FORTRA™

WHITE PAPER

PCI DSS 4.0 Compliance

Tips to Avoid Last-Minute Panic

Maintaining compliance is a difficult job—both in scope and in practical application. Organizations need to comply with a vast array of regulations, and the number is constantly increasing. Compliance is consistently tightening; businesses and financial institutions now have to learn and dive into the new Payment Card Industry Data Security Standard (PCI DSS) 4.0 requirements as the implementation deadline is coming in 2024.

Complying with a new or updated standard is sometimes easier said than done. The reality is that businesses are busy dealing with day-to-day cyber demands, and compliance often gets put off until it becomes a critical need to address. This is particularly the case in enterprises needing more resources, time, people, and a comprehensive strategy required for robust security and compliance.

Talent gaps and understaffed teams are real concerns across all sectors. As a result, time and people are scarce, and businesses tend to focus on urgent timelines rather than longer-term projects. This approach can often lead to last minute compliance panic.

However, retailers and financial entities can address their daily security operations and requirements while at the same time building their PCI DSS 4.0 compliance. They can do so by adopting a "touch it once" strategy of solving two tasks with one single action, satisfying everyday priorities, and transiting efficiently to PCI DSS 4.0. It is about doing things in a way you don't need to revisit. It's more of an ethos, a thought process, an idea that every time you create a new business process, you must do it with the mindset of "how does this make us more secure and more compliant with the PCI DSS 4.0 standard?"

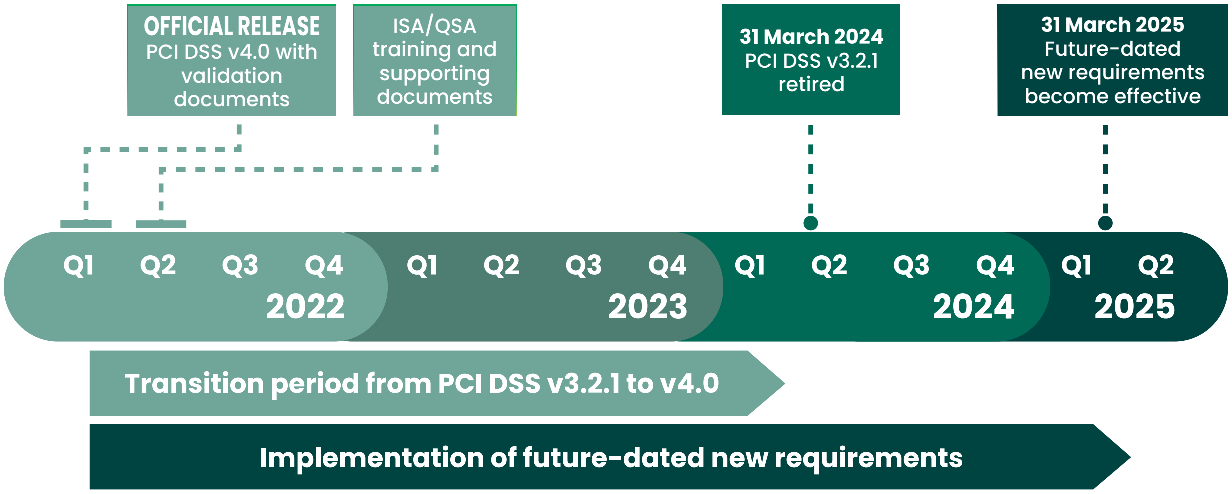
This guide aims to help you understand what is at stake with PCI DSS 4.0 compliance and provide a prioritized roadmap for becoming compliant while protecting your company from everyday cyber risks and threats.

PCI DSS 4.0: What is New?

The Payment Card Industry Data Security Standard (PCI DSS) was developed in 2006 to help businesses that process, store, or transmit payment card data prevent cardholder data theft. While specifically designed to focus on environments with payment card account data, PCI DSS can also protect against threats and secure other elements in the payment ecosystem.

The adoption of PCI DSS 4.0 includes an overlapping retirement date for PCI DSS version 3.2.1 to smooth the transition between versions. This overlap provides organizations time to become familiar with the new version and plan for and implement the changes needed. The diagram below, courtesy of the PCI Security Standards Council (SSC), provides an overview of the PCI DSS 4.0 implementation timeline.

PCI DSS v4.0 Implementation Timeline


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

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.

