FORTRA™

5-Step PCI DSS 4.0 Transition Checklist

Setting the Stage for PCI DSS 4.0

The Payment Card Industry Data Security Standard (PCI DSS) has evolved significantly in response to the rapid digital transformation of recent years. Since its last major update in 2018, the landscape of payments has shifted dramatically. The COVID-19 pandemic fueled a surge in e-commerce, with U.S. Census data showing a 43% jump in online payments and an additional $244.2 billion in e-commerce sales in 2020 alone.[1]

To address the security challenges brought on by this growth, PCI DSS v4.0 was released in March 2022. But the update wasn't driven by e-commerce trends alone. The widespread adoption of cloud technologies, the mainstreaming of contactless payments, and the escalation of sophisticated cyberattacks have all underscored the need for a more flexible, modernized, and resilient approach to payment security.

As of March 31, 2025, PCI DSS 4.0 compliance is no longer optional — it's a requirement for every organization that processes or stores cardholder data. Is your organization fully compliant, or is it still navigating the path to get there? This guide delivers insights and tips to help you meet the new standard with confidence.

Goals of the Shift from PCI 3.2.1 to 4.0

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:

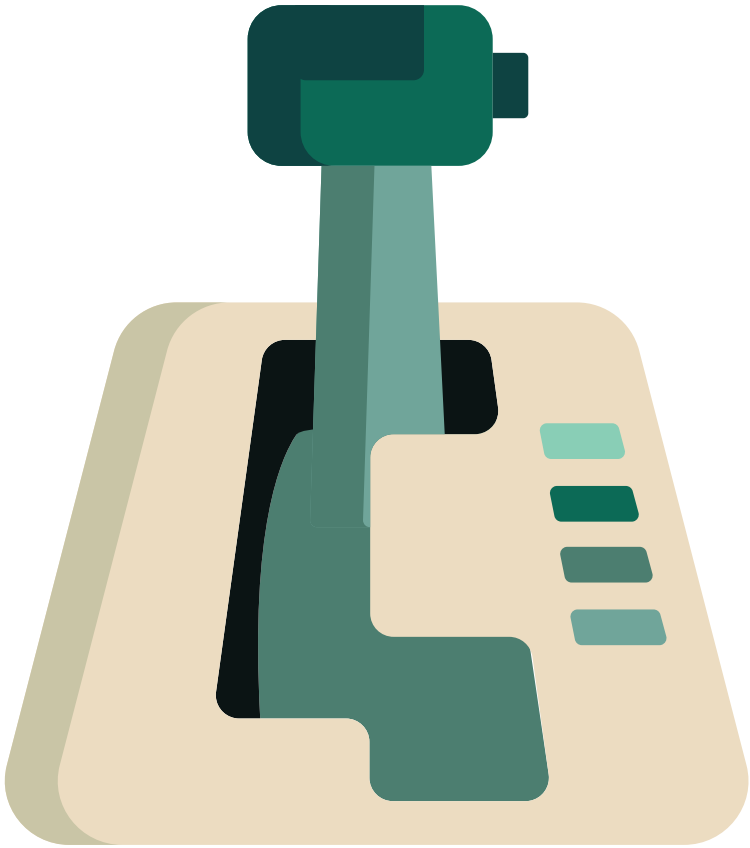
- Clearly assigned roles and responsibilities for each requirement
- Added guidance to help people better understand how to implement and maintain security
- New reporting option to highlight areas for improvement and provide more transparency for report reviewers

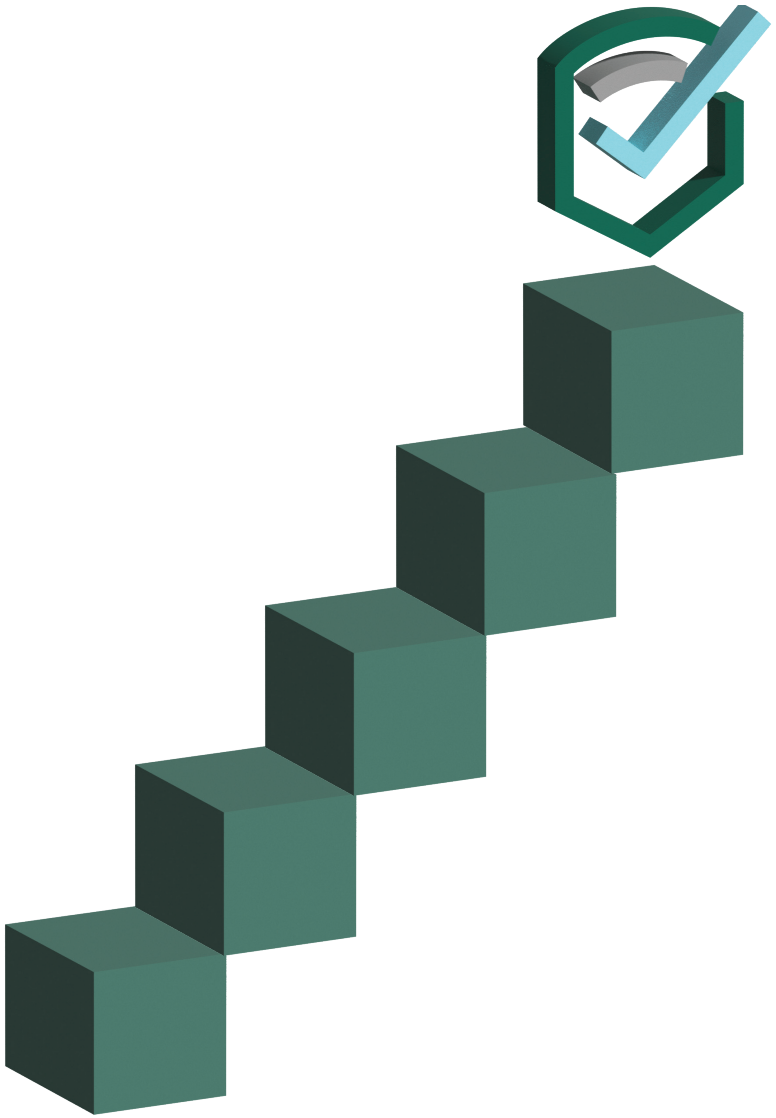
Add flexibility for different methodologies, for example:

