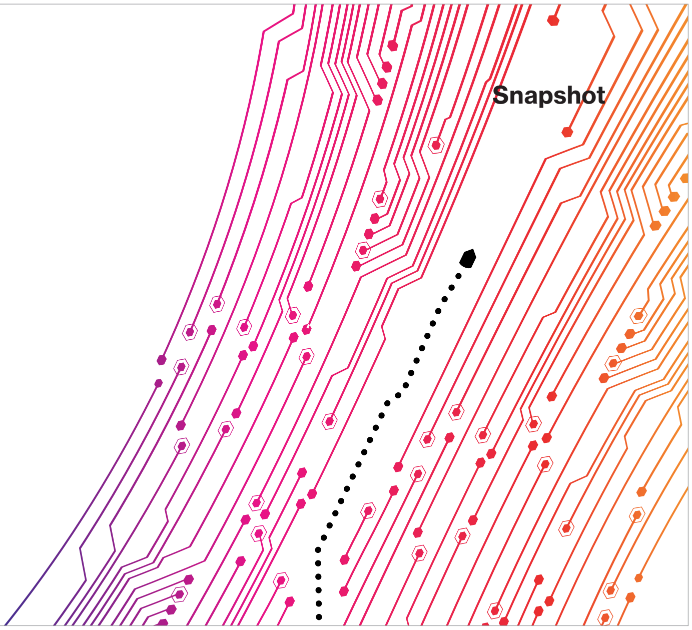


Public Sector: Payment security in the era of PCI DSS v4.0

The Public Sector in the United States has experienced significant payment security challenges in the last several years that are requiring new protocols and innovative solutions. Contactless payments, the growth of online commerce, cloud technologies, digital transformation, and the increase in the number of home-based and hybrid workers are key drivers prompting new payment industry norms in the public sector. Meanwhile, the capabilities of threat actors continue to evolve and escalate, enabling the skillful exploitation of existing and emerging threats and weaknesses within government payment systems and processes. System intrusion and ransomware continue to be particularly pernicious threats for public sector agencies, according to the 2022 Verizon Data Breach Investigations Report (DBIR).[1]

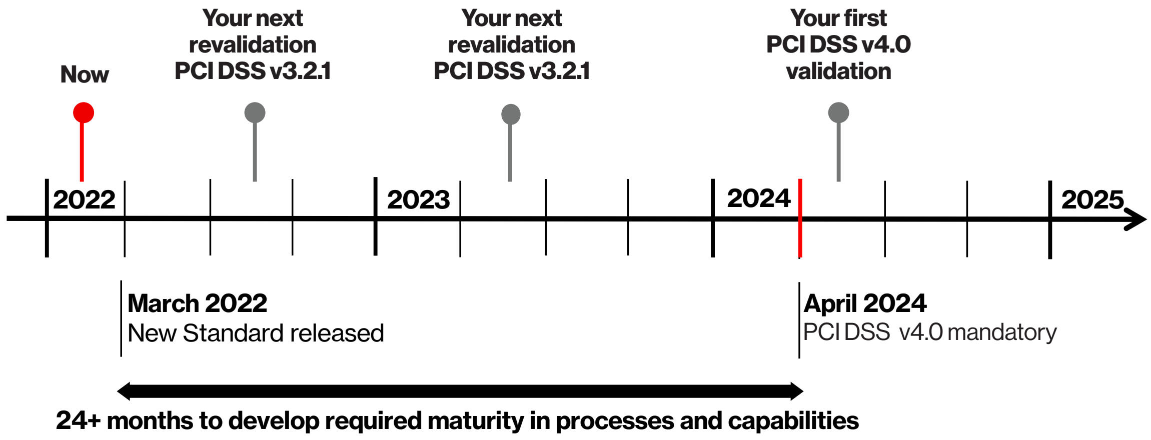
In response to these evolving threats and significant payment changes, the Payment Card Industry Security Standards Council (PCI SSC) instituted a major rewrite of the PCI Data Security Standard (DSS), v4.0, to help organizations better protect data, create flexible security methods and effectively navigate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

