PA DSS to PCI-SSF: Everything that you need to know about the transition

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

The PCI PA-DSS Standard was launched in the year 2008 to help merchants secure their applications and safeguard cardholder data.

The Payment Application Data Security Standard (PA-DSS) applies to all software developed by vendors who store, process, or transmit cardholder data and/or sensitive authentication data.

However, the Payment Card Industry Security Standard Council recently rolled out a new framework to improve security standards of applications that accept payments and use payment data in their environment. With the implementation of the new Standards, the PA-DSS Standards would slowly phase out by 2022.

The transition from PA-DSS to PCI SSF

In 2019, the PCI Security Standards Council released the PCI Software Security Framework (SSF) for the secure design and development of payment software. As stated earlier, the PIC-SSF replaces the PA-DSS with new requirements that support a variety of payment software types, technologies, and development techniques.

However, even though PA-DSS Standards are soon phasing out, it is to be noted that, the new Standard will affect the current payment application within the PCI-DSS environment. The new framework is setup with a unique approach to support traditional and modern payment software, including Cloud and Mobile platforms. The framework is designed to validate the security and development practice of both modern and traditional payment software with an objective-based approach.

The new framework is said to provide flexibility for software vendors and facilitate better alignment of secure application development, as per the industry standard. The framework facilitates software vendors to offer PCI-validated payment software. This shall give merchants confidence that the software added to their environment facilitates compliance with PCI DSS and adheres to stringent security controls.

What Is the PCI Software Security Framework?

The PCI Software Security Framework is a new Standard rolled out with a purpose to secure the design and development of payment application software. This is a crucial move towards improving the security of payment applications and further facilitate reliable online payment transactions.

The latest objective-based security framework supports the evolving landscape of application design and development practice with a modern approach. The new framework can support security requirements in both modern and traditional payment software. The SSF provides vendors with security standards for building and maintaining payment software that protects payment transactions and data, reduces vulnerabilities, and sets a strong defence against attacks. The new methodology adopted for validating software security facilitates robust security development practices in the industry.

The objective of rolling out PCI Software Security Framework

PCI Software Security Framework is a blend of traditional and modern software security requirements that support evolving technologies, software types, and development methodologies. The new framework was designed and implemented to encourage objective-focused security practices that can support both the traditional methods of good application security and the latest development practices.

Impact of transition on your organization

When PA-DSS v3.2 expires in 2022, the Standard will be formally replaced by the new PCI-SSF. So, during the transitional phase, the validation of all PA-DSS will move to the "Acceptable Only for Pre-Existing Deployments" on the PA-DSS listing of applications on the PCI Council website. To make it a hassle-free transition for stakeholders, the PA-DSS and SSF Programs will run parallelly with the PA-DSS Program continuing to operate as it does till the date of expiry.

Existing PA-DSS Validated Payment Application

The PA-DSS Program will remain open and fully supported until October 28, 2022, with no changes to the way the existing PA-DSS validated applications are handled. They will remain on the list of PA-DSS Validated Payment Applications until their expiry dates. Further, as per the normal process, vendors can submit changes until the PA-DSS v3.2 expiry date. On the date of expiry, the PA-DSS v3.2 will automatically be replaced by the PCI Software Security Framework.

New PA-DSS submissions

Vendors will be able to submit new payment software products for PA-DSS validation and listing until 30 June 2021.Low-impact changes can still be submitted for currently valid applications until their expiration date.

On the date of expiry, all PA-DSS validated payment applications will move to “Acceptable Only for Pre-Existing Deployments” on the PCI SSC website.

Originally Published on:- **itsecurityguru**

Written By:- **VISTA InfoSec**

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA +1-415-513 5261 | INDIA +91 73045 57744 | SINGAPORE +65-3129-0397 | UK +442081333131