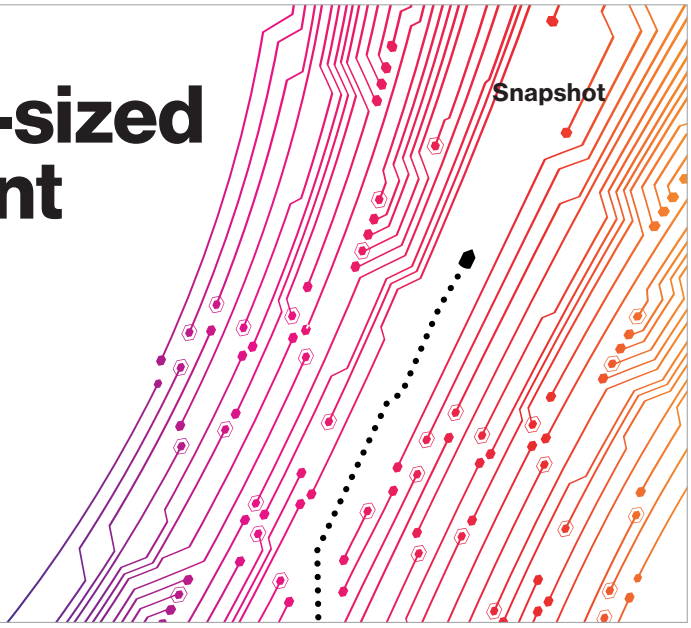
Small- and medium-sized businesses: Payment security in the era of PCI DSS v4.0

Snapshot



Small- and medium-sized businesses (SMBs) experience challenging security constraints because tight financial and staffing limitations can make it difficult to keep pace with compliance requirements. Some SMBs overcome these capacity constraints by strategizing ways to simplify complexity; they increase proficiency by focusing on what matters most.

They continue to be challenged though, as threat actors develop new capabilities to exploit weaknesses within payments systems and processes. Ransomware remains a pernicious threat—one that SMBs were particularly challenged with in 2021, according to the 2022 Verizon Data Breach Investigations Report (DBIR).[1]

In response to these and other payment security changes, the Payment Card Industry Security Standards Council (PCI SSC) instituted a major rewrite of the PCI Data Security Standard (DSS) in v4.0—to better protect data, create flexible security methods and effectively navigate complex compliance environments. It's the most significant update to the DSS since its initial release in 2004.

The PCI DSS is a set of security standards that the card brands (Visa, Mastercard, American Express, Discover and JCB) created to ensure that businesses storing, processing or transmitting payment card data do so within a secured environment that meets a minimum baseline of security control requirements.

SMBs need to adapt to the new PCI DSS v4.0 Standard requirements just as quickly as large businesses, because the PCI DSS applies to all organizations. They need to strictly implement security defenses to avoid becoming breach victims. Additionally, they should have a management strategy—a toolbox with clear instructions for building PCI DSS v4.0 success.

PCI DSS v4.0 still has the six familiar Control Objectives and 12 Key Requirements introduced in 2006. The new version reflects the PCI SCC goals for evolving objectives and requirements.

What to do to avoid a payment card data breach

1. **Use multifactor authentication**
2. **Do not reuse or share passwords**
3. **Use a password keeper/generator app**
4. **Be sure to change the default credentials of the point-of-sale (POS) controller or other hardware/software**
5. **Ensure that you install software updates promptly so that vulnerabilities can be patched**
6. **Work with your vendors to be sure that you are as secure as you can be, and that they are following these same basic guidelines**
7. **Keep a consistent schedule with regard to backups and be sure to maintain offline backups—meaning that they are not on a device connected to a computer**
8. **Ensure that the built-in firewall is switched on for user devices such as laptops and desktops ("on" may not be default)**
9. **Use antivirus software for all your devices. Smartphones, tablets and credit card swipers are just as important as laptops and computers. It won't catch everything, but it will help**
10. **Do not click on anything in an unsolicited email or text message**
11. **Set up an out-of-band method for verifying unusual requests for data or payments**
12. **Make sure the computer used for financial transactions is not used for other purposes, such as social media or email**
13. **Use email services that incorporate phishing and pretexting defenses, and use a web browser that warns you when a website may be spoofed[2]**

verizon

The two most significant updates in PCI DSS v4.0 are increased emphasis on continuous compliance and a new customized approach for compliance control design and validation. Enhanced validation methods and procedures have evolved from a defined-only approach to also include an objective-based, customized-approach option.

