RSI | Datasheet

PCI DSS

In The Cloud

The Payment Card Industry's (PCI) Data Security Standards (DSS) apply to all companies that collect, store, process, or transmit credit card data— regardless of whether services and storage are cloud-hosted or facilitated on-premise. However, leveraging the Cloud for cardholder data (CHD) in regards to management and operations presents additional considerations amongst standard PCI DSS compliance efforts.

Companies and their cloud service providers (CSPs) share PCI DSS responsibilities. The proliferation of cloud services requires most companies to properly implement CHD protections across these complex environments.

RSI Security's PCI DSS Compliance Services for Cloud Environments

RSI Security provides a comprehensive range of services for cloud-based CHD environments and operations.

PCI DSS Scope and Responsibilities

Leveraging cloud services provides efficiencies but complicates PCI DSS reporting. Depending on the types of cloud services used (i.e., Software-as-a-Service, Platform-as-a-Service, or Infrastructure-as-a-Service), the distribution of company and CSP responsibilities vary. RSI Security will assess your company's precise compliance requirements—accounting for technology stack, cloud deployment model, and more—as well as provide a scope-reduction strategy and service model advisory for adopting the best cloud services and future migration path to simplify ongoing adherence.

Scope reduction services include PCI asset definitions and documentation, scope boundary identification and segmentation impacts, and network traffic analysis.

CSP Risk Assessment

Third party risk management counts among the varied RSI Security services. As companies bear PCI DSS responsibility when it comes to choosing their CSPs, these risk assessments will ensure that you partner with compliance-friendly vendors.

Penetration Testing

RSI Security's penetration testing services will identify any cybersecurity infrastructure vulnerabilities, particularly those pertaining to PCI DSS compliance. Penetration testing is used to evaluate cloud computing security, as well as network security, firewalls, web applications, hardware, and mobile devices.

Report on Compliance (ROC)

A ROC involves a comprehensive, on-site assessment conducted by a Qualified Security Assessor (QSA) to evaluate CHD security, procedures, and policies. An RSI Security ROC provides you with ample evidence of in-place and effective security controls.

ROC findings will span cloud and on-premise CHD environments, gap assessments to highlight necessary improvements, best practice recommendations, thorough documentation, and a seasoned QSA that understands your business' compliance efforts.

SAQs & AOCs

Cloud CHD environments complicate Self-Assessment Questionnaire (SAQ) completion, requiring extensive Compensating Control Worksheets (CCWs) and additional information to describe implemented protections. RSI Security's PCI DSS advisory services simplify and streamline the SAQ process, and an Attestation of Compliance (AOC) will be available upon request to validate accuracy if your PCI Level requires it.

Approved Scanning Vendor (ASV)

As an SSC-approved ASV, RSI Security will conduct the quarterly vulnerability scans required for most companies subject to PCI DSS compliance and extend the assessment to cloud CHD environments. Companies will receive recommendations on prioritized vulnerability management, remediation guidance, and progress reports.

Cloud Architecture and Security Services

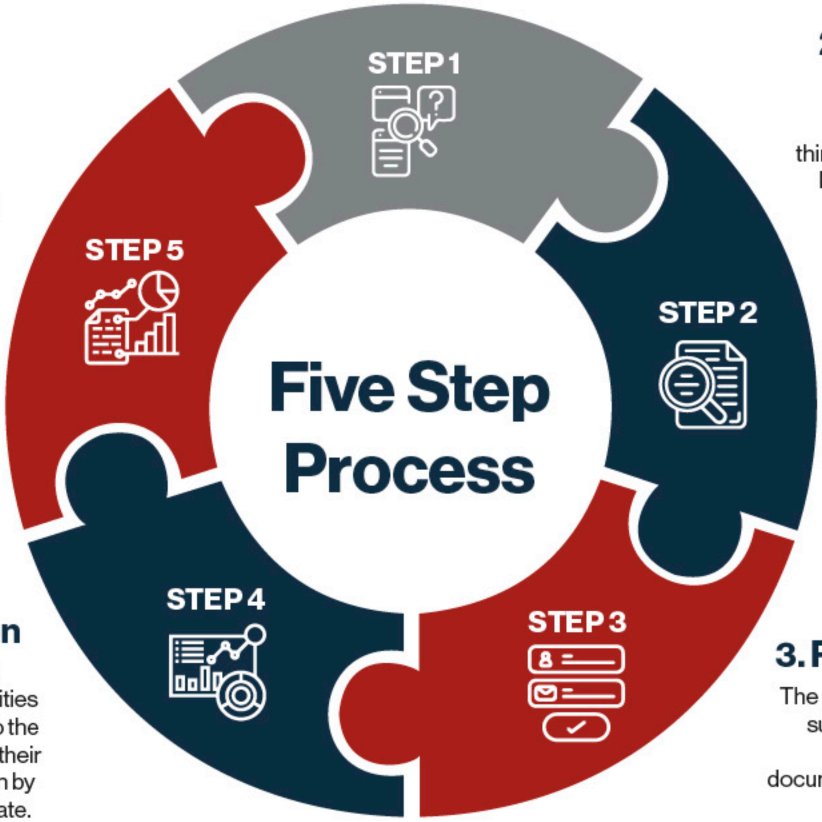
In addition to PCI DSS compliance considerations, RSI Security's managed and advisory services extend to general cloud architecture implementation and ongoing security. Whether your company has transitioned to cloud-only operations or is in the initial stages of planning your migration, we'll help you protect all critical data. RSI Security's scalable cloud services include continuous monitoring and analytics, detection and response, identity and access management, vulnerability assessment, and patch management.

Achieving PCI DSS Compliance with Cloud Services

All PCI DSS compliance efforts follow yearly and quarterly cycles. Each cycle breaks down into five steps.

1. Preparation

Companies 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 a ROC, depending on their PCI Level.

3. Form Submission

The merchant will complete and submit the required forms. Third-party validation documentation provided by a QSA may be required.

4. Remediation

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

5. Ongoing Management

The merchant must maintain compliance efforts between reporting periods, including periodic reassurance that cloud service providers are also meeting their PCI DSS responsibilities.

About RSI Security

RSI Security has provided PCI DSS expertise and compliance services approved by the Security Standards Council (SSC) to over 250 organizations since 2008. As an approved Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), we'll simplify your cybersecurity and compliance efforts no matter your PCI Level, associated reporting requirements, or the make-up of your CHD environments. Whether you must submit QSA-validated documentation or require only SAQ advisory, reach out to us today to ensure your CHD is secure in the Cloud.