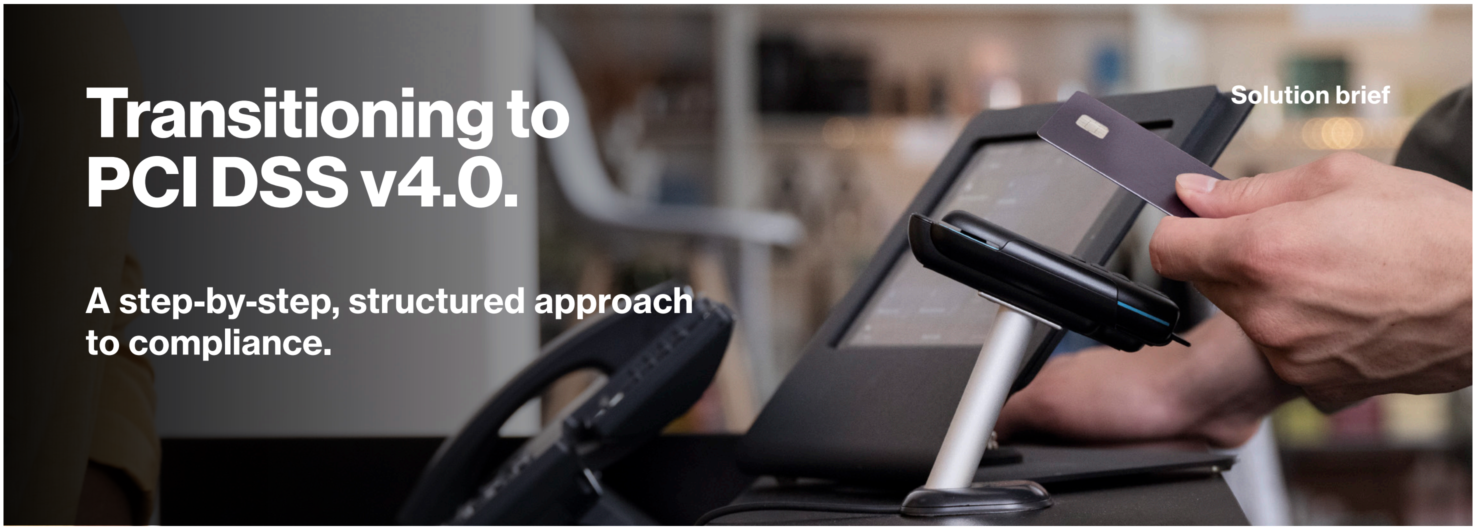

Solution brief

Transitioning to PCI DSS v4.0.

A step-by-step, structured approach to compliance.

In March, 2022 the Payment Card Industry Security Standards Council (PCI SSC) released version 4.0 of the PCI Data Security Standard (PCI DSS v4.0). This major release brings significant changes with compliance requirements, including how to validate and report on compliance. It will help organizations ensure that data security controls remain relevant and more effective in a shifting payment security landscape. It's the most significant update to the PCI DSS since its initial release in 2004.

PCI DSS v4.0 introduces major changes that include requirements for ongoing assessments along with enhanced validation methods. New procedures have evolved from a defined-only approach to include an objective-based, customized approach. Customizing security controls should be applied in a very structured way that delivers measurable and predictable outcomes.

Some organizations may experience unintended consequences from the design and implementation of their customized controls. It's critical to be aware of blind spots and cause-and-effect relationships between controls, control systems and the control environment.

Verizon now offers two services designed to help you navigate the transition to PCI DSS v4.0:

- Interpretation of PCI DSS v4.0
- PCI DSS v4.0 Resource Requirement Assessment

The sequence of these two services offers a structured roadmap, helping organizations understand what to focus on and correctly prioritize actions to reach important milestones. For those that don't have sufficiently high maturity with their security and compliance management processes, this approach helps to avoid chaos. Each service helps organizations become more proactive instead of reactive to the new compliance requirements.

Interpretation of PCI DSS v4.0

Interpreting PCI DSS v4.0 can be a complex endeavor. This service presents a methodology to translate PCI DSS v4.0 requirements to the development, design and processes of a project plan for your unique control environment. Verizon includes valuable data-driven insights from our esteemed Verizon Payment Security Report and Data Breach Investigations Report to provide a rich context for the interpretation of the requirements.