Payment card data is one of the most sought-after data types by external and internal threat actors, because it's one of the easiest types to monetize. Even within these highly sensitive environments, organizations are slow to implement strategies that result in sustainable control effectiveness.

The defined approach simply means that organizations follow the traditional requirements and testing procedures, as written in the PCI DSS. The new customized approach of validating controls allows organizations to follow a tailored process, where they can custom-design security controls or adopt other controls outside the list of defined controls. This is an outcome-based approach rather than a must-implement-based approach. All customized controls must still meet the stated security objective of the requirement.

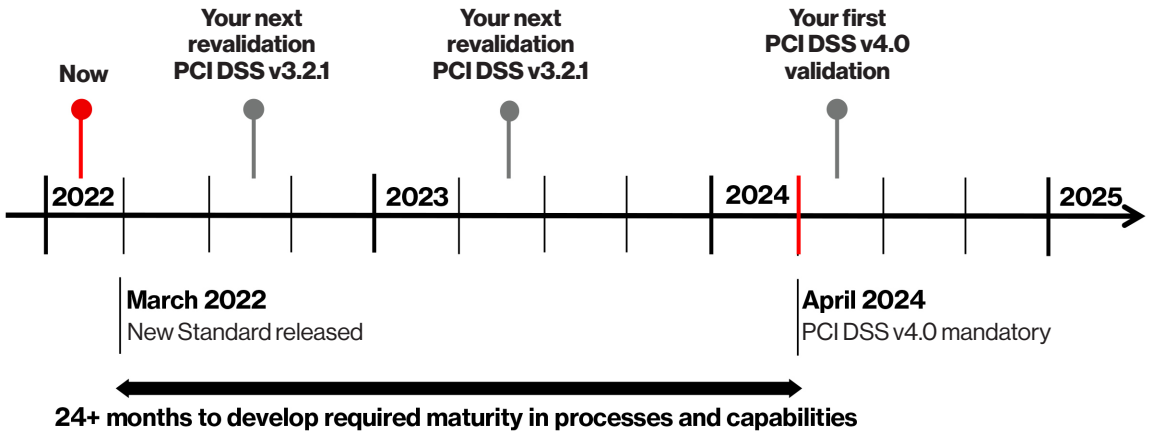
Compliance with v4.0 will not be required until March 2024. PCI DSS v3.2.1 will be active for 18 months after all PCI DSS v4.0 materials are released. When this transition period ends, PCI DSS v3.2.1 will be retired, and PCI DSS v4.0 will become the only active version. In addition to the 18-month period when PCI DSS v3.2.1 and PCI DSS v4.0 will both be active, there will be an extra period of time for phasing in new requirements that are identified as "future dated" in PCI DSS v4.0. Organizations working to upgrade their compliance environments may think they have ample time to resituate their controls. But with significant changes, including the customized approach option, they can't start to prepare soon enough.[3]

A Verizon toolbox can help SMBs transition to v4.0.

Many different approaches exist for designing the management of a compliance program. The key question is: Which is the most effective and efficient? Verizon explained a method for reaching that goal in the "2021 Payment Security Report insights: PCI DSS v4.0" white paper.[4]

Verizon has an exceptional track record on helping clients implement sustainable payment security frameworks. The recently released 2022 Payment Security Report (PSR) is about preparing to successfully negotiate PCI DSS v4.0 – finding the tools you'll need to identify and solve potential challenges and choosing the best path forward to determine and accomplish your goals. This edition explores a toolbox of management methods, models and frameworks to help your organization simplify the complexities of payment security while adapting to the new requirements.

