PCI DSS 4.0

WHAT WE COVER

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards established by major credit card companies, including Visa, Mastercard, American Express, Discover, and JCB, to ensure the protection of sensitive payment card information.

This document covers an overview of the changes so that organisations can prepare for compliance with the new requirements in the latest version of PCI DSS.

WHY IT IS IMPORTANT

Card payments have become an essential part of our daily lives, and we rely on them for convenience and security. In recent years, there has been a significant increase in cybercriminal attacks, and the threat landscape has become more complex and sophisticated. One of the main reasons for the rise in cyberattacks is the increasing dependence on technology and the internet, making it easier for cybercriminals to target individuals and organisations.

The latest version of PCI DSS, version 4.0, aims to address emerging threats to payment card data security, facilitate more effective ways to combat new threats to cardholder information, boost payment flexibility, and improve business procedures to meet security needs.

WHO IT IS GOING TO IMPACT

The PCI DSS standard applies to all organisations that accept, process, store, or transmit credit card information, regardless of size or location.

Organisations that handle payment card information are required to comply with the PCI DSS standard to ensure the security of their systems and protect the sensitive data of their customers.

Organisations may face the following challenges for being non-compliant:

- **Financial penalties** which can vary from £4,000 to £80,000 per month depending on the size of your company and the scale of non-compliance.
- **Legal Action** for failing to protect sensitive customer information.
- **Loss of reputation** which may lead to **Loss of business.**
- **Increased transaction fee** from Card processors.
- **Termination of card processing privileges.**
- Increased risk of data breaches can result in further **financial and reputational consequences.**
- Investment on **Fraud Prevention Technologies** to prevent a breach from taking place again **can be costly.**

WHAT IS CHANGING

The proposed changes to PCI DSS 4.0 are intended to provide organisations with greater flexibility and more customised security controls, while also strengthening authentication requirements, risk management, and validation of service providers.

Some highlights of the proposed changes include:

- Increased flexibility and customisation
- Emphasis on security throughout the software development lifecycle
- Stronger authentication requirements
- Enhanced validation of service providers
- Increased focus on risk management
- More guidance on cloud and mobile payments

Organisations will need to introduce the changes described below to comply with PCI DSS v4.0.

Technical Changes

- **MFA (Multi Factor Authentication) applicability will need to be expanded:**

  ✓ The new recommendation to organisations is to make investments to extend MFA use to additional users and/or systems and devices.
  ✓ MFA should be implemented for all non-console access into the CDE (Cardholder Data Environment) for personnel with administrative access.

- **Setup WAF to prevent public facing web application attack:**

  ✓ Third-party code reviews will no longer meet compliance and must be replaced with a Web Application Firewall (WAF) requirement.
  ✓ The WAF sits in front of the web application and acts as barrier between the web application and incoming traffic to ensure it is legitimate and does not contain any malicious content. WAF can be deployed either on-premises or in the cloud and can be hardware based or software based.

- **Automated Log management for audit log reviews:**

  ✓ Manual log reviews are difficult to perform, even for limited numbers of systems, due to the amount of log data that is generated.
  ✓ Entities should define a targeted risk analysis to define the frequency of periodic log reviews for all system components.
  ✓ Logs for all critical system components and systems that perform security functions need to be collected, correlated, and maintained. A popular tool that can be used to report such changes is SIEM (Security Information and Event Management)

- **Encrypt the data itself not just the disk it is hosted on:**

  ✓ Any stored PAN must also be rendered unreadable through truncation or a data-level encryption mechanism.
  ✓ Storage Account Data (SAD) should be encrypted using a different cryptographic key than is used to encrypt Primary Account Number (PAN), ensuring that two separate keys are required to access the payment card information.

