PRESIDIO®
Future. Built.

SERVICES TO STRENGTHEN PCI DSS COMPLIANCE

As regulations evolve and cyber threats increase, data protection—and customer confidence—depends on expert guidance

The Payment Card Industry Data Security Standard (PCI DSS) safeguards the information that flows between the companies that accept credit card payments and the banks/acquirers that process these payments. PCI DSS compliance is an essential element of retail data security program—and essential to maintaining customer confidence and ongoing revenues.

It's also a strain on staff time and resources. Self-assessment questionnaires (SAQs) are complex and cumbersome. Regulations regularly evolve in response to increasing cyber threats. Meanwhile, any IT solution must meet both PCI DSS requirements and customer demand for quick, easy purchasing mechanisms.

Presidio can help.

COMPREHENSIVE, CUSTOMIZED SUPPORT

We've worked with PCI merchants at all levels, across industries, to establish and implement PCI compliance programs tailored to their business needs and cyber security readiness. Guided by the latest information on technologies, processes, and regulations, our expert teams:

Analyze compliance gaps

Address these gaps through an end-to-end security and infrastructure roadmap

Develop and implement PCI DSS-compliant policies, processes, and technology architectures

Through a presentation and written report, you'll receive an executive summary of current vulnerabilities and a detailed technical picture of risk, supported by vendor-agnostic recommendations. For ongoing support, we'll assist with:

- Network documentation
- Log management
- SAQs
- Compliance reports

You'll find your staff freed up for other projects, your operations aligned with the latest PCI DSS requirements, and your customers and acquirers more confident than ever in the security of your data storage and handling.

PRESIDIO®

SERVICES TO STRENGTHEN PCI DSS COMPLIANCE

UNPARALLELED EXPERTISE IN COMPLIANCE AND CYBER SECURITY

Drawing from a nationwide pool of cloud, infrastructure, data center, and unified communications specialists, Presidio has assembled an elite cyber security team.

This includes Qualified Security Assessors (QSA) who are up to date on changing technologies, standards, and best practices for ensuring secure credit card transactions. They know what to look for—and what to recommend—for minimizing costs and effort while maximizing the effectiveness of PCI DSS compliance efforts.

PROVEN PROCESSES FOR ENSURING ADHERENCE

With more than a decade of engaging with clients large and small, we've developed the industry's most thorough, informed assessment process and methodology, involving:

- **A baseline view of compliance** that includes an assessment of risk, business requirements, and strategy
- **Technical verification** through assessment, penetration testing, executive reporting, and more
- **Operational support** in areas such as the prevention, detection, containment, and correction of security violations
- **Planning and execution** for the design, integration, and optimization of compliant architecture and processes

A FULL-SERVICE, FULLY COMMITTED PARTNER

Presidio operates as an extension of your IT department, collaborating with your team at every step. We take the time to thoroughly understand your risk, resources, and priorities, so we can bring the most informed compliance guidance to your operations and business.

Take steps now to get a benchmark of your compliance risks and recommendations for moving forward. Call Presidio for a comprehensive assessment and support.

PLEASE CONTACT:

CyberSecurity@presidio.com

presidio.com

LEARN MORE ABOUT PRESIDIO'S FULL SUITE OF CYBER SECURITY SOLUTIONS:

ADAPTIVE STRATEGY

Get expert guidance on cyber security strategy and governance, regulatory compliance, policy and procedures, security awareness and training, architecture and next generation risk management.

ADAPTIVE TESTING

Gauge risk and preparedness through vulnerability assessments, penetration testing, red & red/blue team scenarios and comprehensive security analyses. Check compliance with HIPAA, PCI, GDPR, (NIST Cyber Security Framework, NIST 800-53, NIST 800-171) and ISO 27001 regulations and standards, plus all 20 CIS controls.

ADAPTIVE ARCHITECTURE

Achieve a scalable security architecture/roadmap, including cloud and IoT security, through firewall analysis, device hardening, control recommendations, active directory analysis and PKI assessment.

Build and strengthen application, network, data, endpoint, cloud and physical security.

ADAPTIVE SECOPS

Get 24x7x365 next generation risk management that includes device management, threat intelligence and incident response, plus security event and information management that uses event correlation and analysis and machine learning technology.