Get Prepared For PCI-DSS V4.0

How To Approach

THE BIGGEST

Compliance Shakeup in a Decade

MEGAPLANIT | WHITE PAPER

Contents

Executive Summary

The PCI DSS standard is largely responsible for dictating the way organizations all over the world approach cybersecurity and the protection of credit card data. As V4.0 of the standard approaches, organizations should aim to identify and plan updates for the aspects of their security and compliance programs that are most likely to be affected.

A lot of information about PCI DSS V4.0 is already available, and it's shaping up to be the most significant update of the last decade. This white paper will cover everything organizations need to know about PCI DSS v4.0, including what is likely to change, when it will come into effect, and how they can prepare in advance.

Key Learning Points

1. PCI DSS v4.0 is set for release in late 2020 or early 2021. The current version 3.2.1 will remain valid for approximately 12 – 18 months following the release of v4.0 to give organizations a fair opportunity to make any necessary updates to their security and compliance programs.

2. At least seven significant changes to the PCI DSS standard are coming in v4.0. These include updates to the way Cardholder Data Environments (CDEs) are scoped, broader encryption requirements, and a demand for more stringent risk assessments and security awareness training.

3. A huge change in v4.0 is the move to "Outcome Orientation", which will see all 12 requirements reworded to focus on security outcomes instead of specific requirements. In addition to the traditional Defined Implementation approach, organizations will have the option to demonstrate how their security protocols meet the intent of each requirement instead of being forced down a specific security route.

4. Following the release of the RFC Process Guide in February 2019, the PCI Security Standards Council is taking a more formal approach to RFC for PCI DSS v4.0. One final RFC round will be open to all stakeholders from December 2019 – January 2020, and all feedback will be considered by the Council.

The World's #1 Compliance Standard

Developed as a mechanism to ensure merchants and service providers were processing, transmitting, and storing payment card details securely, the Payment Card Industry Data Security Standard (PCI DSS) has become much more than that.

Since Cardholder Data (CHD) is one of the most sensitive and important digital assets that many organizations hold, PCI DSS has often become the lens through which they see cybersecurity as a whole. For this reason — and the fact that it applies to more organizations globally than any other security standard — PCI DSS is arguably the single most important compliance standard.

So when a new version of the standard is announced, organizations across all industries and geographic locations naturally sit up and take notice. Changes to the standard 12 requirements could potentially cost organizations a lot of money — particularly if they are found to be non-compliant — so the stakes are high.

The Biggest Update in Years

PCI DSS v.4.0 is the next major iteration in the standard's 15-year history. By the time v4.0 is live, at least seven years will have passed since the last major update — v3.0 — was released in 2013. While there have been three sets of minor revisions in the intervening years, v4.0 will constitute a much greater reform of the standard than the community has seen in a long time.

In fact, if the comments made by members of the PCI Security Standards Council are accurate, v4.0 may well constitute the biggest PCI DSS shakeup since the first version was launched in 2004.

And since many organizations' security programs are heavily informed by PCI DSS compliance requirements, it's important for them to understand as early as possible what the new version will require.

After reading this paper, you'll know:

- When PCI DSS v4.0 is expected to launch, and why a new release of PCI DSS is needed.
- How v4.0 is expected to change PCI DSS, and what organizations will need to do to stay compliant.
- Why "Outcome Orientation" will change the way organizations evidence PCI DSS compliance.
- What the new Request for Comments (RFC) process looks like, and how to get involved.
- How to prepare for v4.0, and why MegaplanIT is the ideal compliance partner for your organization.

PCI DSS v4.0: What to Expect

Exact details about what will be different in PCI DSS v4.0 are still forthcoming. The results and alterations from two more Request for Comments (RFC) rounds are yet to be seen, and it's entirely reasonable to expect further updates. With that said, fundamental revelations about the purpose and nature of the changes that we can expect to see in v4.0 are known, even if the precise wording is not yet set in stone.

When Will PCI DSS v4.0 be Released?

While the PCI Security Standards Council has not yet set a hard launch date, the v4.0 standard is expected to be published in late 2020 at the earliest.

As with previous updates, the existing version 3.2.1 will remain valid for a period of time to give organizations a fair opportunity to make any changes needed to comply with v4.0. Based on the experience of past PCI DSS updates, expect 3.2.1 to remain valid for approximately 12 – 18 months.

Why is a New Version Needed?

