PCI DSS Compliance Services

PROTECT CUSTOMER CARDHOLDER INFORMATION THROUGH ADVISORY, READINESS & CERTIFICATION

WHAT IS PCI DSS?

When you take card payments, you rely on customer trust in your ability to protect their financial data. With the Payment Card Industry Data Security Standard (PCI DSS), established by major card brands, your business can demonstrate adherence to stringent security measures. The protocols of the standard are designed to safeguard transactional data, deter identity fraud and prevent costly security breaches, enhancing your reputation as a trustworthy business.

The PCI DSS v4.0.1 is a set of requirements explaining how to protect you and your customers when taking card payments. These are industry-spanning requirements, so all suppliers taking payments should take the PCI DSS seriously.

If you cannot prove you are protecting customer cardholder data, the consequences could be severe for both sides, including:

- Lawsuits
- Financial penalties
- Reputational damage
- Customer disillusionment and distrust
- Theft of customers' money and identities

WHO CREATED THE PCI DSS?

Visa, MasterCard, Discover Financial Services, JCB International and American Express created the PCI DSS in 2004.

WHAT WE OFFER

Our accredited PCI DSS certification service, provided by Panacea Infosec (acquired by SGS in January 2026), confirms your compliance with the 12 key PCI DSS requirements and positions you to manage ongoing security challenges effectively.

WHO IS IT FOR?

An organization that starts taking card payments has 90 days to meet the PCI DSS requirements. After this, you must maintain compliance and show it at least once a year.

Every organization is different, from its size and type to its information security and cybersecurity measures. Therefore, an organization is judged individually. What you must do to comply depends on your potential security risks.

KEY BENEFITS

- Manage risk, increase awareness: significantly minimize the risk of security incidents
- Build trust and relationships: foster trust among customers, partners and vendors
- Save time, money and effort: enhance operational efficiency and avoid noncompliance fines
- Improve your position in the marketplace: boost brand recognition, gain a competitive edge and access international markets
- Achieve continual improvement: pursue continual improvement for long-term business sustainability

THE CERTIFICATION PROCESS IN BRIEF

Foundation

- Understand the 12 PCI DSS requirements
- Identify your compliance level and applicable requirements
- Map your payment card data flows and access points

Assessment

- Complete the appropriate Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)
- Review and confirm security controls and protocols
- Conduct quarterly Approved Scanning Vendor (ASV) scans

Validation

- Perform a risk assessment of the payment environment
- Conduct a gap analysis against the PCI DSS requirements
- Complete an internal audit

Certification

- Establish continuous monitoring
- Engage a Qualified Security Assessor (QSA) and complete the formal assessment

UNRIVALED PCI DSS EXPERTISE AND SUPPORT

As the world leader in testing, inspection and certification, we offer in-depth data security expertise for your business operations. Our comprehensive PCI DSS services are tailored to your organization's needs, regardless of size or sector. We guide you through every step – from initial gap analysis to continuous compliance maintenance. Our global presence and experience ensure that your data security measures meet international standards, helping you navigate and adapt to the evolving landscape of cyber threats.

For more information, email: Certification@sgs.com.

SGS DIGITAL TRUST