There are four primary reasons for the changes included in version 4.0:

- Ensure the standard meets the requirements for secure digital payments
- Foster security as a continuous dynamic process
- Make validation procedures more robust
- Support any additional methodologies that achieve the same security goals

In addition, the new version introduces the concept of a customized approach. According to the idea, not all security approaches are the same, and there may be many ways to achieve a security objective. Version 4.0 will allow customization of requirements and testing procedures to accommodate this approach.

Many companies have security solutions that meet the security objective of a requirement. The customized approach lets businesses showcase how their particular solution meets the purpose of the security objective and addresses the risk, providing an alternative way to meet the requirement.

The good news is, the 12 core PCI DSS requirements do not fundamentally change with PCI DSS v4.0, as these are the critical foundation for securing payment card data. However, the requirements are now written as outcome-based statements focused on implementing security control. For many requirements, this is achieved by simply changing the language from stating what "must" be implemented to what the resulting security outcome "is."

The most far-reaching changes concern authentication and data encryption. As the payments industry has gradually moved to the cloud, the PCI DSS focuses on applying more robust authentication standards to payment and control process access log-ins. The new requirements include using multi-factor authentication for all accounts accessing the cardholder data, not just for the administrators accessing the cardholder data environment. In addition, PCI DSS 4.0 includes a broader applicability for encrypting cardholder data, which now expands on trusted networks. You can read the whole list of changes in the respective Summary of Changes guide.

A Prioritized Approach to PCI DSS 4.0 Compliance

By its comprehensive nature, PCI DSS provides a large amount of security information—so much information that some people responsible for the security of payment account data may wonder where to start. The PCI Security Standards Council has developed a Prioritized Approach to compliance to help organizations understand how to reduce risk earlier in their PCI DSS compliance journey.

Per the guide, "*The Prioritized Approach maps all PCI DSS requirements into six risk-based security milestones that are intended to help organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance.*"

The PCI DSS Prioritized Approach includes six milestones:

1. **Do not store unnecessary sensitive authentication data and limit cardholder data retention.** Businesses can limit the impact of a breach if sensitive authentication data and other account data are not stored.
2. **Protect access points to systems and networks and be prepared to respond to a breach.**
3. **Secure payment applications.** Weaknesses in these apps are a common vector for breaching systems and obtaining unauthorized access to cardholder data.
4. **Monitor and control access to your systems.** Have clear visibility of who, what, when, and how the cardholder data environment is accessed.
5. **Protect stored cardholder data.** If storing cardholder data is a business necessity, implement controls to protect this data.
6. **Complete remaining compliance efforts, and ensure all controls are in place.**

These milestones intend to help organizations incrementally protect against the highest risk factors and threats while on the road the PCI DSS 4.0 compliance.

The Prioritized Approach and its milestones provide the following benefits to all businesses:

- A structured approach to address risks in priority order
- "Quick wins" using a realistic approach to cybersecurity and PCI DSS 4.0 compliance
- Financial and operational planning
- Objective and measurable progress indicators

Everyday Best Practices for Building Up Your PCI DSS 4.0 Compliance

Being compliant with PCI DSS version 4.0 may be difficult, but it offers an enhanced way to mitigate the advanced tactics used by threat actors. First, read the PCI DSS 4.0 standard and get familiar with the more significant changes that could impact your compliance process. Then start formulating plans to implement changes in your cybersecurity processes to keep you on track for PCI DSS 4.0 compliance.

The following paragraphs will guide you through the standard 12 requirements and offer you everyday best practices that will allow you to secure your organization from daily threats and build your PCI DSS 4.0 compliance at the same time. For a more detailed view, refer to PCI DSS resources.

Requirement 1: Install and Maintain Network Security Controls

Network firewalls are vital for your security. However, you need more than simply installing a firewall on your organization's network perimeter to secure you.

1. **Create a firewall configuration baseline:** Before implementing firewall settings, document settings and procedures such as hardware security settings, port or service rules needed for business, justification for these rules, and consider both inbound and outbound traffic.
2. **Test all settings:** After implementing firewall configuration settings, test the firewall externally and internally to confirm settings are correct.
3. **Limit outbound traffic (not just inbound):** Often, we worry too much about blocking inbound ports and need to remember to limit outbound traffic from inside the network to just what is required. This limits the attackers' paths for exfiltrating data.
4. **Configure firewalls on personal mobile devices:** Set up personal firewalls on mobile computing platforms to limit the attack surface and minimize malware propagation when connected to unsecured networks.
5. **Disable external firewall management:** Only manage the firewall from within your network. Disable external management services unless they are part of a secure managed firewall infrastructure.

