PCI DSS Assessment

Solution brief

Keeping PCI DSS compliance simple and effective.

Continuous improvement of a sustainable and effective data security compliance program is a complex business problem that many organizations find challenging to navigate. How do you choose what to prioritize and focus on? How do you choose your goals and objectives? How do you unravel requirements and remove constraints?

Verizon helps countless organizations progress with sound security program innovation, practical frameworks and novel advice. This is increasingly important when navigating the requirements with one of the most significant changes in the PCI DSS to date—the tenth release of the Payment Card Industry Data Security Standard (PCI DSS), v4.0.

To help give you and your customers better peace of mind, PCI DSS was designed to help protect payment data from the point of purchase onward. But even among organizations that achieve PCI DSS compliance, many struggle to sustain it even in the short term. The 2020 Verizon Payment Security Report identifies that fewer than one third (27.9%) of surveyed organizations achieved 100% compliance during their interim compliance validation. This improved to nearly half (43.4%) in 2020 with focus and Verizon's security management toolbox set of methodologies.

As an expert in PCI security standards, Verizon knows that compliance assessments should be more than a long checklist of requirements to meet. With our consulting and compliance services, we'll help you build out your security strategy to not only address PCI DSS compliance requirements, but improve your risk profile.

Don't take shortcuts with your security.

The overall goal of PCI DSS compliance should be to develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing protection of payment card data in a consistent, predictable and sustainable manner. To achieve this goal, the PCI DSS compliance program should be integrated with—and supported by—a business model, strategy, security operating model, and additional security frameworks.

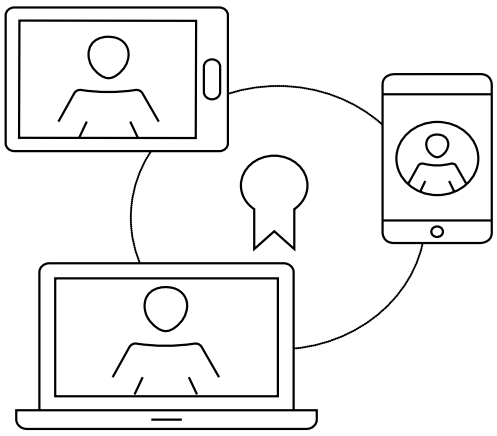
In a complex operating environment, however, the process of safeguarding valuable data can be overwhelming at times.

PCI DSS v4.0

The latest update to the flagship PCI DSS will help organizations ensure that data security controls remain relevant and more effective in a shifting landscape.

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

You may feel overwhelmed by the quantity and complexity of information being made available on the topic of PCI DSS v4.0. In order to simplify what you need to know, Verizon has published the definitive guide to PCI DSS v4.0 compliance.

We can help you achieve a sustainable control environment by simplifying your compliance obligations and clarifying requirements. By supporting the development, implementation and improvement of efficient control processes, the outcome should be the predictable performance of your data security program and the ability to drive continuous improvement.

Our long-standing relationships with all of the leading payment card brands means that we have a clear understanding of their compliance expectations. With a security team of over 600 consultants in 30 countries and one of the largest teams of PCI Qualified Security Assessors located around the globe, we can perform PCI DSS reviews in a variety of languages at any of your operating locations. The service at all of those locations can be managed from one central hub—offering you a single view into your control environment.

We help clear the fog and answer key questions to improve your security compliance management capability, such as:

1. Are you presently attaining your security and compliance goals?
2. What is keeping your strategy and program from progressing?
3. What is keeping your control environment from reaching its full potential?
4. How do you choose your goals and objectives?
5. Do you know where to focus your efforts?
6. How do you choose what to prioritize and what to spend time on?
7. How prepared are you and your team to meet the new PCI DSS v4.0 requirements?
8. How do you unravel requirements and remove constraints?
9. What exactly are the constraining factors? Everyone on your team has an opinion, but which is right?
10. How do you sort out the important few constraints from the trivial many?

With one of the largest global teams of Qualified Security Assessors (QSAs), Verizon has a firm grasp on what it takes to achieve and maintain PCI DSS compliance.

Planning

- Appropriately validate the scope of people, processes, technologies and locations

Execution

- Ensure a timely kick-off of assessment activities
- Conduct interviews, collect required documentation and evidence of compliance
- Make observations and provide detailed progress tracking

Remediation

- Clarify communication of findings along with remediation guidance
- Provide decision support guidance on remediation options
- Provide post-remediation validation

Review and close-out

- Conduct an internal quality assurance review of the report deliverables
- Deliver and review report and recommendations

Stakeholder engagement

- Help identify and communicate with the key personnel involved in your data security strategy and compliance program
- Clarify the objectives, priorities, capabilities and capacity management to support associated security compliance projects

Strategic alignment

Support aligning your organization's structure, resources, decisions and actions with your business environment and data security strategy to better enable the achievement of your strategic goals.

By relying on us for your PCI security assessments, you'll have peace of mind knowing your payment data security measures are being analyzed and validated by an experienced security advisor.

Why Verizon

As an industry thought leader, we've written the book on PCI DSS 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/.

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

verizon