The service provides quality guidance on the following:

- Constructing a successful PCI DSS v4.0 Interpretation project
- Perspective on the scope of the PCI DSS v4.0 requirements – the quantity of changes
- Perspective on the magnitude of the PCI DSS v4.0 requirements: High-impact vs low-impact changes
- Control design and implementation
- Compliance validation changes
- Clarification on when to use the customized approach to controls

Methodology

The service is delivered in a series of up to three onsite or remote Workshops depending on your needs. Each Workshop includes between two and four hours of interactive discussions and includes a documented Workbook that contains the process framework with individual steps and milestones. The Workbook is designed to structure and facilitate conversations and includes a high-level walkthrough of the requirements with a focus on new and updated requirements. Interpreting the PCI DSS v4.0 consists of three components: (1) Kick-off Meeting; (2) Workshops; and (3) Final Project Meeting.

- **Kick-off Meeting:** Develop an initial view of your payment security program and develop the Project plan.
- **Workshop 1:** How to digest the PCI DSS v4.0 documentation – a recommended method
- **Workshop 2:** Interpreting the PCI DSS v4.0 requirements
- **Workshop 3:** Understanding the PCI DSS v4.0 compliance validation requirements
- **Project Review:** At the conclusion you'll have clarity and confidence about the soundness of your interpretation of the PCI DSS v4.0 requirements. And you'll have an accurate estimate of the scope of activities and a plan to achieve high-quality communication and readily identify resources needed to assign responsibilities and track progress.

PCI DSS v4.0 Resource Requirement Assessment

Payment Card Industry Data Security Standard (PCI DSS) v4.0 Resource Requirement Assessment provides an assessment of the amount of effort and the technical and operational level of change that will be required for your existing payment security program to achieve compliance with PCI DSS v4.0. Verizon's analysis can greatly assist executives with the complex process of resource and capacity planning for the required changes to their payment security programs.

Methodology

The PCI DSS v4.0 Resource Requirement Assessment consists of four components delivered over the course of about two weeks:

- Initially, Verizon will develop a view of your business processes, IT, and systems that store, process, and/or transmit Card Holder Data (CHD) subject to PCI DSS requirements.
- We then conduct Workshop interviews with your designated contacts on your security and compliance teams to gather operational and technical information needed to evaluate Customer CardHolder Data Environments (CDEs), connected system components, and existing controls and to determine the general level of PCI DSS compliance for each Customer CDE.
- Verizon conducts additional interviews with your designated operational and technical personnel to assess the level of change required for your current payment security program to achieve compliance with PCI DSS v4.0.
- Upon completion of these activities, Verizon provides a PCI DSS v4.0 Resource Requirement Assessment Report that identifies the level of change and estimated number of person work hours required for each CDE. Verizon will assign level of changes as: (1) No Change; (2) Documentation Only; (3) Configuration Change; (4) Network Architecture Change; (5) Business Process Change; or (6) Business Model Change.

Why Verizon

As an industry thought leader, we've written the book on PCI security compliance – literally. Since 2010, we've regularly published the acclaimed Verizon Payment Security Report (PSR), a report dedicated to payment security issues and the only one of its kind to offer unique insights into the current state of PCI DSS compliance.

Verizon has the most experienced and one of the largest PCI Security QSA teams in the world, and has conducted more than 19,000 security assessments for companies of all sizes, including many Fortune 500 and multinational organizations.

We keep up with the rapidly changing nature of cyber threats by analyzing more than 1 million security events every day at our global network operations centers and security operations centers. And, for over a decade, we've offered our knowledge through thought leadership with publications such as the Verizon Data Breach Investigations Report.

Learn more:

For more information on the Verizon PCI DSS Assessment, contact your account representative or visit: https://www.verizon.com/business/products/security/cyber-risk-management/governance-risk-compliance/payment-card-industry-advisory-service/.

To read the latest Payment Security Report, go to: https://www.verizon.com/business/resources/reports/payment-security-report/.

To read our 2021 Payment Security Report PCI DSS v4.0 insights white paper, go to: https://www.verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf.

For more information about the other security solutions and services we offer, visit: https://www.verizon.com/ business/products/security/.

verizon✓