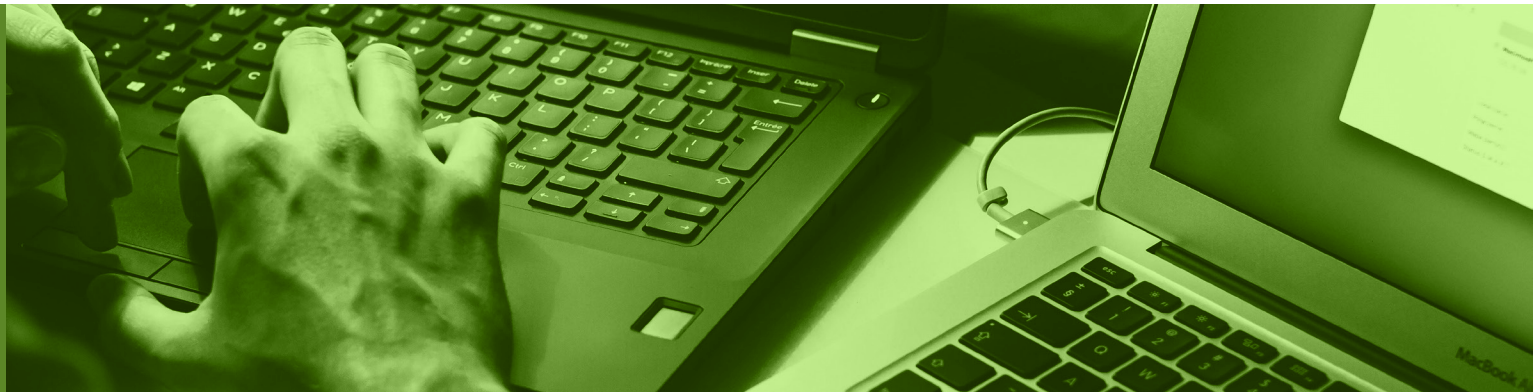
- **Java script validation to prevent e-skimming and man-in the-middle attacks:**

  ✓ Deploy a change-and-tampered detection mechanism to alert for unauthorised modifications to the HTTP headers and contents of payment pages as received by the consumer browser.
  ✓ The mechanism should run at least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis)
  ✓ Mechanism that can be used to report such changes are Web Monitoring tool, embedding tamper detection scripts (using python or java script) or usage of reverse proxies and Content Delivery Networks.

The new Standard introduces a number of Procedural Changes

- ✓ Document and circulate the Roles and responsibilities for performing activities in PCI DSS requirements. (For example: Set up of RACI matrix)
- ✓ Changes with respect to ECommerce Web application include additional documentation required for SSL certificates, including when they need to be renewed, who will be responsible for monitoring the expiration, and the strength of the encryption.
- ✓ Third-party APIs: Organisations need to keep a list of their third-party APIs and other code components. Entities should also implement a mechanism to review external connections and third-party access periodically.
- ✓ Targeted risk assessment- PCI DSS 4.0 focus on moving away from enterprise risk assessment approach to Targeted risk assessment. This new concept helps to define the periodicity of certain requirements. For example: Define the frequency of periodic POI device inspections.
- ✓ Customised approach - This new concept provides greater flexibility for those more mature organisations that must comply with PCI DSS. Entities can determine and implement controls to meet the objective and perform their own testing to verify that the control is working. The level of documentation and effort required to validate customised implementations will be greater than for the defined approach.
- ✓ Periodic diligence of merchants and service providers.