Requirement 2: Apply Secure Configurations to All System Components

1. **Change default settings to reduce inherent weaknesses:** Devices come with factory defaults like usernames and passwords. Defaults make device installation and support more effortless, but they also mean every model originates with the same username and password. When defaults aren't modified, it provides attackers with an easy pathway into your ecosystem. Changing vendor defaults on every system accessing cardholder data is vital.
2. **Harden the Cardholder Data Environment (CDE) according to industry best practices:** Any system used in your CDE must be hardened before it goes into production. The goal of solidifying a system is to remove unnecessary functionality and configure those required securely. Every application or device connected to a system introduces vulnerabilities. According to PCI DSS requirement 2.2, you must "*address all known security vulnerabilities and [be] consistent with industry-accepted system hardening standards.*"
3. **Exercise consistency and keep inventory current:** Once system hardening is implemented and documented, the settings must be applied to all systems in the environment consistently. Once each system and device in the domain has been appropriately configured, you need to assign the responsibility for keeping the inventory current and up-to-date. This way, applications and systems not approved for use can be identified and removed.

Requirement 3: Protect Stored Account Data

1. **Know where your data resides:** Use a data discovery tool to identify the location of unencrypted data so you can delete or encrypt it. They also help determine which processes or flows might need to be fixed. Cardholder data can easily be exposed due to poor processes or misconfigurations. Start by looking where you believe the data is, and then investigate all the locations where it shouldn't be.

2. **Encrypt all your stored data:** Stored card data must be encrypted using industry-accepted algorithms. Many organizations unknowingly hold unencrypted primary account numbers (PAN). In addition to encrypting card data, businesses must protect the encryption keys. Not safeguarding the encryption key location using a solid management process is like storing your house key in your front door lock.

3. **Minimize the data you hold:** Don't keep any data you don't need. Minimize the scope of PCI DSS and ask yourself if you really need a data record.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

1. **Secure data transmitted over open and public networks:** Identify where you send cardholder data. You must encrypt your data while on the move over open public networks.

2. **Stop using obsolete versions of SSL/TLS:** Older versions of SSL and TLS are known to have security vulnerabilities. You must discontinue the use of these deprecated encryption protocols unless the business needs mandates maintaining backward compatibility, such as using POS hardware not supporting later versions of secure TLS.

Requirement 5: Protect All Systems and Networks from Malicious Software

1. **Regularly update antivirus:** Vigilant vulnerability management is the most effective way to proactively reduce the window of compromise, considerably narrowing the opportunity for attackers to penetrate your systems and steal valuable data successfully. As part of your vulnerability management strategy, include updated antivirus software.

Requirement 6: Develop and Maintain Secure Systems and Software

1. **Regularly update and patch systems:** The timely implementation of security updates is critical to your security posture. Patch all critical components in your environment, including browsers, firewalls, applications, databases, POS terminals, and operating systems. Update your software consistently to comply with PCI DSS requirement 6.3.3 which states that organizations must "install critical patches within a month of release." Remember critical software installations like credit card payment applications and mobile devices. Another way to mitigate vulnerabilities is vulnerability scanning, which provides the best method for discovering known security gaps that cybercriminals can exploit to gain access to and compromise an organization.

2. **Establish secure software development processes:** If you develop payment applications in-house, you must use strict development processes and secure coding guidelines. Remember to develop and test applications according to industry-accepted standards like OWASP.

3. **Install web app firewalls:** PCI DSS requirement 6.4 mandates regular monitoring, detection, and prevention of web-based attacks by protecting public-facing web applications with web application firewalls (WAF). These solutions specialize in monitoring and blocking malicious web-based traffic.

Requirement 7: Restrict Access to System Components and Cardholder Data

1. **Restrict access to data and systems:** You should have a role-based access control (RBAC) system with a defined and up-to-date list of roles, which grants access to cardholder data on a need-to-know basis. Restricting access helps prevent exposing sensitive data to unauthorized individuals.

Requirement 8: Identify Users and Authenticate Access

1. **Establish policies for strong and unique passwords and deploy a password manager:** If a username or password doesn't meet the requirements for length, uniqueness, and complexity, it becomes a

vulnerability. To address the limits and risks posed by human nature, consider deploying corporate password management software, so password complexity does not undermine the user experience.

2. **Robust account management:** PCI DSS requires disabling default accounts and having unique user and admin account names. By placing more barriers in an attacker's pathway, a company can be more secure.

