VIGIONE

VigiOne for Merchants and Third Party Service Providers enables successful migration to PCI DSS 4.0 and beyond

PCI DSS 4.0

PCI DSS is the global data security standard utilised by the payment card industry to protect the cardholder. It is set by the PCI SSC (Payment Card Industry Security Standards Council) and applies to any organisation that processes, stores or transmits account data (cardholder data and/or sensitive authentication data). The standard is upgraded periodically, the version of the Standard known as PCI DSS v. 3.2.1, is now to be replaced with PCI DSS 4.0. This new version of the Standard places increased focus on risk analysis and governance, and requires oroganizations to be prepared to report continuously rather than annually. Following industry consultation, the revised standard also allows for more flexibility to report in ways that suit organisational needs and risk exposure. The updated version was recently released, so companies who want to comply with industry 'best practise' will want to implement the changes as soon as possible. Use of a compliance management platform such as VigiOne to manage further transition to full and ongoing compliance is more or less essential for complex organizations.

Timeframe

Presently, the revised new rules are optional. They will not fully replace the current Standard until March 31 2024, when 3.2.1 will be retired, with some of the new 4.0 requirements still not being mandatory until March 31, 2025. However, organizations will need to prepare for PCI DSS 4.0, assess the gaps and validate compliance programs, between now and then, in order to ensure continuous compliance to the new standard from March 31 2024 onwards. Organizations will have to identify any current compliance gaps and to commence planning and implementation, particular where new tailored processes, to satisfy the updated rules, are opted for, as part of the customized approach. This customized methodology is "intended for risk-mature entities that demonstrate a robust risk-management approach to security, including, but not limited to a dedicated risk-management department or an organization-wide risk management approach", such a process genuinely requires a single systemized platform.

Major Changes

There are many changes to the standard and these are outlined in the document **Payment Card Industry Data Security Standard, Summary of Changes from PCI DSS Version 3.2.1 to 4.0, Revision 1 May 2022** available at https://www.pcisecuritystandards.org/document_library. To summarise however, the key changes are;

Customized Approach

Organizations may want to adopt a customized approach to PCI DSS, because of the particular and unique nature of their risks and practices, or to integrate with an established organization wide security program that ensures compliance to multiple security or data standards
Having elected to implement a customized approach, an organizations must then design and prepare proposed controls to meet the security objective of the requirements and share them with their qualified security assessors (QSAs) to get feedback on whether the controls meet the stated security objective. The PCI SSCl has provided new Appendices D and E that include further information and sample templates for documenting the controls matrix, as well as the targeted risk analysis, both of which are mandatory for each requirement, using this new flexible approach. This new approach, requires documentation and evidence, as well as a targeted risk analysis for each such customized control. The entity would also need to monitor and maintain evidence about each customized control's effectiveness. VigiOne's Assessment 360 enables customizable assessments, integrated asset register and incorporated Document/Evidence Library will facilitate and streamline this potentially complex process.

New Requirements for All Entities

The changes in v4.0 reflect changes in technology, the environment and security practice over the past four years, There are many new technical requirements, which will remain best practice until March 31st 2025, but which should be planned, implemented and tracked in the meantime. Some changes are exceedingly granular, but they are likely to require organizations carry out and maintain an asset and data inventory, as well as evaluating and perhaps updating their incident response plan. One of the new requirements that is effective immediately for any organization undergoing a v4.0 assessment is the documentation requirement for roles and responsibilities of the individuals in charge of each section's requirements, and making sure that they are assigned and understood. VigiOne's Asset Register, Assessment Tool and Task Management tools will considerably aid these processes.

Service Providers

There are 13 new requirements for TPSP (Third Party Service Providers), including a number of new ones only for "multi-tenant service providers". PCI DSS scope remains unchanged, the standards apply to "entities with environments where account data is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE [cardholder data environment]." Therefore the requirement apply to TPSPs as well. TPSPs can validate PCI DSS compliance to their customers either by an annual PCI DSS assessment, with evidence to customers that it meets the standards or by undergoing assessments from each customer upon request of the customer, again processes that are easily supported from VigiOne.

VigiOne and PCI DSS 4.0

A significant proportion of VigiTrust's customers already use VigiOne to manage compliance to PCI DSS 3.2.1. Many of them use it because they can manage compliance to multiple standards, national (e.g. NIST, Cyber Essentials), international (e..g. ISO/IEC 27001/27002, GDPR, ETSI) and industry specific standards (e.g. PCI DSS, UL) with the one system, a single program and even one set of controls. VigiOne's key components, outlined below, are integrated to provide the capability to prepare, validate and implement continuous compliance to PCI 4.0 across any complex and challenging environment, whether from the foundation of PCI DSS 3.2.1, or from alternative but aligned standards or indeed from "square one".

While VigiOne can and does provide a comprehensive GRC/IRM solution for organizations across multiple standards, VigiTrust has established a robust solution for PCI DSS compliance which utilizes VigiOne in three guises

1. A simple and straightforward tool that allows merchants (Stores, Hotels, Restaurants, Franchisees etc.) maintain, assess and report on compliance to the required controls on a continuous basis year in, year out.
2. A fully white labelled managed service offering for Third Party Service Providers (TSSPs) including Independent Sales Organizations, ISOs, Transaction processors, Payment gateways, Web hosting companies, Managed Security Services Providers (MSSPs), Third party marketing firms, Vendors, QSAs and other assessors, that allows them to manage continuous compliance in collaboration with or on behalf of their customers.
3. A fully white labelled PCI DSS Merchant Compliance Platform (MCP) for merchant aggregators such as Franchisors, Payment Services Providers, Acquiring Banks, Corporates and even industry groups.

VIGIONE FEATURES & FUNCTIONALITY for PCI DSS

• Integrated LMS (Learning Management System) for PCI DSS & Security Awareness Training with a portfolio of 200+ pre-packaged role-based modules. Each module has sections ranging from 1 min to 5 min in duration which can be mixed and matched. The system links awareness and understanding with policy implementation. Interactive, multilingual eLearning courses with testing and certification. eLearning tailored for multiple user types, technical and payment staff, program managers, senior executives, merchants and franchisees.
• Entity (Business Unit, Department, Vendor, Customer, Subsidiary, etc.) compliance assessment, scope determination, definition and clarification
• Gap analysis and prioritized remediation planning
• Continuous Self-Assessment, including supported and validated self-assessment
• Upload, collation and review of evidence documentation per assessment, requirement or control
• Create remediation plans to address non-compliance, assign tasks with clear deadlines to entities and individuals internally and externally. Track and report on progress.
• Production of reports including gap analysis, audits, standard specific documents (e.g. ROC & SAQ)
• Scheduling, reporting and results investigation of penetration testing and vulnerability scanning services (via 3rd party approved scanning and testing vendors)
• Integrated view of policy and procedure across an organization and a clear methodology for an "assessor" to track implementation, and if required, review local variations
• Collaborative approach to assessment and validation, to allow advisors and third party service providers, support end users in self-assessment or in the provision of responses and a evidence documentation
• Share and unified scorecards, dashboards and reporting for multiple standards
• A continuous, overarching view of compliance to data and information security compliance regulations, that ensures the compliance process is ongoing and not solely reliant on 3rd party involvement