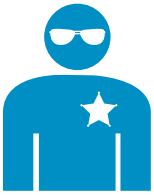
COMPLIANCE VALIDATION SERVICE (CVS)

OVERALL COMPLIANCE PROCESS MANAGEMENT

Trustwave's CVS program assists organizations of all sizes achieve compliance with the Payment Card Industry Data Security Standard (PCI DSS). Delivered through our award-winning, cloud-based TrustKeeper® platform, the CVS program benefits any business, anywhere.

The PCI DSS, for merchants and service providers, includes 12 requirements that specify the framework for a secure payment environment for any business that stores, processes or transmits payment cardholder data. Businesses must attest to compliance under different requirements based on their function, as merchants or service providers, and the amount of payment transactions conducted per year.



ON-DEMAND COMPLIANCE & VULNERABILITY MANAGEMENT

The Trustwave CVS Compliance program is delivered through Trustwave's leading compliance tool, TrustKeeper. A secure web-based portal, TrustKeeper combines all of the necessary tools needed to manage and validate compliance in an easy-to-use one-stop shop.

TRUSTWAVE CVS: PHASES FOR COMPLIANCE

Trustwave CVS consists of four, progressive phases, with an option to add remediation services if needed:

1. Engagement Scoping

Dedicated Trustwave consultants work closely with organizations to identify and validate all locations, applications and flows of cardholder data to ensure that they are included in the scope of the CVS engagement.

2. Primary Document Collection & Mapping

The PCI DSS requires documentation and evidence to be collected during the assessment process. Trustwave will review and analyze submitted documentation to include all policies, procedures, system configurations, network diagrams, dataflow diagrams and other evidence as required for validating PCI DSS compliance.

3. On-Site Assessment

Organizations processing greater than 6 million transactions per year must undergo a third party validation of compliance with the PCI DSS, including onsite assessment. Trustwave will assign a Qualified Security Assessor (QSA) to validate a company's compliance with the data security requirements by conducting interviews with business and operations personnel, and perform required tests. The QSA will coordinate and schedule activities and resources with the client company and ensure the quality of all Trustwave deliverables.

4. Report on Compliance & Finalization

Entities found to be compliant by Trustwave will receive a written Report on Compliance (RoC) to be provided to acquiring banks and an Attestation of Compliance (AoC) as a declaration of compliance status.

TRUSTWAVE VULNERABILITY MANAGEMENT

Trustwave's proprietary scanning services enable an organization to meet requirement 11.2, while providing security, support, self-scan and reporting capabilities.

External Vulnerability Scanning (EVS)

- PCI Approved Scanning Vendor (ASV) compliant
- An "intelligent" automated scanning engine
- Tests for thousands of unique vulnerabilities
- Extremely accurate in eliminating false positives
- 16 scans per year for up to 256 IP addresses
- No hardware or software needed

Internal Vulnerability Scanning (IVS)

- Managed IVS, delivered via a dedicated managed appliance or Trustwave Unified Threat Management (UTM)
- Vulnerability database comprised of the SANS top 20 as well as more than 3,000 of the latest vulnerabilities
- Unlimited scans for up to 256 IP addresses

MANAGED SECURITY TESTING

Managed Security Testing from Trustwave Spiderlabs delivers on-demand, precision penetration testing with just a few clicks of a mouse. With a subscription, users can login to the portal and schedule web application and internal or external network testing on demand and with pre-defined pricing.

- Prevent exposure between annual tests
- On-demand retesting at no additional cost
- Ongoing testing throughout the subscription term
- You control the breadth and depth of testing

TRUSTKEEPER COMPLIANCE MANAGER: REAL-TIME REPORTING DASHBOARD

TrustKeeper Compliance Manager provides a central point to manage the annual assessment process, including providing features for management oversight, document transfer, system sampling, PCI DSS requirement management and reports delivery.

- Detailed Report on Compliance (RoC) and rich customer interaction with your QSA, including:
  - On-demand charts and report creation, such as control status and asset status reports
  - QSA feedback
- Information sharing across compliance applications, including data feeds from:
  - Managed Security Testing
  - Enterprise Vulnerability Management
- Management of annual PCI validation assessments

TRUST INDICATORS

As part of CVS, businesses receive Trustwave's industry-recognized trust indicators:

The Trusted Commerce℠ Seal: When displayed on a website, this seal raises recognition of the commitment to data security, distinguishing businesses as committed to handling payment card data in a secure manner. The seal confirms a company's enrollment in Trustwave's program to validate compliance with the PCI DSS.

Trustwave Extended Validation (EV) SSL Certificate: CVS clients receive one Extended Validation (EV) SSL certificate for one year, helping them establish a new standard for Internet reputation and online security. When an EV SSL is presented during an online session, your customer's browser address bar is shaded green to call attention to and promote your website's security. Additionally, an EV SSL certificate fulfills a number of e-commerce requirements within the PCI DSS.

The green Internet-address bar displayed in Internet Explorer by a Web site that presents an EV SSL Certificate

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com