PCI DSS v4.0



Verizon services

Verizon also offers many services designed to help you navigate the transition to PCI DSS v4.0. This sequence of services provides a structured roadmap to achieving compliance. It helps organizations avoid uncertainty—for those that don't have sufficiently high maturity with their security and compliance management processes. Each service helps organizations become more proactive instead of reactive to the new compliance requirements.

Service 1: Interpretation of PCI DSS v4.0
This service is designed to help clients develop a structured approach to understanding the PCI DSS. It includes a framework to help clients communicate the Standard to their organizations across internal teams including:

- Front-line staff
- Risk and compliance teams
- Internal audit teams and senior management
- External parties and vendors

It includes presentations and guidance on the:

Why: Goals and objectives, outcomes and expectations of PCI DSS v4.0

How: Guidance (hardcopy workbooks or support for developing e-learning/online)

Who: Targeted messaging for each of the stakeholder groups (internal and external)

When: Recommendations on the steps and order of when to start each communication and its duration

Service 2: PCI DSS v4.0 Resource Requirement Assessment
The Resource Requirement Assessment provides an integrated analysis of the scope, requirements and constraints. The analysis focuses on: (1) Formalization, (2) Process, (3) Configuration, (4) Architecture, (5) Culture, (6) Business model change. The service is delivered in about two weeks in a series of interviews with security and compliance teams, and allows the customer to calculate work hours required to achieve compliance with PCI DSS v4.0 objectives.

Service 3: PCI DSS v4.0 Gap Assessment
The Gap Assessment pinpoints the exact difference (gap) between your current PCI DSS v3.2.1 and PCI DSS v4.0 requirements (present vs future reality). It results in a gap assessment report that details the PCI DSS requirements and controls that need remediation, and a focus on the type and quality of evidence needed to be submitted during the formal compliance validation.

Service 4: PCI DSS v4.0 Preassessment
The PCI DSS v4.0 Preassessment reviews a sample of compliance evidence and assessment preparedness to determine readiness for the formal assessment. It checks the readiness of security and compliance teams to participate in the formal validation assessment, and includes a last-minute check to confirm the adequacy of evidence of compliance, pinpointing any adjustments or corrections needed in advance of the formal assessment.

Service 5: Formal PCI DSS v4.0 Compliance Validation Assessment
This assessment is the formal, annual compliance validation against all applicable PCI DSS v4.0 requirements. It results in a Report on Compliance (ROC) and Attestation on Compliance (AOC).

Ten significant PCI DSS v4.0 requirement changes

- Disk- or partition-level encryption is no longer enough
- An anti-phishing solution is required
- A web application firewall (WAF) is required
- Multifactor authentication (MFA) is required
- A cryptographic key is required for stored hash values
- Certificates protecting cardholder data (CHD) need to be signed by a valid certificate authority (CA)
- Enforced integrity controls for payment page scripts are required
- No hardcoded passwords for applications
- Authenticated vulnerability scans are required
- Application/System account passwords must expire

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, 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 one of the largest PCI Security Qualified Security Assessor (QSA) teams in the world with deep experience 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 cyberthreats 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 verizon.com/paymentsecurityreport

Read the latest Payment Security Report: verizon.com/business/resources/reports/payment-security-report/

Read our 2021 Payment Security Report PCI DSS v4.0 insights white paper: 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 verizon.com/business/products/security/

verizon

1 Verizon 2022 Data Breach Investigation Report, 2022. https://www.verizon.com/business/resources/reports/dbir/

2 Verizon Data Breach Investigation Report, 2022. https://www.verizon.com/business/resources/reports/dbir/

3 Verizon 2022 Payment Security Report, 2022. verizon.com/paymentsecurityreport

4 Verizon 2021 Payment Security Report insights: PCI DSS v4.0, 2021. https://www.verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf/