S|3 SPECIALIZED SECURITY SERVICES

READY OR NOT: HERE COMES PCI 4.0

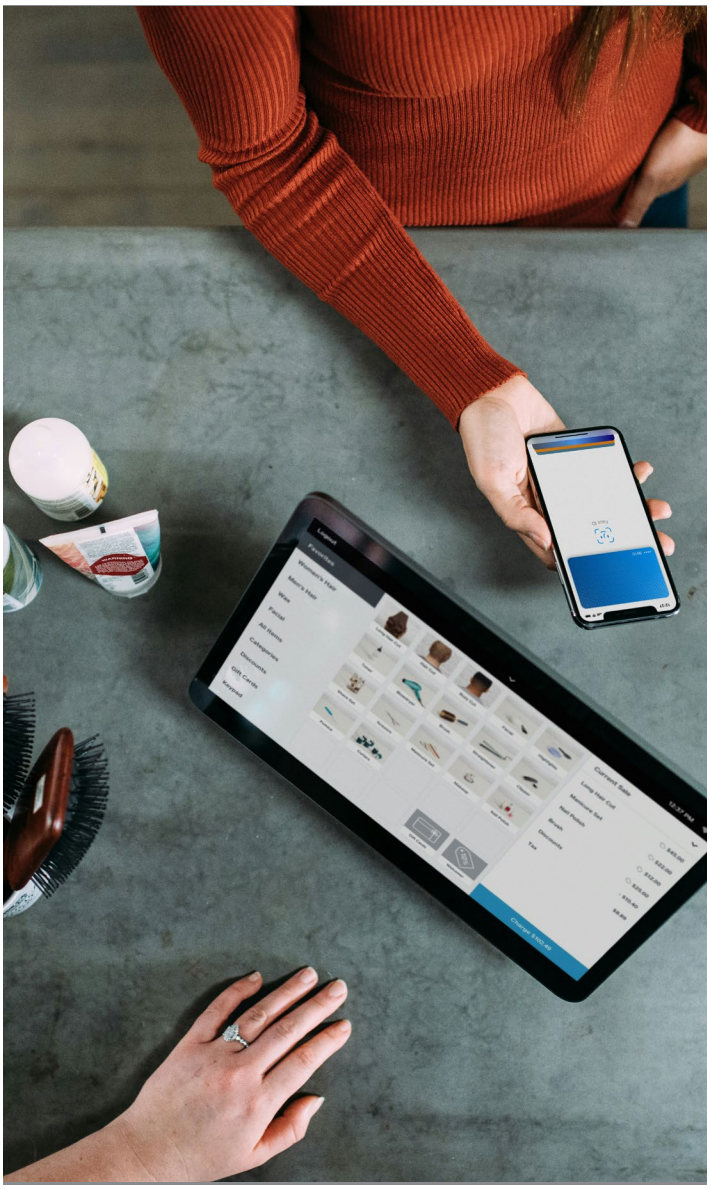
Navigating the Next Phase in Payment Security

NAVIGATING THE NEXT PHASE IN PAYMENT SECURITY

The Payment Card Industry Security Standards Council (PCI SSC) is set to roll out PCI Data Security Standard version 4.0 (PCI 4.0) on March 31 with an overarching goal of enhancing industry security practices in response to evolving cyber threats.

For the last 25 years, S3 Security experts have worked side-by-side with clients to help maintain compliance and protect against cyber attacks. We've been a trusted partner for payment card security including Visa, Master Card and American Express since 2001, and a QSA/ASV firm since 2004 when the Payment Card Industry Security Standards Council was first established.

In short, S3 Security is committed to providing straightforward guidance for proactive cyber security programs that support business goals, build trust and deliver peace of mind. So, this white paper is just the first step in helping you in navigate changes in the New PCI 4.0 Data Security Standard.



KEY OBJECTIVES OF PCI DSS 4.0

1. **Adaptative Security Practices**

   Continue to meet the security needs of the payment industry through security practices that evolve as threats change. This includes embracing multi-factor authentication, updating password/passphrase requirements and addressing emerging threats involving e-commerce and phishing.

