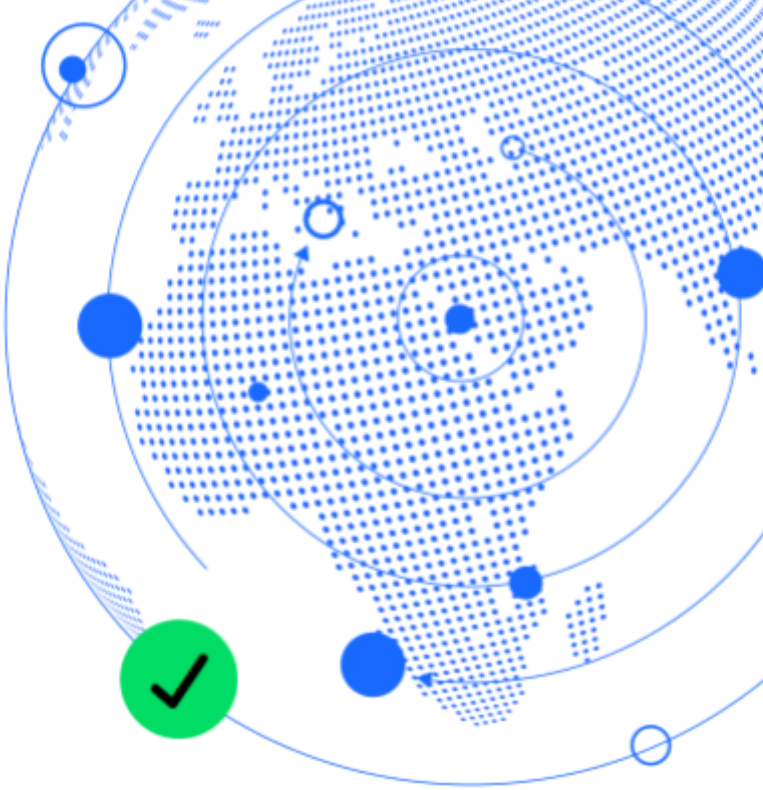
Payment Card Industry Data Security Standard **v4.0**



Are you ready for PCI DSS v4.0?

An updated version of the Payment Card Industry Data Security Standards (PCI DSS) has been released - PCI DSS v4.0. It's important you comply with the new standards – find out more below.

What's PCI DSS?

PCI DSS is a set of technical and operational requirements designed to protect cardholder data. It's a mandatory standard that applies to all businesses accepting card payments.

Why's the update important?

The risk landscape is ever-evolving with new threats to payment data emerging frequently. PCI DSS v4.0 addresses these risks; it reinforces security as a continuous process, increases flexibility for businesses that use different security technologies and enhances validation methods.

What's changing and when?

Currently, v3.2.1 is running in parallel with v4.0 until 31 March 2024. Version 4.0 will be the **only** standard accepted from 1 April 2024.

What do I need to do?

To demonstrate your business is PCI compliant, you need to carry out an assessment of your payment environment and complete a set of validation documents, such as the Self-Assessment Questionnaire (SAQ)

PCI compliance is an ongoing process that requires regular assessments, updates and training. There are several new requirements that you'll need to consider, some of which may need additional resources to help you manage and maintain this. Some examples of the new requirements:

- Ensuring multi-factor-authentication is in place for all that have access to the Cardholder Data Environment (CDE)
- Implementing phishing prevention technologies
- Monitoring ecommerce sites for script changes
- Clearly assigning roles and responsibilities for individuals working on each requirement.

For businesses that take card-not-present transactions and outsource their payment processing and have historically benefitted from the scope reduction offered by SAQ A, there's the addition of potential scanning requirements. While iFrames and page redirects may still reduce your PCI DSS scope overall, you may be subject to these new requirements.

How does this affect my existing assessment?

If you've already completed your annual PCI DSS assessment, your validation documents are still valid for the usual 12 months. When it's time to revalidate, you should use v4.0.

globalpayments

If you use our Global Fortress service run by our partner SecurityMetrics, this is already taken care of for you, as v4.0 is already being presented as an option (in addition to v3.2.1). Validations that take place after 1 April will only be offered v4.0 by the portal and the Global Fortress customer service team.

If you complete the SAQs yourself or have an external Qualified Security Assessor (QSA) complete them for you, make sure you're using the most up-to-date templates as part of the assessment process. If you're having a full external audit via a QSA, you should check with them which version you're being assessed against before they produce their Report on Compliance (ROC).

What happens if I don't comply?

Any SAQs or ROCs that are dated from 1 April 2024 using v3.2.1 won't be accepted and you'll be deemed non-compliant. You risk missing out on any additional security controls that can leave your payment environment vulnerable to a data breach and you may incur non-compliance fees.

What tips do you have for managing the transition to v4.0?

You should ensure you have a full understanding of the PCI DSS v4.0 requirements and how they impact your business. Communicating the information appropriately to your stakeholders and partnering with the right companies are key elements to having a successful PCI DSS transition. More tips on how to do this:

- **Scope management.** Identify all areas of your CDE, such as locations and flows of account data, as well as any connecting networks; this will help you understand the scope of the PCI DSS assessment.
- **Utilise secure technology**. Only partner with trusted companies that have been tested and validated against their own relevant security standards. The Payment Card Industry Security Standards Council (PCI SSC) maintains a list of some of these, such as Point-to-Point Encryption (P2PE) solutions, validated Payment Software, approved PIN Transaction Security (PTS) devices, and Approved Scanning Vendors (ASVs). Visa's Global Registry Service Providers is another useful resource.
- **Understand the requirements.** Review the standards so you fully understand the requirements–it contains detailed guidance against each control that's not included in the SAQs.
- **Mind the gap.** Analyse the differences between version v3.2.1 and v4.0 to identify any actions you need to take for when you're assessed against the new standards. If scanning is a new requirement, start testing your systems to establish any vulnerabilities.
- **Compliance education.** Everyone in your business should be updated on PCI DSS v4.0 so they're aware of any potential vulnerabilities and action can be taken to avoid non-compliance.
- **Acquirer and assessor partnerships.** Partner with acquirers for guidance and best practices. Their partnerships with certified QSAs and security technology firms can help with vulnerability monitoring, ecommerce site control, securing your CDE, gap analysis and all things that impact PCI DSS.

For more information about PCI, visit the PCI SSC website. For specific details about the new version release, read their blog or visit the PCI DSS v4.0 Resource Hub.

If you have any questions about PCI compliance or want to know how we can help, visit our PCI FAQs, contact your Customer Success Manager, email PCICompliance.UK@globalpay.com or call us on 0345 702 3344*.

*Lines are open from 9am to 6pm, Monday to Friday, except public holidays.
If you have a speech or hearing impairment, you can call us using the Relay Service by dialling 18001 followed by 0345 702 3344*. Calls may be recorded. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property.