The Public Sector, the government segment of the economy, is being forced to pivot and adapt to these changes just as quickly as the private sector because the challenges and security requirements are the same. The requirements are set by the PCI DSS. While PCI DSS v4.0 doesn't alter the fundamental structure of the PCI Standard (it still has the six familiar Control Objectives and 12 Key Requirements introduced in 2006), the new version reflects the Council's goals for evolving objectives and requirements. The two most significant updates in PCI DSS v4.0 are continuous compliance and customized controls and control environments. 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 current (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 of the list of defined controls. This new approach is outcome-based rather than a must-implement-based approach. All customized controls must still meet the stated security objective of the requirement.

PCI DSS v4.0 timeline


Now
Your next revalidation PCI DSS v3.2.1
Your next revalidation PCI DSS v3.2.1
Your first PCI DSS v4.0 validation
2022
2023
2024
2025
March 2022
New Standard released
April 2024
PCI DSS v4.0 mandatory
24+ months to develop required maturity in processes and capabilities

Compliance with PCI DSS 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. Whether choosing a defined or customized approach, all government entities must take the necessary steps to comply with PCI DSS v4.0 by the 2024 deadline.[2]

Verizon’s toolbox can help agencies transition to PCI DSS v4.0.

Many different approaches exist to designing the management of a compliance program. The key question is: “Which is the most effective and efficient?” Verizon has an exceptional track record on helping clients implement sustainable payment security frameworks.

The 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 of the PSR 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. This special set of management tools is designed to harness the combined capabilities within public sector agencies and establish better management of PCI security programs by helping plan, design, navigate and fix your agency on its journey through changing waters.

Social engineering and ransomware—growing, persistent problems

A recent 10-month investigation by the U.S. Senate Homeland Security Committee found that the U.S. government is failing to effectively track ransomware incidents in both the public and private sector.[3] Due to insufficient reporting, only about one-quarter of ransomware attacks are accounted for, according to the Cybersecurity and Infrastructure Security Agency (CISA). Meanwhile, from 2021 to 2022, the number of ransomware breaches doubled. The rapid rate of increase exceeded in one year the rate of the last five years combined, according to the 2022 DBIR.[4] Ransomware “is present in almost 70% of malware breaches this year,” states the DBIR. The motive? Some 89% of ransomware breaches were financially motivated; 11% were espionage. Organized crime was responsible for about four in five of those breaches. Out of the DBIR’s 2,792 recorded incidents (537 with confirmed data disclosures), 81% were System Intrusion, Miscellaneous Errors and Basic Web Application attacks. State and Local Government Plus Education (SLED) is particularly vulnerable to attacks because SLED often operates on limited resources. With a notable uptick in security breaches, it’s imperative to ask the critical question: “What steps should the public sector start taking to prepare for the transition to PCI DSS v4.0?”

Verizon services

Verizon offers many services designed to help you focus on and navigate the transition to PCI DSS v4.0. This sequence of services offers 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 the 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 Business Impact Analysis 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
- 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) must be signed by a valid certificate authority (CA)
- Enforcement of integrity controls for payment page scripts is required
- Hardcoded passwords for applications are not permitted
- 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. With a large PCI Security Quality Security Assessor (QSA) team, we have 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 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. verizon.com/business/resources/reports/dbir/

[2] Verizon 2022 Payment Security Report, 2022. verizon.com/paymentsecurityreport

[3] Marks, Joseph and Schaffer, Aaron, "The government's still mostly in the dark on ransomware," The Washington Post, May 24, 2022. https://www.washingtonpost.com/politics/2022/05/24/governments-still-mostly-dark-ransomware/

[4] Verizon 2022 Data Breach Investigation Report, 2022. verizon.com/business/resources/reports/dbir/