KPMG

Payment Card Industry Data Security Standard Version 4.0.1

kpmg.com/in

KPMG. Make the Difference.

The PCI Security Standards Council was formed in 2006 by major card companies Visa, MasterCard, American Express, Discover and JCB to manage the ongoing evolution of the PCI Data Security Standards (PCI DSS). The primary objective of the PCI SSC is:

- Developing and maintaining security standards.
- Providing resources and guidance to help organisations implement these standards.
- Certifying qualified security assessors and approved scanning vendors.
- Raising awareness and educating stakeholders about payment security.

PCI DSS - key takeaways

The PCI DSS is a comprehensive set of security requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

PCI DSS compliance is applicable to any entity that stores, processes or transmits cardholder data.

Below are the six core principles of PCI DSS

01 **Build** and maintain a secure network and system

02 **Protect** cardholder data

03 **Maintain** a Vulnerability Management Programme

04 **Implement** strong Access Control measures

05 **Regularly** monitor and test networks

06 **Maintain** an Information Security policy

PCI DSS version 4.0.1 – what are the major additions?

On 31 March 2022, PCI DSS version 4.0 was released. On 11 June 2024, PCI DSS version 4.0.1 was published with certain additions in 4 requirements and the appendix section. This is currently the latest version of the requirements.

Requirement 3 clarifies new applicability notes for issuers. The Keyed Hashing Scope (Requirement 3.5.1.1) has been updated to include Customised Approach Objective and applicability for organisations using keyed hashes to render PAN unreadable has been elaborated.

Requirement 6 includes new applicability notes for managing payment page scripts. The 30 - day Patch (Requirement 6.3.3) has been updated to define that patches should be applied within 30 days only for 'critical' vulnerabilities as opposed to the previous version which required 'critical' and 'high' severity vulnerabilities.

Requirement 8 clarifies new applicability notes for multi-factor authentication (MFA) for all non-administrative access into the Cardholder Environment. For Phishing-resistant factors (Requirement 8.4.2), the update allows use of phishing-resistant factors to be used instead of MFA and includes controls to deal with the evolving security threats.

Requirement 12 includes new applicability notes to clarify points about relationships between customers and third-party service providers.

Appendices are updated to refer to Customized Approach sample templates available on the PCI SSC website. Definitions for 'Legal Exception', 'Phishing Resistant Authentication', and 'Visitor' have been added.

Frequently asked questions

The PCI DSS is a comprehensive set of security requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. Effective date for implementation of v4.0 will be 31 March 2025.

When will PCI DSS v4.0 be retired?

There will be a period where both the current and updated version will be active at the same time. V4.0 will be retired on 31 December 2024.

Does PCI DSS v4.0.1 change the 31 March 2025 effective date for the new requirements?

No. This limited revision does not impact the effective date of these new requirements. The updated requirements will be in effect according to the dates provided.

Are there any new requirements in PCI DSS v4.0.1?

No. As this is a limited revision, there are no new or deleted requirements. Refer to the Summary of Changes from PCI DSS v4.0 to v4.0.1 for the full details.

When will the PCI DSS v4.0.1 ROC template and AOCs, along with the SAQs be published?

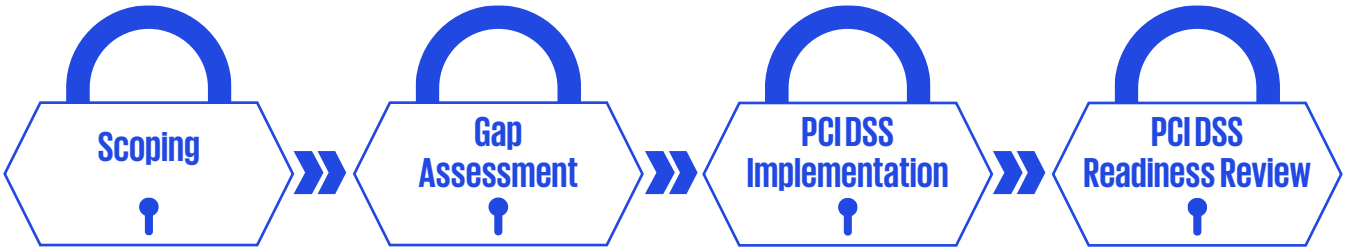
v4.0.1 Report on Compliance, Template and Attestations of Compliance, along with Self-Assessment Questionnaires are targeted for publication in in quarter 3.

How KPMG in India can help

KPMG in India's has deep domain knowledge of cyber security and has diverse experience across emerging and developed markets. The firm's experience spans across multiple industry sectors including aviation, banking, education, insurance, consumer retail, hospitality, entertainment, internet infrastructure, securities, private equity and financial technology.

We understand that your organisation continuously manages strategy, financial, operational, technology, and compliance to focus on business objectives. Our approach is tailored to have less impact on business operation as well as providing added value in response to the challenges.

Project Management and Documentation



Our capabilities and differentiators include:

- Various methodologies for Cyber Security across various industries
- KPMG in India is one of the leading professional services firm which is part of the drafting committee for international standards
- KPMG in India's benchmarking databases include information across companies, data points and KPIs.
- KPMG in India is one of the largest Centers of Excellence for cyber security
- Dedicated ISO Certified Cyber Labs facilities across India for providing cyber capabilities, knowledge bases and tools

We have served our clients in their endeavor to achieve PCI DSS compliance. A representative list of select credentials is illustrated below.

Large multinational bank	UK-based large investment firm	Multinational insurance company	Indian technology giant
Large Indian telecom service provider	Indian fashion and retail giant	East Asian airline company	Indian business process outsourcing company

Contributors:

- Aakansha Gupta
- Madhuri Gangaramani
- Aaradhya Kamle

KPMG in India contacts:

Akhilesh Tuteja
Head – Clients & Markets,
Global Head – Cyber Security
T: +91 98710 25500
E: atuteja@kpmg.com

Atul Gupta
Partner, Head of Function – Digital
Trust and Cyber
T: +91 98100 81050
E: atulgupta@kpmg.com

Kunal Pande
Partner, Co-Head - Digital Risk
and Cyber Leader - Digital Trust for FS
T: +91 98926 00676
E: kpande@kpmg.com

Rohan Padhi
Partner and
Co-Lead Digital Risk and Cloud Security
T: +91 99302 24081
E: rohanpadhi@kpmg.com

Romharsh Razdan
Partner, Lead Payment Risk and
Co-Lead Cloud Security
T: +91 99755 96366
E: romharsh@kpmg.com

kpmg.com/in

Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.