RSI | Datasheet

PCI DSS

Compliance Services

The Payment Card Industry's (PCI) Data Security Standards (DSS) apply to merchants and service providers storing, processing, or transmitting credit card data. These entities must adhere to the DSS' 12 Requirements overseeing cardholder data (CHD) and demonstrate compliance via regular reporting and scanning. This requires validation from approved third parties known as Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV).

At RSI Security, we've helped over 250 organizations achieve and demonstrate PCI DSS compliance for more than a decade. As an approved QSA and ASV, we'll simplify your cybersecurity and compliance efforts with sample-based evidence, testing results, roadmaps, and industry best practice recommendations from qualified experts.

RSI Security's PCI DSS Compliance Services

RSI Security provides a comprehensive range of services that meet any merchant's PCI DSS compliance needs.

ROCs

A Report on Compliance (ROC) involves an onsite assessment conducted by an approved QSA to evaluate CHD security, procedures, and policies. An RSI Security ROC provides you with sample evidence of in-place and effective security controls, best practice recommendations to close security and compliance gaps, thorough cardholder data environment (CDE) documentation, and a seasoned assessor that understands your business' compliance efforts.

SAQs & AOCs

RSI Security leverages our PCI DSS expertise to simplify and guide you through your yearly Self-Assessment Questionnaire (SAQ). An Attestation of Compliance (AOC) will be available upon your request to validate the SAQ's completion if your PCI Level requires it.

PCI DSS Scope Reduction

RSI Security will thoroughly assess your IT environment and develop a comprehensive strategy to reduce PCI asset scope. Scope reduction services include PCI asset definitions and documentation, scope boundary identification and segmentation impacts, and network traffic analysis.

Penetration Testing

RSI Security's penetration testing services will identify any vulnerabilities. Additionally, we'll make recommendations on PCI compliance best practices. Penetration testing may focus on a merchant's network security, firewalls, cloud computing, web applications, hardware, mobile devices, and any compliance-specific requirements.

Vulnerability Scanning

RSI Security's PCI DSS expertise ensures that your company's existing vulnerabilities are identified and addressed. Partners will also receive recommendations on prioritized vulnerability management, remediation guidance, and progress reports.

Gap Assessment

RSI Security will assess the gap between your current PCI compliance efforts and the industry standard. Gap assessment relies on an integrated methodology that utilizes network and card data flow diagrams, policy and procedure reviews, and system component configuration sampling.

Patch Management (PCI DSS Requirement 6.2)

Combining forefront cyberthreat intelligence with industry-specific compliance requirements, RSI Security stays up-to-date on and informs partners of current hardware, software, and firmware patches.

Employee Education and Cybersecurity Training

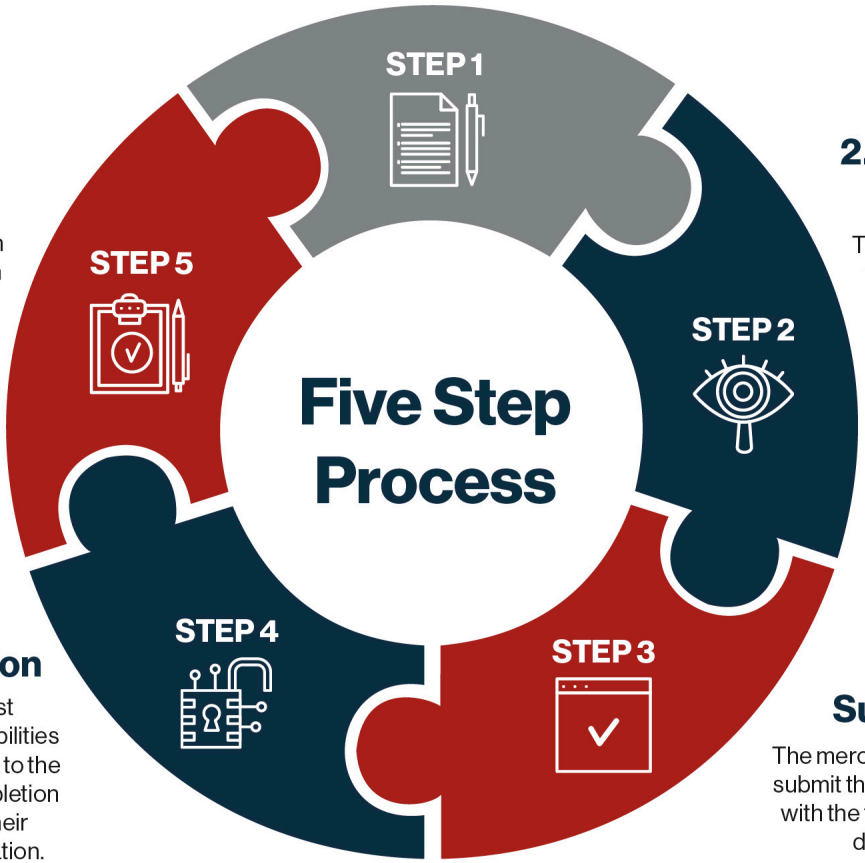
RSI Security will educate and train your staff on best practices for minimizing, identifying, and responding to cyberthreats. RSI Security's education services include a library that features over 400 training assets.

Achieving PCI DSS Compliance

PCI DSS compliance efforts follow yearly and quarterly cycles. Each cycle can be broken into a five-step process.

1. Preparation

Merchants must determine their PCI asset scope, conduct initial scanning for potential vulnerabilities, and fix any current violations.



2. Official Testing & Evaluation

The merchant will undergo third-party assessment, such as ROCs or compliance scans.

3. Form Submission

The merchant will complete and submit the required forms along with the third party's validation documentation.

4. Remediation

The merchant must remediate any vulnerabilities or violations according to the Action Plans and completion dates specified in their reporting documentation.

5. Ongoing Management

The merchant must maintain compliance efforts between reporting periods.

About RSI Security

RSI Security is dedicated to helping our partners rethink their cybersecurity and compliance efforts. Our PCI DSS expertise combines the latest cyberthreat intelligence with over a decade of helping organizations successfully demonstrate their compliance efforts at each reporting Level. Whether you need a Security Standards Council (SSC) approved third party to complete an ROC or merely wish to consult with specialists who will walk you through every step of an SAQ, reach out to us today to get started.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com