There are two primary reasons why a new PCI DSS version is needed:

1. Changes to the payment landscape

In recent years, the payment environments, technologies, and methodologies used by organizations have evolved significantly. While the standard has always aimed to be "technology-neutral", major new technological and procedural advancements such as cloud hosting, SaaS, and ApplePay have fundamentally changed the way in which payments are made. These changes are beyond what could reasonably be handled in a minor update, which is a major reason why the PCI Security Standards Council decided on a full new release.

2. Lack of uniformity in payment and security protocols

While the goal of security is always the same, there is no single "correct" path to achieve it. As the manner in which organizations have chosen to set up their payment systems and security has evolved, it has become less appropriate to assess every organization in the same way.

In light of this, the PCI Security Standards Council decided that the new version of the PCI DSS standard would make it possible for organizations to demonstrate their adherence to the principles of the standard (i.e., ensuring card data security and privacy) without having to achieve them in a specific, prescribed way.

What's Changing in v4.0?

The first thing to understand about v4.0 of the PCI DSS standard is that the 12 core requirements will remain essentially the same. In the words of an official statement on the PCI Security Standards Council blog:

"The 12 core requirements will not fundamentally change in PCI DSS version 4.0. Updates will be made to improve security and provide more flexibility for meeting security objectives."[1]

However, while the intent of the standard and its 12 core requirements will remain as-is, based on announcements so far there will be some significant alterations to PCI DSS as a whole. Specifically, the Council has announced four overarching objectives for v4.0:

1. Ensure the standard continues to meet the security needs of the payments industry.
2. Add flexibility and support for additional methodologies to achieve security.
3. Promote security as a continuous process.
4. Enhance validation methods and procedures.

In light of these objectives — and the new payment industry trends mentioned earlier — a number of specific updates from v4.0 have already been announced.

v4.0 Specific Updates

As of November 2019, seven specific updates have been announced for PCI DSS v4.0. Again, while the specific nature of changes is not yet certain, a great deal is already known about these updates.

1. More Stringent Scope Validation

Determining scope is a huge part of PCI DSS, so it's no surprise that v4.0 will provide further clarity on requirements. Based on what's been announced so far, increased testing and documentation will be required from organizations and Qualified Security Assessors (QSAs) to ensure that scoping of the Cardholder Data Environment (CDE) is accurate and complete. There will also be new processes to periodically validate CDE scope.

2. Best Practice Authentication

As has been expected for some time, v4.0 of PCI DSS will allow organizations greater flexibility in the use of authentication techniques and solutions within the CDE.

Why is this needed? In some areas, v3.2.1 includes specific authentication requirements that no longer align with industry best practice. For example, right now the standard demands password changes every 90 days, while the most recent guidance from NIST (and many industry experts) suggests that it is more secure to use longer passwords that are changed less frequently. To reflect this, expect to see less prescriptive language used in v4.0 to enable organizations to stay in line with the latest industry best practice, rather than being held to specific, outdated requirements.

While they have not been announced yet, it's likely that we'll also see changes to multi-factor authentication (MFA) requirements in v4.0.

3. Cardholder Data (CHD) Encryption

In v3.2.1, organizations are responsible for ensuring CHD is encrypted whenever it is transmitted between public networks. In v4.0, this requirement may be expanded to include all transmissions of CHD — even those within an organization's secure, private networks.

5. Enhanced Security Awareness Training

Similar to risk assessments, many organizations have considered security awareness training to be primarily a checkbox-style requirement. For PCI DSS v4.0, the requirement will be expanded to mandate the inclusion of information on current cyber threats such as phishing and social engineering.

6. Recognition of New Technologies

While PCI DSS has always aimed to be a technology-neutral standard, the Council has noted that updates are needed to reflect the significant technological changes that have occurred since the last major release in 2013. In keeping with this, v4.0 will see all PCI DSS requirements updated to accommodate the use of technologies such as cloud hosting services.

7. Additional Sampling Guidance

Sampling is the process by which a QSA determines how many of a population of systems must be tested in order to be sure that a representative sample has been reached. In previous versions, the guidance was sufficiently vague that two QSAs could come up with noticeably different minimum sample sizes.

To address this, v4.0 will include clearer guidance for QSAs to ensure that sample sizes are determined consistently.

General Layout Updates

In addition to the seven specific updates listed above, the Council has also announced some more general updates to the standard's layout. These include:

- More accurate requirement titles
- Expanded guidance throughout the standard
- Requirements organized into Security Objectives

Once full details of the changes listed above have been announced, MegaplanIT will provide updated guidance, specific advice, and detailed recommendations. Contact us for further help at info@megaplanit.com.