3. **Implement multi-factor authentication:** A single password, no matter how strong it is, cannot be the only security precaution. Multi-factor authentication (MFA) is the most effective solution to secure remote access and is a new requirement under PCI DSS 4.0. Your authentication methods should be out-of-band and independent of each other. There should be a physical separation between authentication factors so that access to one factor does not grant access to another. If one factor is compromised, it does not affect the integrity and confidentiality of any other factor. Additionally, PCI DSS requires that you "*incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.*"

Requirement 9: Restrict Physical Access

1. **Control physical access to your premises:** Mitigate physical security risks by implementing physical security policies that preserve on-premises safety for critical assets and data. For example, you can protect these critical assets in a hardened facility. You could also limit outsider access to one monitored entrance and require non-employees to wear visitor badges.

2. **Keep track of POS terminals:** Businesses that use POS systems or mobile payment devices must maintain an updated list of all devices, periodically inspect these devices, and provide staff awareness training for individuals who interact with card-present devices daily.

Requirement 10: Log and Monitor All Access

1. **Regularly review system logs and alerting:** Systems that keep track of logs monitor network activity, examine system events, warn of questionable activity, and record user actions that take place in your environment. The collection and transmission of logs to a centralized location, an on-site logging server, or an internet service is required. To look for mistakes, irregularities, or suspicious activity that deviates from the usual, businesses should analyze their records daily. A more effective security program and quicker response to security occurrences are both benefits of diligent log monitoring. In addition to demonstrating your commitment to adhere to PCI DSS rules, log analysis, and regular monitoring will also aid in thwarting inbound and outbound threats.

Requirement 11: Test Security of Systems and Networks Regularly

1. **Recognize your environment and regularly search for vulnerabilities and conduct penetration tests:** Attackers may get access to an environment through flaws in browsers, email clients, POS software, operating systems, and server interfaces. Many of the recently discovered flaws and vulnerabilities can be fixed before attackers can take advantage of them by installing security updates and patches for systems in a cardholder or sensitive data environments. To find vulnerabilities and repair them, a vulnerability scanning method is helpful. Code testing and independent penetration testing can reveal many of the flaws frequently found in application code in the case of customized internal applications. Penetration testing and vulnerability scans complement each other to promote the highest level of network security. These scans and tests are the best lines of defense in identifying weaknesses so businesses can correct them before deployment.

Requirement 12: Support Information Security with Organizational Policies and Programs

1. **Document and regularly update all business security practices:** All employees should have easy access to written policies. In the event of a breach, documentation might assist in shielding your company from potential liabilities. Security policies and procedures that are fully and precisely recorded make it easier for forensic investigators to see your firm's security measures and show how proactive and committed your company is to security. Companies should periodically update their security measures and actions documentation for PCI DSS 4.0 compliance.

2. **Establish a risk assessment process:** PCI mandates that every entity conducts an annual risk assessment that pinpoints key resources, threats, weaknesses, and dangers. Organizations may identify, organize, and manage information security threats using this activity. Giving the identified threats a ranking or score is a component of risk assessment. This will provide you guidance on which vulnerabilities to address first and help set priorities. By methodically classifying, evaluating, and mitigating risks, you can shorten the window of opportunity for an attacker to gain access to your systems, damage them, and eventually shut down the attack.

3. **Create and test the incident response plan:** You must get ready for a data breach's repercussions. You are responsible for maintaining control of the event, minimizing customer harm, lowering costs related to a data breach, communicating properly with various authorities as specified by various standards and rules, and safeguarding your company. An effective incident response strategy can lessen the effects of breaches, lower fines, lessen negative publicity, and speed up your return to normal operations.

4. **Provide awareness training to all your employees:** Most breaches can be linked to human mistake. Even though many employees are not malicious, they frequently forget security best practices or are unsure of exactly how they are expected to perform. Unfortunately, a lot of criminals will use human error to obtain private information. Specific guidelines must be given to employees, as well as ongoing training. They will be reminded of the value of security through a security awareness program that involves frequent training, especially by keeping them informed of new security policies and procedures.

Final Thoughts

There is still plenty of time until the 2024 PCI DSS 4.0 compliance deadline. Start early, and you will be on the right path to make the transition. Don't wait until 2024 to begin switching over to PCI DSS 4.0. Spread your efforts and upgrade to PCI DSS 4.0 as you go.

Think about your future needs and weave this into your organizational strategy and security program so that you are using your time effectively. Focus on things that are broadly beneficial for the organization on a very long-term basis.

