# Payment Card Industry Data Security Standard (PCI DSS)

**Enhanced cardholder data security**

As the world goes cashless, making sure card payments are secure proves 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. The standard 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 Solutions' deep understanding of cybersecurity and global payment compliance requirements, we can help you implement and integrate PCI DSS within your enterprise's risk management program, helping you demonstrate compliance and contributing to your enterprise's cybersecurity resilience.

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

**Advisory services**

- PCI DSS compliance support
- PCI DSS strategy and implementation – PCI DSS as part of a robust cybersecurity program
- Third-party vendor PCI DSS compliance
- PCI DSS training

**Assessment services**

- PCI DSS gap assessment
- PCI DSS QSA-led assessment

UL Solutions

## Comprehensive payment systems security solution

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

### 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 should 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 and P2PE application vendors.

### 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 use devices that have been tested and approved under the PCI PTS program.

### 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. This program replaces the PA-DSS Program that was retired in October 2022.

### 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 Solutions expert to find out the PCI security standard with which you must comply. Visit UL.com/pcidss.**

UL Solutions

Safety. Science. Transformation.™


IMS22CS530903
043.01.1022.EN.CYB