SecureTrust™
a Trustwave® division

Payment Card Industry Data Security Standard

SELF-ASSESSMENT VALIDATION

The PCI DSS Self-Assessment Validation is an additional layer of assurance—a third party review—for self-assessment questionnaire (SAQ) eligible entities. We provide assurance in addition to your self-assessment. The PCI DSS Self-Assessment Validation service is an impartial validation of the compliance of your cardholder data environment (CDE).

How it Works

You tell us which self-assessment questionnaire (SAQ) you complete and we assess the same environment, independently. If we find that indeed you are compliant with the applicable PCI DSS controls, SecureTrust will provide an assessment report and countersign an Attestation of Compliance (AOC) as a declaration of your compliance status with the applicable client self-assessment questionnaire (SAQ). If we identify areas of non-compliance, SecureTrust will provide a non-compliant assessment report detailing those findings and corrective guidance.

What You Get

Your organization will gain access to a qualified security assessor (QSA) who assesses your environment, determines whether your organization is compliant and documents their findings. A Managing Consultant (MC) is assigned to every project as a secondary point of contact for questions and guidance. The MC is also available for escalations, project oversight and reporting quality assurance for the QSA.

Our proprietary software, Compliance Manager, is included to manage the engagement with dashboards, action items and a file repository to securely store evidence, documentation, and deliverables.

The final output is our assessment report and, if found compliant, we will countersign your attestation of compliance (AOC). In section 3 of the PCI DSS SAQ and the AOC, you will declare that you are not storing sensitive authentication data, that you are maintaining a vulnerability management program and that you have found all other applicable controls in place. If our assessment finds these things to be accurate, we will indicate our involvement in the process and the role we performed and will attach the signature of a duly authorized officer of SecureTrust.

Delivery Process

Key activities include discovery, PCI DSS requirement testing, quality assurance (QA) and then we close out the project with a meeting to discuss our findings and deliver our report. Reviews of individual requirements cannot lead to the assertion that an organization is compliant. Rather, an understanding of the environment as a whole is needed to validate the scope is accurate, the correct SAQ selection and the status of applicable controls.

For discovery we will conduct an in-depth examination of your policies and procedures, asset inventories, data flow diagrams, network diagrams, and other documentation which defines the environment. PCI DSS requirement testing is performed through interviews, discussions as well as facility inspections and control analysis. We will collect and test using evidence testing action items assigned in the Compliance Manager Application. Ultimately, we will analyze evidence in accordance with the PCI DSS requirement and draft our assessment report and conduct a closeout meeting summarizing the current state of your PCI DSS

BENEFITS

Clients that complete SAQ's are frequently found non-compliant during a full PCI assessment by a QSA due to, either, a fundamental misunderstanding of the requirements or inaccurate scoping. Undergoing a self-assessment validation with full QSA review of the applicable controls will ensure that you are accurately assessing your own environment and providing accurate findings to your acquiring bank or other partners. With a proper scope and a comprehensive understanding of the intent of each requirement, you are better prepared to maintain compliance. And, by extension, your entity is also better prepared to progress to a full onsite assessment and make a smooth transition to level one status.

- Comfort and additional assurance for your SAQ
- Independent review of the applicable client environment
- Additional assurance that scope was properly identified
- Additional assurance that controls are understood
- Review of SAQ findings
- Signed attestation of compliance
- Easy transition to full, third party, onsite review of compliance

compliance and deliver your report. We will countersign your AOCs as a declaration of your compliance status if the environment is found compliant with the PCI DSS.

Please note, SecureTrust will not complete an SAQ on your behalf. Rather, the engagement includes an independent onsite assessment and is a complete PCI DSS assessment for the applicable SAQ controls. SecureTrust will review applicable evidence from your systems and processes as required to demonstrate compliance with the specific requirements. Our report is not intended to be shared with an acquiring bank or brand—that's what the SAQ and the AOC are for. Our report can provide assurance for your SAQ answers with our independent validation of scope, SAQ selection and our determination of your compliance status. And, in the case of non-compliant findings, our report will direct your organization on areas of non-compliance and possible corrective actions.

Learn More

To learn more, please contact us and ask about our PCI DSS Self-Assessment Validation service.

www.securetrust.com

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com