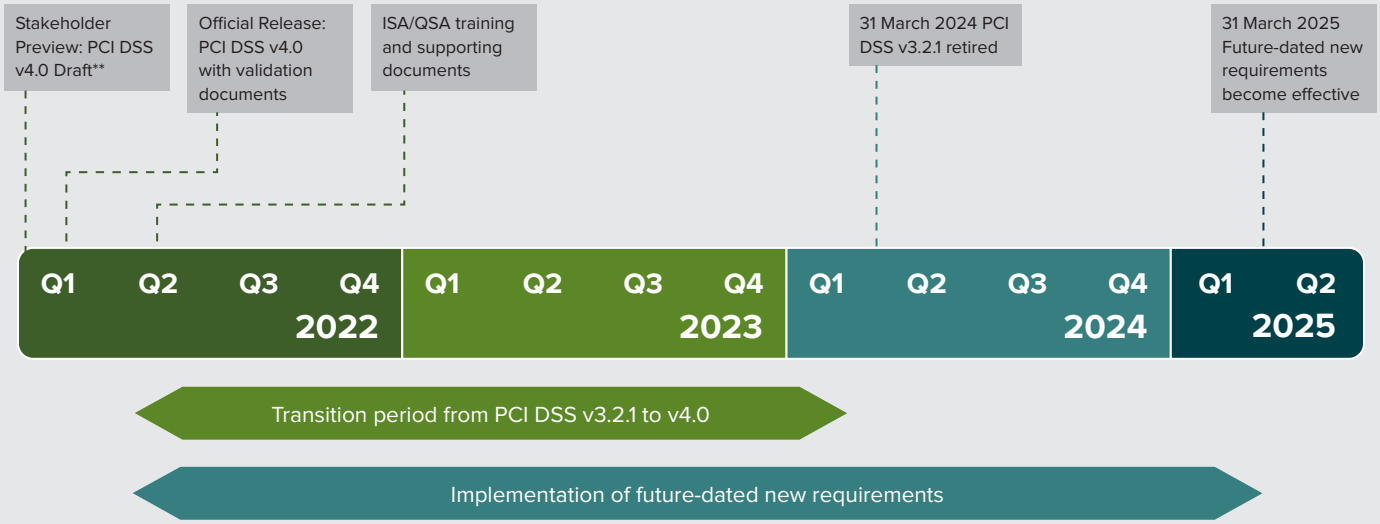
- At least every 12 months and upon a significant change, document and confirm the PCI DSS scope of the in-scope environment.
- Target risk analysis for any controls that use the customised approach at least every 12 months with written approvals by senior management.
- At least an annual risk analysis for any controls that have flexibility for the frequency of controls.
- At least an annual review of cipher suites and protocols.
- At least an annual review of hardware and software technologies in use with a plan to remediate outdated technologies approved by senior management.



WHEN IT WILL BE EFFECTIVE

The PCI DSS Council recognises that it takes time for assessed entities to implement new security controls and fulfil all the new requirements. Below diagram represents the transition period from previous version to latest version.

PCI DSS v4.0 Implementation Timeline*



***All dates based on current projections and subject to change**
**Preview available to Participating Organisations, QSAs, and ASVs

Most of the changes recommended in the latest version will be effective by 31st March 2025, organisations that have implemented controls to meet the new requirements and are prepared to evaluate the controls before the effective date can audit. However, there are couple of requirements that companies need to adhere to immediately.

The immediate requirements recommended by PCI DSS are:

- Roles and responsibilities for performing the following activities are documented, assigned, and understood. (For e.g., setup and agree a RACI matrix)

  ✓ Apply Secure Configurations to All System Components.
  ✓ Protect Stored Account Data.
  ✓ Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
  ✓ Protect All Systems and Networks from Malicious Software.
  ✓ Develop and Maintain Secure Systems and Software.
  ✓ Restrict Access to System Components and Cardholder Data by Business Need to Know.
  ✓ Identify Users and Authenticate Access to System Components.
  ✓ Restrict Physical Access to Cardholder Data.
  ✓ Log and Monitor All Access to System Components and Cardholder Data.
  ✓ Test Security of Systems and Networks Regularly.

- In adopting a Customised Approach, perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customised approach.

- Document and confirm PCI DSS scope at least every 12 months and upon significant changes to the in-scope environment.

Retail Reply has a breadth of real-world industry experience that can help organisations understand the impact of PCI-DSS v4 regulations on their business and determine the best way to deliver any required changes to achieve certification. We have supported organisations with initiatives to deliver PCI-DSS compliant payment services for online and physical channels.

To find out more, please contact retail.uk@reply.com or reach out to our authors:

Mark Wilson, Senior Consultant
ma.wilson@reply.com

Sini Cherukad Manayil, Senior Consultant
s.cherukadmanayil@reply.com

www.reply.com/retail-reply/en/

REPLY RETAIL

Retail Reply
38 Grosvenor Gardens - London SW1W 0EB - UK
Tel +44 (0) 207 730 6000 - retail@reply.com
www.reply.com