Trustwave®
Smart security on demand

DATA SHEET

Trustwave Compliance Validation Service Bundles

PCI SERVICES OPTIONS FROM THE INDUSTRY LEADER

BENEFITS

- Designed to help you meet your organization's unique requirements for achieving and maintaining PCI DSS compliance
- Flexibility even within the bundle options, you can add or subtract services according to your needs
- Opportunity to mix bundle options within a contract period; selecting three different options for a three year contract for example
- Guidance from the industry-leader in PCI services with a proven methodology
- Ongoing support for your Business-As-Usual approach to maintaining your PCI DSS compliance

Most organizations struggle to maintain enough people, time and money to secure their networks on a daily basis, much less manage the annual requirements for Payment Card Industry Data Security Standard (PCI DSS) assessment. Organizations with mature in-house compliance teams may find that a "one size fits all" approach to PCI services does not address their needs.

The flexibility of the Trustwave Compliance Validation Service (CVS) bundles helps you strengthen your security posture and validate your PCI DSS compliance in line with your organization's unique requirements. We know that each organization operates differently, so we make it possible for you to select the appropriate level of service according to your organization's maturity in with its security and compliance program.

HOW TRUSTWAVE PARTNERS WITH YOU

Organizations seeking to validate compliance must obtain a Report on Compliance (ROC) and an Attestation of Compliance (AOC) by a Qualified Security Assessor Company (QSA-C). Prior to the onsite assessment, your organization will need to prepare, implement and maintain processes to monitor and respond to compliance matters in an effective manner.

Built-in best practices and industry-leading compliance tools simplify technology deployment and reduce the time and resources you spend on achieving and maintaining compliance. Compliance validation is achieved in five progressive phases:

1. **Engagement Scoping and Discovery**
   Your QSA assesses the scope of the cardholder data environment determined by your organization to verify that all locations, applications and flows of cardholder data have been included.
2. **Onsite Assessment and PCI DSS Requirement Testing**
   Trustwave conducts interviews and observes systems and processes to validate your company's compliance. The review includes your organization's documentation of all policies, procedures, system configurations, network diagrams, dataflow diagrams and other evidence.
3. **Draft Report on Compliance Creation**
   Your QSA drafts your ROC and AOC based on the previous steps.
4. **Quality Assurance, Final ROC and AOC**
   The Trustwave independent Quality Assurance team evaluates the reports to be sure they maintain the highest quality of required and supplemental supporting detail and can withstand internal and external scrutiny.
5. **Closeout Meetings and Delivery of Final Reports**
   Completion of the process results in a written ROC to be provided to acquiring banks and an AOC which states your organization's compliance status.

Offered in three comprehensive bundles

The CVS Bundles are designed to help you achieve your regulatory compliance objectives and adopt a "business as usual" approach to maintaining PCI compliance. As every organization is unique, the CVS Bundles offer varying levels of assistance and remediation as shown in the chart below.

CVS BUNDLES	PREMIUM	ESSENTIALS	BASICS
PCI Readiness Workshop	●		●
PCI Readiness Subject Matter Expert (SME)	optional		optional
Gap Assessment	●	●	
Gap Assessment Consulting	optional	optional	
Compliance Validation	●	●	●
Quarterly Business-as-Usual Reviews	●	●	●

If your organization is new to PCI or this is your first year validating compliance with an onsite assessment, we recommend you opt for our most comprehensive service with the Premium bundle. The Premium bundle guides you through the key steps of inventorying assets and processes for payment card processing, identifying and getting rid of vulnerabilities to cardholder data and preparing for demonstrating compliance through assessment.

The Essentials bundle is appropriate for organizations who are familiar with the process but need assistance identifying and prioritizing vulnerabilities. The Essentials bundle is designed for organizations who would like to gain assurance with testing and consulting by a QSA on the effectiveness of administrative, physical and technical controls meant to protect cardholder data before the final compliance validation assessment.

And, for organizations with mature compliance programs, we recommend the Basics bundle. The Basics bundle readiness activities are intended to focus on confirmation that business processes remain in place to protect cardholder data as well as address changes to people, process and technology before moving directly into final compliance validation activities.

KEY CVS BUNDLE ACTIVITIES

PCI Readiness Workshop

- Critical concepts for achieving and demonstrating PCI DSS compliance
- What to expect from the assessment
- Review of required administrative, technical and security controls
- Establish required PCI DSS compliance activities and individual ownership
- Review, define and validate formal scope of the cardholder data environment

PCI Readiness Subject Matter Expert (optional)

- Subject matter expert assistance to address key PCI readiness challenges
- Coaching for individuals responsible for assessment interviews and compliance demonstration

Gap Assessment

- Conduct interviews, discussions and facilities inspection
- Analyze results of assessment activities to define client PCI DSS compliance posture
- Create and deliver PCI DSS Gap Assessment Report

Gap Assessment Consulting (optional)

- Create remediation action plan
- Determine evidence needed to prove compliance
- Identify client key challenges
- Establish self-assessment procedures
- Client provides evidence of remediation completion

Compliance Validation

- Virtual Kickoff Meeting
- Collect primary documentation and evidence
- Perform PCI readiness check
- Confirm scope and sampling methodology
- Conduct interviews, perform facilities inspection and controls analysis
- Identify action items and missing evidence
- Analyze results of assessment activities in accordance with PCI DSS requirements
- Define PCI DSS compliance status
- Create and deliver PCI DSS Report on Compliance

Quarterly Business-as-Usual Review

- Review control monitoring activities
- Review processes to ensure control failures are detected and responded to in a timely manner
- Review changes to the environment
- Review PCI DSS scope
- Review hardware and software technologies
- Review status and evidence uploaded to TrustKeeper® Compliance Manager portal

Trustwave®
Smart security on demand

For more information: www.trustwave.com