Trustwave®

Trustwave Payment Application Assessment Service

INDUSTRY-LEADING VALIDATION AND REMEDIATION SERVICES

Trustwave has deep roots and leadership in Payment Card Industry (PCI) compliance. Trustwave delivers industry-leading payment application assessment services to application vendors who require PCI Payment Application Data Security Standard (PA-DSS) validation status.

Delivering a Range of Payment Application Services

As a Payment Application (PA) Qualified Security Assessor (QSA), Trustwave provides a number of services to support your PA-DSS initiatives. They range from validation services to supporting remediation services. They include:

- PA-DSS Validation
- Application Penetration Testing
- Remediation Assistance
- Implementation Guide Development
- Change Impact Analysis and Review
- Maintenance
- Application Security Review

The PA-DSS Validation Process

The PA-DSS validation consists of a structured review of a payment application resulting in either a report attesting to the application's compliance with a Report on Validation (ROV) or identification of the areas of improvement needed. The service starts with initialization and ends with submission to the PCI Security Standards Council (SSC) as described in the following steps.

1. **Initialization**
   The initialization phase opens the line of communications between the Trustwave security consultant and the point of contact at your company. The date for the kickoff meeting is set.

2. **Kickoff Meeting**
   In the kickoff meeting, the scope, timing of activities and deliverables due dates are agreed upon. The kickoff meeting also aims to include all involved parties from both Trustwave and your organization to understand the role each person will play during the engagement.

3. **Information Gathering**
   The goal of this phase is to maximize our understanding of the application's functionality, data handling processes and design parameters before conducting the application testing portion of the validation.

   Trustwave conducts interviews with your system architects, application developers, database developers and other members of the application team. The goal is to dive deeper into the individual requirements and obtain a clear understanding of how each requirement is met. In addition, Trustwave examines applicable documentation and may request a demonstration of the application's capabilities.

4. **Application Testing**
   During the application testing phase, the PA QSA conducts all of the tests required by the PA-DSS Testing Procedures. This includes running all types of transactions supported by the application as well as monitoring the data's flow through the application. Penetration testing is performed with additional testing for web-based applications. See the Application Penetration Testing section for more information. A working document is maintained by the PA QSA to record the results of the tests that have been performed and whether they meet the requirements.

   The goal is to ensure that each of the PA-DSS requirements is being met wherever the application stores, transmits or processes cardholder data.

5. **Forensic Review**
   Once testing is completed, Trustwave performs a forensic review of the collected data. Trustwave uses powerful forensic analysis tools to detect any data leakage or data in obscure, insecure or unintended places in the system.

   Should any cardholder data be detected in locations not mentioned during developer interviews, Trustwave will report the finding back to you for analysis and response; should cardholder data be found in clear-text in a non-compliant location, Trustwave will mark it as a non-compliant finding in the working document for remediation.

6. **Reporting**
   The PA QSA will combine the updated Executive Summary document with the working document to create the PA-DSS Report on Validation (ROV). This document is the end product that will be sent to the Trustwave Quality Assurance (QA) department who in turn reviews the report.

   If the application is found to be in full compliance, you will be given the opportunity to review and comment on the report. If, however, the report requires additional information or changes, Trustwave will contact you for any required information or remediation.

7. **Submission to the PCI SSC**
   Once you have reviewed the ROV and approved it, Trustwave requires a signed copy of the Attestation of Validation (AOV) for upload to the SSC. The SSC requires that the Implementation Guide is included in the submission.

   At this point the engagement is considered complete. The report is either in the hands of the PCI SSC for acceptance or you are working on updating your application to meet the PA-DSS requirements.

Application Penetration Testing

The PCI PA-DSS requires an application penetration test. For web-based applications, additional testing is required. This test is performed by Trustwave SpiderLabs to determine how secure the application is from a web application-layer perspective. The result is a detailed report on the environment and any remediation steps that should be taken.

Remediation Assistance

If your final Report on Validation contains areas of non-compliance, you may request Trustwave remediation assistance in working through the effort of updating your application documentation and/or the application. In this case, Trustwave is available to assist you on an hourly consulting basis.

Implementation Guide Development

The PA-DSS requires that software vendors develop, implement and provide an updated Implementation Guide for their customers, resellers and integrators to mitigate the risk that a PA-DSS compliant application will be installed incorrectly and leave it vulnerable to attack.

Trustwave can provide you with consulting services to assist in the development of an Implementation Guide. The document will be created in conjunction with your staff to ensure that it reflects the specific software application undergoing PA-DSS validation.

Change Impact Analysis and Review

After a specific version of an application has been validated and listed as compliant, any change to the application must undergo a PA-DSS revalidation in order for the updated version to be listed by the PCI SSC. In this process, you complete a PA-DSS Change Analysis document and Trustwave will determine the level of application change based on the PA-DSS guidelines. Depending on the impact of the change, additional application testing may be required before submission to the PCI SSC by Trustwave.

Maintenance

The Maintenance Program is available to you for one year after your payment application(s) is listed on the PCI SSC Validated Payment Application website following your Trustwave PA-DSS assessment.

The program can consist of both remote and onsite assessment activities. If possible, Trustwave will maintain a working version of your application(s) in our ActiveLab in order to quickly deploy a testing environment for new application versions.

Application Security Review

For payment-acceptance applications that operate on any consumer electronic handheld devices (e.g., smartphone, tablet, or PDA) that are categorized as Category 3 by the PCI SSC, Trustwave offers application security reviews.

Trustwave®