PCI Security Standards Council At-a-Glance

The PCI Security Standards Council (PCI SSC) is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. Our role is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders. We achieve this with a strategic framework to guide our decision-making process and ensure that every initiative is aligned with our mission and supports the needs of the global payments industry.

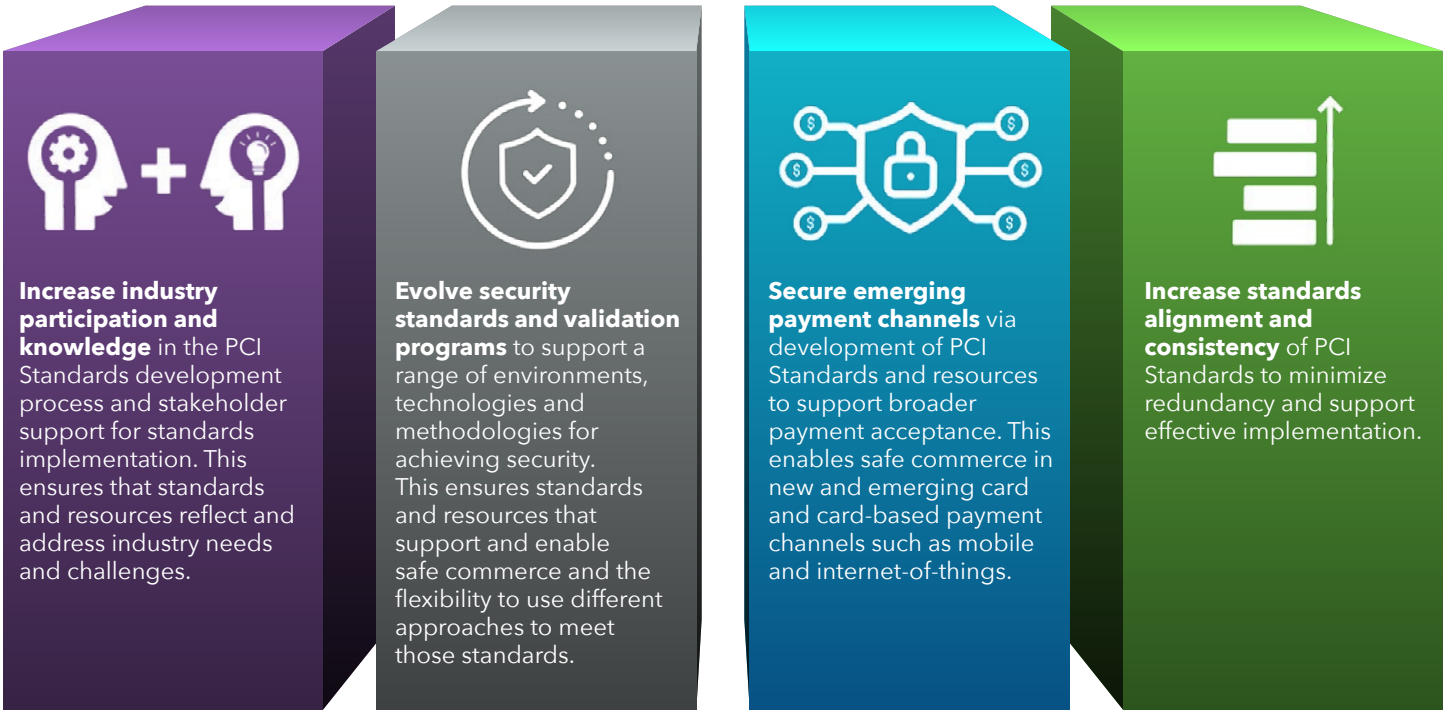
The PCI SSC is led by a policy-setting Executive Committee composed of representatives from American Express, Discover, JCB International, Mastercard, UnionPay and Visa Inc. Enforcement of compliance with PCI Standards and determination of any non-compliance penalties are carried out by the individual payment brands and not by the PCI SSC. This At-a-Glance describes how the PCI SSC leverages the Strategic Framework to help stakeholders enhance security for payment cardholder data.

