements, which were released in March 2022 and will become mandatory for all organizations that process or store cardholder data in March 2024.

The proliferation of online transactions isn't the only reason the PCI Council created the v4.0 standard. Recent years have also seen a surge in cloud use, the rise of contactless payments, and cybercriminals using increasingly sophisticated methods of intrusion and fraud.

**GOOD TO KNOW**

In addition to an 18-month period when v3.2.1 and v4.0 will both be active, there will be an extra period of time defined for phasing in new requirements that are identified as "future-dated" in v4.0.

## Goals of the Shift from PCI v3.2.1 to v4.0

Since its inception in 2004, PCI DSS has been continuously updated to keep pace with the evolution of cyberthreats and the growing complexity of the technology landscape. Currently, organizations need to mitigate threats posed by emerging attack vectors while proving compliance in increasingly heterogeneous IT environments.

**These are the fundamental goals of this latest update after gathering feedback from more than 200 organizations, according to the PCI Council.[2]**

- **Continue to meet the security needs of the payment industry, for example:**
  - Expanded multi-factor authentication requirements
  - Updated password requirements
  - New e-commerce and phishing requirements to address ongoing threats
- **Promote security as a continuous process, for example:**
  - Clearly assigned roles and responsibilities for each requirement
  - Added guidance to help people better understand how to implement and maintain security
  - New reporting option to highlight areas for improvement and provide more transparency for report reviewers
- **Add flexibility for different methodologies, for example:**
  - Allowance of group, shared, and generic accounts
  - Targeted risk analyses empower organizations to establish frequencies for performing certain activities
  - Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives
- **Enhance validation methods, for example:**
  - Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance

### WHAT CHANGED IN THE v4.0 REQUIREMENTS?

A high-level overview of requirement changes from PCI v3.2.1 to PCI v4.0:

- **Requirement 2:** Broader scope defining the need for security configuration management (SCM) on more types of assets.
- **Requirement 3:** "Account Data" instead of "Cardholder Data" indicates a potential increase of scope for PCI assets.
- **Requirement 4:** Less specificity on the type of encryption used means your organization is freer to follow industry best practices. An important takeaway is to internally define what those technical standards are and be able to justify why they are now "Strong Cryptography" so that you can still pass your PCI audit (essentially, just document what standards you are following and why).
- **Requirement 5:** It is no longer sufficient to just have standard antivirus software, as this requirement now specifically calls for anti-malware to be in place—necessitating a strong antivirus solution with malware protection or EDR/MDR/XDR solution.
- **Requirements 7–9:** These requirements are primarily the same as before, but the big takeaway is that instead of just enforcing access controls to systems, it's now being requested that it's done more granularly to specific components such as software, databases, etc.

## Your Five-Step Transition Checklist

Guiding your organization toward complete PCI DSS v4.0 compliance isn't a one-time effort—making the transition efficiently and effectively will require a phased approach. In addition to adopting new technical procedures, this new PCI release also calls for a shift in culture: Helping your organization view compliance as a security measure and fostering a security mindset among your teams is going to make a positive impact and help with PCI best practice alignment.

Follow these five steps to ensure you are leading your organization down the correct path for complete PCI v4.0 adherence in the necessary time frame. Using this checklist will help you avoid audit fines and help keep your organization's name out of data breach headlines.

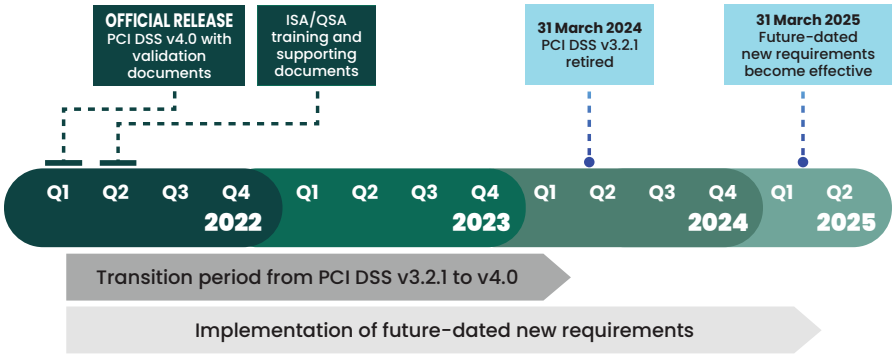
### 1. Plan a Phased Implementation According to the PCI Timeline

As you know, the updated PCI DSS v4.0 release is already available—but it doesn't become mandatory until March 2024. Use this time cushion to create an action plan broken down into distinct phases and save your teams from a last-minute scramble to the finish line.

This isn't the end of the road, however, as there are additional steps to be taken by March 2025 as well. PCI has allotted an additional year from the time v4.0 becomes mandatory for the adoption of additional best practice requirements.

Compliance is meant to be an ongoing process rather than a point-in-time project, so documenting a phased implementation approach will set your organization up for greater audit success and tighter security.

### Implementation Timeline




PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed.[3]

## 2. Review Potential Changes to Scope

The expansion of Requirement 3 now encompasses the protection of account data as opposed to the previous cardholder data. What does this mean for the scope of your compliance operations? The broader category of account data equates to a significant growth in scope.