- 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





5 Critical Steps to Achieve PCI DSS 4.0 Compliance

Achieving full PCI DSS v4.0 compliance isn't a one-and-done task. It's a strategic journey that demands a phased, deliberate approach. Beyond implementing new technical controls, this latest version of the Standard requires a cultural shift: Compliance must be embraced not just as a checkbox, but as a core element of your organization's security posture. Building a security-first mindset across teams will drive lasting change and help align with PCI best practices.

Follow these five steps to ensure you are leading your organization down the correct path for PCI 4.0 adherence. Using this checklist will help you avoid audit fines and help keep your organization's name out of data breach headlines.

1. No More Grace Period: It's Time to Act

PCI DSS 4.0 is now officially in effect, and organizations must comply with its updated requirements. If you haven't already, now is the time to solidify your action plan — broken down into clear, manageable phases — to ensure your teams stay on track and avoid reactive, last-minute efforts.

Remember, PCI compliance is not a one-time milestone but an ongoing process. By documenting and following a phased implementation strategy, your organization will be better positioned for audit readiness and improved security posture over time.

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 4.0. 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 in 4.0 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 Security Configuration Management 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 4.0's wider SCM scope, ensure 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 4.0 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.

Solutions that combine SCM with file integrity monitoring (FIM) can help your organization to meet the 4.0 standard well before the deadline. Whether your needs are to comply with Requirement 11 using FIM, or to expand configuration monitoring throughout your environment, Fortra can help.

Streamline PCI DSS 4.0 Compliance with Fortra

PCI DSS 4.0 is here — and it's transforming the compliance landscape with new expectations and greater complexity. Achieving and maintaining compliance can feel like an overwhelming, unattainable goal. But with Fortra by your side, compliance becomes more than just a requirement, it becomes a competitive advantage.

We don't just help you meet PCI DSS 4.0. We empower you to exceed it with expert guidance, powerful solutions, and a proactive approach to evolving threats.

Whether you're tackling one PCI DSS requirement or navigating the full Standard, Fortra is here to support you every step of the way.

	PCI DSS 4.0 Requirement	Fortra Solutions That Help
1	Install and Maintain Network Security Controls	Fortra Data Loss Prevention Fortra Integrity and Compliance Monitoring Fortra Vulnerability Management
2	Apply Secure Configurations to All System Components	Fortra Integrity and Compliance Monitoring Fortra Vulnerability Management
3	Protect Stored Account Data	Fortra Data Loss Prevention Fortra Integrity and Compliance Monitoring
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Fortra Data Loss Prevention Fortra Integrity and Compliance Monitoring Fortra Vulnerability Management
5	Protect All Systems and Networks from Malicious Software	Fortra Cloud Email Protection Fortra Integrity and Compliance Monitoring Fortra Security Awareness Training Fortra Vulnerability Management
6	Develop and Maintain Secure Systems and Software	Fortra Application Security Testing Fortra Extended Detection and Response Fortra Integrity and Compliance Monitoring Fortra Managed WAF Fortra Vulnerability Management

	PCI DSS 4.0 Requirement	Fortra Solutions That Help
7	Restrict Access to System Components and Cardholder Data by Business Need to Know	Fortra Integrity and Compliance Monitoring
8	Identify Users and Authenticate Access to System Components	Fortra Integrity and Compliance Monitoring
9	Restrict Physical Access to Cardholder Data	Fortra Data Loss Prevention Fortra Integrity and Compliance Monitoring
10	Log and Monitor All Access to System Components and Cardholder Data	Fortra Data Loss Prevention Fortra Extended Detection and Response Fortra Integrity and Compliance Monitoring
11	Test Security of Systems and Networks Regularly	Cobalt Strike Core Impact Fortra Extended Detection and Response Fortra Integrity and Compliance Monitoring Fortra Managed WAF Fortra Vulnerability Management Outflank OST
12	Support Information Security with Organizational Policies and Programs	Fortra Extended Detection and Response Fortra Integrity and Compliance Monitoring Fortra Security Awareness Training

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

FORTRA™

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

tw-gd-0425-r2-rb