How Fortra Can Help

Fortra's portfolio of cybersecurity and compliance offerings provide a wide range of solutions and services to help businesses comply with the PCI DSS 4.0 requirements and fulfill the daily demands of protecting the company from risks and threats. The following table maps PCI DSS 4.0 requirements to Fortra's solutions.

PCI DSS 4.0 Requirement	Fortra Solution
Requirement 1 Install and maintain network security controls	
Requirement 2 Apply secure configurations	Fortra's Tripwire Enterprise security configuration management functionality ensures businesses monitor the configurations of networks, servers, firewalls, and all other components.
Requirement 3 Protect stored account data	With Fortra's Digital Guardian Enterprise DLP product, customers can use pre-defined PCI policies to monitor and block the egress of credit information across a variety of common egress points. Fortra's Digital Guardian Network DLP appliances inspect all network traffic and enforce pre-configured policies for PCI and other compliance needs to protect data.
Requirement 4 Protect cardholder data with strong cryptography during transmission over open, public networks	Fortra's GoAnywhere MFT is a secure managed file transfer solution that helps users keep sensitive data transfers compliant with PCI DSS. Fortra's Secure Collaboration protects files containing sensitive PII and PCI data no matter where or how it is shared. Organizations can encrypt and control access to cardholder data, as well as track and audit the data and revoke access to it.
Requirement 5 Protect systems and networks from malicious software	Fortra's Powertech Antivirus protects your servers from a comprehensive set of viruses, malware, ransomware, and more.
Requirement 6 Develop and maintain secure systems and software	Fortra's Beyond Security helps detect application vulnerabilities early in the development process with dynamic application security testing (DAST) and static application security testing (SAST) solutions. Fortra's vulnerability management solutions help identify and prioritize vulnerabilities in your environment to close security gaps before attackers find them. Fortra's Tripwire Enterprise's configuration management capabilities help detect unplanned changes in your environment for strong system integrity. Fortra's Alert Logic MDR Essentials includes exposure assessment and management tools, utilizing external, network and agent-based scanning to build a 360-degree view of exposures within IT environments on premise and in cloud. Fortra's Alert Logic is an approved PCI scanning vendor. Fortra's Alert Logic Managed WAF protects web applications by providing continuous detection and prevention for web-based attacks.
Requirement 7 Restrict access to system components and cardholder data	Fortra's Core Security Access Assurance Suite helps identify and manage access across your organization in a single interface. Core Privileged Access Manager (BoKS) helps you control access and privilege to critical systems and information.
Requirement 8 Identify users and authenticate access	Fortra's Core Password is a leading solution for secure self-service password management, with multiple access options, robust service desk integration, and the ability to enforce consistent password policies for any system, application, or web portal.
Requirement 9 Restrict physical access	

PCI DSS 4.0 Requirement	Fortra Solution
Requirement 10 Log and monitor all access	Fortra's Tripwire LogCenter is a correlation engine that provides centralized log collection, analysis, and delivery. Fortra's Alert Logic MDR Professional service includes log management, storage and analysis for suspicious/malicious activity at the point of ingestion, using advanced analytics such as UBAD and triaged by a SOC analyst when appropriate. Fortra's Alert Logic Health Console and Network Health View monitor and notify on the health of Alert Logic security appliances.
Requirement 11 Test security of systems and networks regularly	Fortra's Tripwire Enterprise's integrity management capabilities provide a clear picture to help realize when and where changes were made. As a PCI Approved Scanning Vendor (ASV) Fortra's vulnerability management solutions help you perform comprehensive security assessments which allow you to prioritize the risks that matter most to your organization. Fortra's Alert Logic MDR Essentials includes exposure assessment and management tools, utilizing external, network and agent-based scanning to build a 360-degree view of exposures within IT environments on premise and in cloud. Fortra's Alert Logic is an approved PCI scanning vendor. Fortra's Core Security Core Impact helps conduct advanced penetration tests efficiently. With guided automation and certified exploits, you can safely test your environment using the same techniques as today's adversaries.
Requirement 12 Support information security with policies and programs	Fortra's Terranova Security provides a targeted, engaging, and practical people-centric approach to security awareness training and includes a training module specifically for PCI DSS.

If you don't have the capacity to manage all these activities, our Tripwire and AlertLogic managed services teams can act as an extension of your team to reduce your security risks and simplify PCI DSS 4.0 compliance.

If you would like to learn more about how Fortra can help you achieve PCI DSS 4.0 compliance, take a look at our additional PCI resources or contact us. We will be happy to listen and see how we can help.

FORTRA™

Fortra.com

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.