WHY PAYMENT SECURITY MATTERS

- Security of cardholder data affects everyone
- A breach or theft of cardholder data can trigger large financial loss
- Compromised cardholder data can impact the entire payment ecosystem
- Following PCI Standards will improve cardholder data security and help reduce fraud

Four Strategic Pillars Define the Role of PCI SSC

The Strategic Framework provides the PCI SSC with four pillars of activity that define the Council's role for account data security. The pillars include:



Increase industry participation and knowledge in the PCI Standards development process and stakeholder support for standards implementation. This ensures that standards and resources reflect and address industry needs and challenges.

Evolve security standards and validation programs to support a range of environments, technologies and methodologies for achieving security. This ensures standards and resources that support and enable safe commerce and the flexibility to use different approaches to meet those standards.

Secure emerging payment channels via development of PCI Standards and resources to support broader payment acceptance. This enables safe commerce in new and emerging card and card-based payment channels such as mobile and internet-of-things.

Increase standards alignment and consistency of PCI Standards to minimize redundancy and support effective implementation.

February 2021

What PCI SSC Does

Technical Security Standards

- Develops and maintains a broad range of 15 security standards and supporting programs
- Systematically updates standards and programs in response to industry feedback and emerging threats
- Addresses payment security for issuers, merchants, vendors and solution providers, acquirers and processors

Validation Resources for Professionals and Products

- Provides a valuable resource for entities to find payment security products that have met a strict set of security requirements
- Qualifies and lists a range of assessors who validate compliance with PCI Standards
- Approves and lists network of security evaluation laboratories that test and approve payment solutions
- Trains, approves, and lists forensic investigators who investigate data breaches

Security Training

- Provides wide range of in-person, computer-based, and instructor-led online training program
- Furnishes Security Awareness Training, and qualification for PCI Professionals and Internal Security Assessors

Security Guidance

- Provides industry bulletins to provide education and guidance on common cyber security threats.
- Provides detailed technical guidance for new and emerging technology

Stakeholder Engagement

- Provides engagement opportunities which include Request for Comments (RFC) process, Regional Engagement Board, Global Executive Assessor Roundtable, Technical Advisory Board, Board of Advisors
- Provides membership to Strategic and Affiliate members and Participating Organizations, which allows stakeholders to help shape PCI Standards and guidance
- Includes Task Forces and Special Interest Groups which enables hands-on technical input by stakeholders
- Conducts annual series of Community Meetings and Town Halls in North America, Europe, Asia Pacific, Latin America, India, and Africa/Middle East
- Provides ongoing webinars and publications help keep stakeholders current on PCI Standards and emerging issues for payment security

Who Follows PCI Standards?

Compliance with the PCI Data Security Standard and other applicable PCI Standards may be necessary for entities that store, process or transmit cardholder data. PCI Standards are for entities accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

Who's in Charge of Compliance?

Compliance and enforcement of PCI Standards is the role of the payment brands and acquiring banks, not the PCI SSC. Each of PCI SSC's participating payment brand members currently have their own PCI compliance programs for the protection of their affiliated payment card account data. Entities should contact the payment brands directly for information about their compliance programs.

Each payment brand has its own scheme rules and processes for ensuring the security of cardholder data. These are respectively adopted and implemented by the acquiring banks, who in turn establish their own rules defining the approach their customers must undertake for adopting, implementing, and complying as appropriate with the range of PCI Standards.

Compliance. Contact your merchant bank (acquirer) or payment brand directly for information about PCI Standards compliance programs. Contact details are in FAQ#1142 on our website.

PCI SSC does not receive copies of compliance assessment reports, nor is it involved in and has no information about penalties or fines for non-compliance.

Forensic Investigations. Access the list of approved PCI Forensic Investigators on our website. PCI SSC is not involved in any aspect of a forensic investigation and does not receive copies of forensic reports produced as part of an investigation. Entities should also follow local and regional regulatory requirements in the event of a data breach.

Assessments. If you require the services of a PCI Assessor, PCI Recognized Laboratory, or PCI Forensic Investigator, contact details are on our website. Fees and charges are agreed upon between the entity and the assessor company. PCI SSC does not set or have any influence over fees and charges for services provided.

Where to Learn More About PCI Standards

Learn about all PCI Standards and documents, training and qualifications, lists of qualified assessors and validated solutions and products on our website.

February 2021