For example, an email system that wasn't previously beholden to PCI may become in-scope for v4.0. It may be necessary to restructure your network to adequately protect account data. There is a strong budgetary consideration here if your organization needs to expand its PCI compliance program to adhere to this revised standard.

## 3. Conduct a People and Processes Evaluation

One of the major changes to consider in v4.0 is the emphasis on cultivating a security mindset within the organization. Approaching compliance as a box to check with the completion of technical processes misses the point—the true intention of the payment card industry standard is security, after all.

Teams must begin to view compliance as a continuous activity that protects sensitive data more so than simply a set of tasks designed to pass audits. What does this look like from a functional standpoint? Have your security and compliance teams work together to implement a defined process for maintaining security of the cardholder data environment (CDE), including routine reviews of configurations and security reviews.

When you have documentation of a process, a group of internal reviewers, and a steady cadence, your organization checks the compliance box while simultaneously ensuring a high level of security.

## 4. Strengthen SCM Processes

Requirement 2 broadens the scope of security configuration management. Rather than focusing on vendor-defined defaults, the onus is now put on organizations to have their own security configuration program. In order to meet v4.0's wider SCM scope, ensure that your team is monitoring the configurations of networks, servers, firewalls, and all other components.

In addition to hardening your attack surface against intrusion, SCM also helps auditors track compliance status (improvements and setbacks) over time. Configuration security is so crucial that almost all industry standards and regulations incorporate some version of an SCM mandate for specifying how configurations should be set up. SCM tools help you substantially reduce the time it takes to prepare for an audit and speed up the actual audit process as well.

## 5. Onboard a Tool That Automates Continuous Compliance

The simplest way to achieve continuous v4.0 compliance is to deploy a solution that continuously monitors for configuration drift that takes assets out of compliance. Like most of the security industry, the PCI Security Standards Council is following the approach that compliance is something that must be proven every day—this is an attainable goal.

Solutions that combine SCM with file integrity monitoring (FIM) can help your organization to meet the v4.0 standard well before the deadline. Whether your needs are to comply with Requirement 11 using FIM, or to expand configuration monitoring throughout your environment, Tripwire can help.

## How to Streamline PCI v4.0 Compliance with Tripwire

Fortra's Tripwire® Enterprise alerts you to misconfigurations as soon as they occur (real-time) with comprehensive FIM and SCM. As the founders of FIM, Tripwire has stayed the gold standard for Requirement 11.5's change detection mandate since the creation of the first PCI standards.

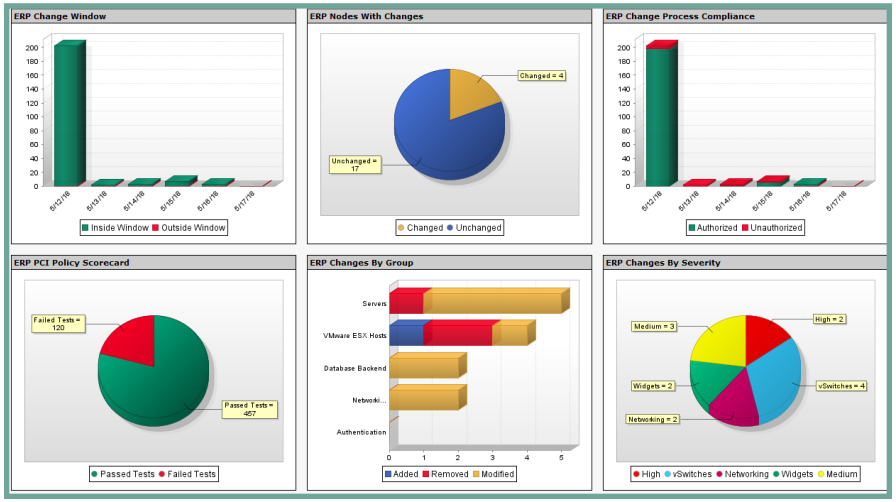
How does it work? Tripwire Enterprise measures the observed state against the hardened, compliant state as described by PCI DSS. And it doesn't just let you know you've failed a policy test: Its granular, step-by-step remediation instructions help you get back in compliance fast.

When it comes time to supply your auditor with documentation, your teams can pull reports from any point in time to demonstrate your configurations' alignment with PCI (along with many other compliance standards). Tripwire has the largest and broadest library of supported policies, with over 4,000 policy and platform combinations covering the widest range of OS versions and devices.

**SCHEDULE A DEMO TODAY**

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit www.tripwire.com/demo

## Tripwire Enterprise Change and Compliance Dashboard




Tripwire Enterprise's customizable dashboards provide at-a-glance confirmation of your infrastructure's change and compliance status. When integrated with user homepages, these dashboards allow each user of the system to have a customized display that provides high-level compliance information, fine-grained views of systems or elements, or any level in between.

## Sources

1 https://www.census.gov/library/stories/2022/04/ecommerce-sales-surged-during-pandemic.html#:~:text=According%20to%20the%20most%20recent,to%20%24815.4%20billion%20in%202020
2 https://blog.pcisecuritystandards.org/at-a-glance-pci-dss-v4-0
3 Ibid

FORTRA™

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.



tw-gd-0723-r1-hm