Payment Card Industry Data Security Standard (PCI DSS)

Enhanced cardholder data security

As the world goes cashless, making sure that card payments are secure is crucial to any entity's consumer experience and brand reputation. The Payment Card Industry Data Security Standard (PCI DSS) helps protect cardholder data. It applies to all entities that store, process, or transmit cardholder data, including **issuers, merchants** and **acquirers**. It also applies to entities that can impact the security of the cardholder data environment like **point-of-sale terminal** and **software vendors, cloud service providers** and **data centers.**

With UL's deep understanding of cybersecurity assurance and global payment compliance requirements, we can help you implement and integrate PCI DSS within your enterprise's risk management program, ensuring compliance and contributing to your enterprise's cybersecurity resilience.

End to end support for establishing and maintaining PCI DSS compliance & cybersecurity resilience

Advisory Services
- PCI DSS Compliance Support
- PCI DSS Strategy and Implementation – PCI DSS as part of a robust cybersecurity assurance program
- Third-party vendor PCI DSS compliance and cybersecurity assurance
- PCI DSS Training

Assessment Services
- PCI DSS Gap Assessment
- PCI DSS Formal QSA Assessment

Are you complying to all that you need?

Depending on your role in the payment ecosystem, you may need to comply to more than one PCI program. As the sole security industry expert offering the most number of PCI services globally, UL helps you simplify all of your PCI compliance needs for a cohesive risk management program.

UL is also the only Approved Application Scanning Validator (ASVV) and Consumer Electronic Clearing System Approved Evaluation Facility.

PCI PIN

All entities responsible for secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and payment terminals must comply to the requirements stated in PCI PIN. Entities include payment processors, acquirers, terminal vendors and key injection facilities (KIFs)

PCI Point to Point Encryption (PCI P2PE)

PCI P2PE is a cross-functional program incorporating various PCI security standards. It addresses both the physical and logical security of point-to-point encryption solutions. The program applies to P2PE solution vendors, P2PE component providers, P2PE application vendors, and other third-party entities like data centers who are part of a P2PE solution.

PCI PIN Transaction Security (PCI PTS)

PCI PTS focuses on the physical and logical security of devices used to protect cardholder PINs and other payment processing related activities. Financial institutions, processors, merchants and service providers are advised to only use devices that have been tested and approved under the PCI PTS program.

PCI 3-D Secure (3DS)

PCI 3DS Core security standard applies to entities who provide 3DS Server (3DSS), 3DS Directory Server (DS) or Access Control Server (ACS) functions as part of a 3DS solution. Entities need to discuss with the relevant card brands to determine when they need to go through a formal assessment as per the PCI 3DS Core standard.

PCI Payment Application Data Security Standard (PCI PA-DSS)

PCI PA-DSS addresses the logical security of payment applications. This program applies to payment software vendors and terminal vendors developing secure payment applications to be sold, distributed or licensed to third-parties.

PCI Token Service Providers (PCI TSP)

PCI TSP focuses on the physical and logical security of Token Service Providers – to protect the environments where the TSP performs tokenization services. The standard applies to all entities that generate and issue EMV payment tokens.

Software Security Standard (S3) Framework

The S3 framework aims to address the logical security of payment applications that support existing and future innovations in payment and software practices. Once launched, PCI PA-DSS will be integrated within this framework, including all validated PA-DSS applications.

PCI Software-based PIN Entry on COTS (PCI SPOC)

This standard addresses the physical and logical security of a payment-acceptance solution that allows a cardholder's PIN to be entered on a commercial-off-the-shelf (COTS) device. PCI SPOC applies to entities developing PIN CVM applications, or managing and deploying PIN CVM solutions.

Speak to a UL expert to find out which other PCI security standards you may need to comply with. Visit IMS.UL.com or email us at IMSecurity@ul.com.

Empowering Trust™