The Evolution Of PCI DSS

The PCI DSS framework has 12 basic requirements to protect payment card data. The 12 requirements have fundamentally remained the same but have evolved over the years to adjust for technology changes and evolving threats.

PCI Evolution Timeline

2004 **PCI 1.0:** PCI DSS framework created

2006 **PCI 1.1:** Enhanced to address evolving web application security

2008 **PCI 1.2:** Enhanced to address evolving wireless security

2009 **PCI 1.2.1:** Enhanced with input from industry contributors

2010 **PCI 2.0:** No major changed; Designed to provide greater clarity and flexibility to facilitate improved understanding of the requirements and eased implementation for merchants

2013 **PCI 3.0:** Focuses on helping businesses integrate payment security into daily business practices.

2015 **PCI 3.1:** Addressed vulnerabilities in the SSL protocol

2015 **PCI 3.2:** Addressed growing threats to customer payment information

2018 **PCI 3.2.1:** Minor update to address customer migration to enhanced TLS Security

What will PCI DSS 4.0 Bring?

You Can Anticipate a Focus on:

- Continued enhancement of the standard to meet today's payment security needs.
- Assessments adhering to validation requirements as a consistent experience across the industry.
- Payment security in the context as a continuous process.
- Increased flexibility in the methods used to implement payment security.

Critical Control Testing Frequency

- Organizations may become a 'designated entity' if identified as one by an acquirer or payment brand.
- Once deemed a 'designated entity', organizations will have to undergo a series of additional validation procedures to provide greater insight into and assurance that an organization's PCI DSS controls are being effectively maintained.
- The 'designated entity's' supplemental validation requirements are usually reserved for companies that have experienced a breach. However, the requirements may become a compliance standard for more businesses.

Monitoring Technology Advancement Requirements

- To meet the continuous compliance requirement of PCI DSS, more companies are likely to adopt the **PCI Software Security Framework.**
- With the adoption of the PCI Software Security Framework, organizations are likely to increase risk management activities of PCI DSS controls in their deployment life cycles.

Authentication: Deeper Focus on NIST MFA/Password Guidance

- To enhance consumer protection online merchants may likely integrate with card issuers using 3-D secure technology for card not present payments.

Sources:

https://blog.pcisecuritystandards.org/pci-dss-looking-ahead-to-version-4.0

https://www.pcisecuritystandards.org/pdfs/09-07-06.pdf

https://www.pcisecuritystandards.org/pdfs/pr_080930_PCIDSSv1-2.pdf

https://www.pcisecuritystandards.org/pdfs/pr_101028_standards_2.0.pdf

https://www.pcisecuritystandards.org/pdfs/13_11_06_DSS_PCI_DSS_Version_3_0_Press_Release.pdf

https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf

https://www.pcisecuritystandards.org/pdfs/PCI-DSS-3.2.1-Release.pdf

Our Credentials

Founded in 2016 and named one of the fastest-growing start-ups in 2020 by CB Insights, Very Good Security is backed by Visa and leading venture firms, including Goldman Sachs and Andreessen Horowitz. VGS is also a Visa Level 1 Global Supplier.

contact@verygoodsecurity.com

verygoodsecurity.com

VERY GOOD SECURITY