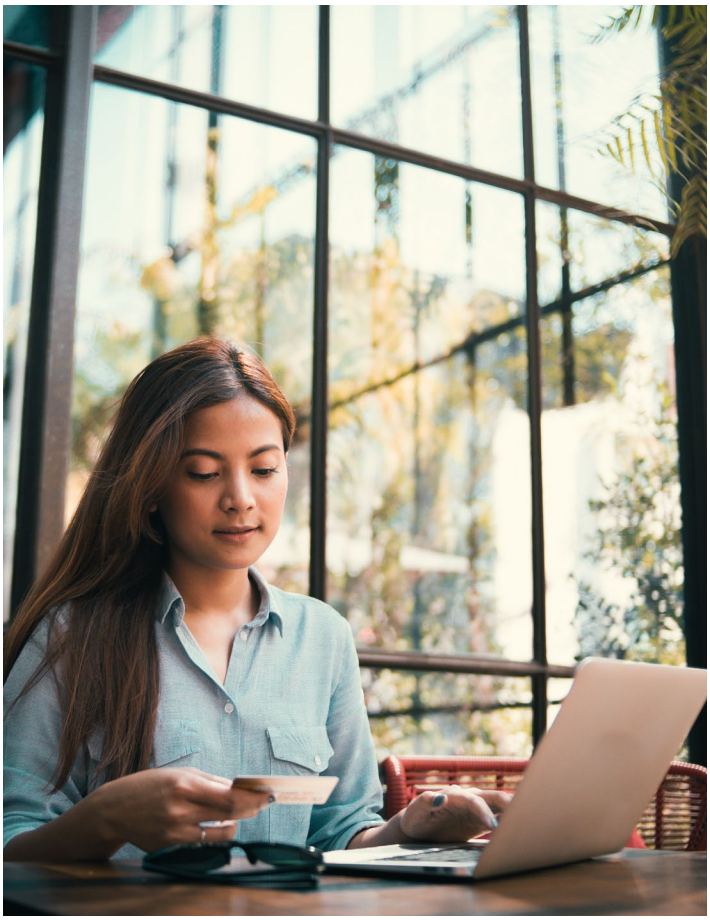
2. **Adaptative Security Practices**

   Recognize cybersecurity as an ongoing commitment. Clearly defined roles and responsibilities, comprehensive guidance, integrated risk analysis and new reporting options ensure a proactive approach to safeguarding payment data.

3. **Enhanced Flexibility for Innovation**

   PCI 4.0 fosters adaptability by increasing flexibility to achieve security objectives. This includes supporting payment technology innovation with features like targeted risk analysis which enables organizations to establish frequencies for specific activities.

Moreover, PCI 4.0 allows for a customized approach to fulfill requirement objectives, accommodating organizations leveraging innovative methods. It also permits group, shared and generic accounts to provide additional flexibility in meeting compliance requirements.



CHANGES EFFECTIVE MARCH 31, 2024

- **Significant Change Guidance**
  Clarification on what constitutes a significant change for PCI.

- **Roles and Responsibilities**
  Expanded documentation of roles and responsibilities for performing activities related to all 12 requirements.

- **Scope Confirmation**
  Entities must document and confirm PCI DSS scope at least every 12 months and upon significant change to the in-scope environment.

- **Timeframe Expectations**
  Streamlined timeframes for more explicit compliance expectations. Changes now reflect the set number of days (1 day vs. daily, 7 days vs. weekly, 30 days vs. monthly, 90 days vs. quarterly, etc.)

- **PCI 4.0 Templates Increased Length**
  Lengthier templates provide a comprehensive documentation framework, and these templates can sometimes be twice the length of PCI 3.2.1 counterparts.

- **Target Risk Assessments (TRA)**
  New TRAs are required for all PCI requirements where entities define the frequency of control activities (nine new requirements).

- **Build/Maintain a Secure Network and Systems**
  Replaced “firewalls” and “routers” with “network security controls” for a broader security technology scope.

- **Third-Party Service Providers (TPSP)**
  New requirements for TPSP to enhance transparency and support customers’ requests to provide PCI DSS compliance status and information about PCI DSS requirements that are the responsibility of the TPSP (12.8.4 & 12.8.5).

CHALLENGES AND OPPORTUNITIES

PCI 4.0 challenges organizations to enhance their security posture. Mature IT security environments have a head start, but others must upgrade to meet the new requirements.

Decisions for changes effective March 31, 2025, need careful consideration, as budgetary allocations for 2024 may be necessary for a seamless transition. For example, increasing the password length to 12 may require the replacement of applications that handle credit card information—processing, storing, or transmitting it—to comply with this requirement.

PREPARING YOUR ORGANIZATION FOR PCI 4.0 COMPLIANCE

Review & Discuss PCI DSS 4.0

- Download a copy of the applicable template vyour organization will file along with related transition documents.
- Read and review with your IT, Security and Business teams.
- Increase organizational awareness of changes that require time, talent and budgets to remain compliant.
- Evaluate vulnerability scans to address vulnerabilities as soon as possible.
- Consult with a QSA for guidance or a more detailed walkthrough of requirements.

Strategize Your Transition

- Consider your scope and inventory new projects in development that may affect that scope.
- Schedule a PCI 4.0 Gap Assessment as soon as possible.
- Evaluate and consider whether you will take a defined or customized approach.
- Identify your risk assessment framework.
- Establish your internal implementation timeline and assign projects to appropriate teams.

PREPAREDNESS IS POWER

PCI 4.0 is fast approaching and will become mandatory within a short timeframe. If your organization falls under the compliance mandate, it's crucial to plan proactively and take action to meet the requirements set for March 31, 2024, while gearing up for subsequent changes scheduled for March 31, 2025.

These changes will impact how you do business – and may take significant effort – but the payoff goes far beyond a stamp of approval.

PCI 4.0 is not just a mandate; it's an opportunity to bolster your organization's security infrastructure. Partner with us to seamlessly transition into the future of payment security, ensuring you're compliant and resilient in the face of evolving threats.

GET 4.0-READY WITH CUSTOMIZED GUIDANCE FROM S3 SECURITY

S3SECURITY.COM | 972-378-5554

Wherever you are in your compliance journey, S3 Security is your trusted partner for PCI DSS. We've helped our clients progress through previous updates – and we'll help guide you through all these changes, too.

We not only understand the challenges you face, but that one of the greatest benefits of compliance is professional peace-of-mind. So, whether PCI compliance is a business obligation or part of your broader cyber security strategy, our goal is to enhance your organizational efficiency, security and profitability for the long haul.

Contact us today and let our QSAs walk you through new requirements, updates to controls, testing procedure guidance and reporting. Learn how PCI DSS 4.0 can mature your security program by addressing evolving payment security risks, promoting security as a continuous process, and supporting payment technology innovation.