Outcome Orientation: A New Way to Evidence Compliance

In perhaps the biggest single change to the standard, in PCI DSS v4.0 all 12 requirements will be rewritten as outcome-based statements. Instead of being forced down a single route for payment security and compliance, organizations will have the opportunity to demonstrate how their security protocols meet the intent of each requirement.

What does that mean in practice? The language used for each requirement will be altered so that instead of stating what must be done or implemented, it states what the resulting security outcome is. Each requirement will have a clearly stated security outcome attached to it, which organizations can choose to meet in the way that best suits their needs and CDE infrastructure.

This outcome-based approach naturally requires a more customized approach to compliance validation.

Customized Implementation & Validation

The new customized approach is intended to support organizations using security approaches that differ from the traditional PCI DSS requirements, but which meet their intent. Not only will this give organizations — particularly those with mature security and risk management programs — more freedom to adopt the best approach for their needs, it should also help v4.0 remain relevant as new technologies are adopted.

Customized validation is an evolution of compensating controls — the incumbent provision that allows organizations to demonstrate how they meet the intent of a requirement in an alternative way. Unlike compensating controls, however, customized validation will not require organizations to have a business or technical justification to meet a requirement in an alternative way. Also, since the updates in PCI DSS v4.0 build flexibility into the requirements, customized validation will not require the use of a separate appendix.

Of course, while the customized approach is intended to provide flexibility to organizations that need it, the existing defined approach will still be available. Organizations can choose to validate compliance using the defined approach, the customized approach, or a blended approach that utilizes the most appropriate option for each requirement.

By offering multiple validation approaches, v4.0 will enable organizations to choose the approach that best fits their needs.

Defined vs. Customized Implementation

Defined Implementation	Customized Implementation
• Uses existing requirements and testing procedures • Suitable for organizations with security implementations that align with current requirements • Provides directive instructions on how to meet security requirements	• Focuses on the intent of each requirement • Requires some additional steps for organizations and QSAs • Suitable for organizations that need greater flexibility to demonstrate how security controls comply with requirements • Most likely to suit organizations with mature security and risk management programs

Additional Steps for Customized Validation

For obvious reasons, opting for customized validation will require both organizations and QSAs to go through some additional steps.

Under customized validation, **organizations** will:

1. Implement adequate security controls to meet the intent of each PCI DSS requirement.

2. Provide documentation to the QSA that describes the customized implementation for each requirement. This includes providing evidence of how implemented controls meet the intent of each requirement, how the controls are maintained, and how effectiveness is assured.

Note: All customized controls and related documentation must be supported by an adequate risk assessment that determines the level of protection achieved is at least equivalent to what would have been achieved using a standard defined implementation.

To assess a customized validation, QSAs will:

- Review documentation provided by the organization.
- Develop a set of testing procedures based on the controls implemented and documentation provided.
- Document details of the testing procedures used — and results achieved — in their Report on Compliance (RoC).

Assessing organizations using customized validation will naturally take more time on the part of QSAs, as they will need to familiarize themselves with each customized control and develop appropriate testing procedures. A QSA will only be able to certify a control as compliant if they are satisfied it provides a level of security that is equivalent to (or better than) the defined PCI DSS implementation.

The RFC Process for v4.0

One of the hallmarks of new PCI DSS releases in recent years has been the Request for Comments (RFC) process. The PCI Security Standards Council (SSC) needs feedback from the global payment card industry to ensure each new release is viable in the real world, and RFC is the process they use to get it.

RFC periods are opportunities for stakeholders to provide feedback on new and existing PCI DSS releases. According to an official statement:

> **"PCI SSC stakeholder feedback plays a key role in helping ensure that PCI Standards continue to meet the needs of the global payment card industry. This feedback, together with the changes in payments, technology, and security, is driving our approach to PCI DSS v4.0."** [2]

During an RFC period, registered stakeholders are able to provide any and all feedback they have about the latest proposed release. The PCI SSC guarantees that all feedback will be looked at and considered, and all comments and feedback — including the organization's name and any resulting actions taken — will be available to view by any stakeholders that participated in that RFC.

Who counts as a stakeholder? Depending on the RFC round, the list can include:

- PCI recognized labs
- PIN Transaction Security (PTS) vendors
- Participating organizations
- Qualified Security Assessors (QSAs)
- Approved Scanning Vendors (ASVs)
- Qualified PIN Assessors

What's Different for v4.0?

As of February 2019, the PCI SSC has formally documented the RFC process in its new RFC Process Guide. The revamped process, which itself is based on community feedback, is intended to increase participation from PCI stakeholders by letting them know in advance exactly what to expect from each RFC round and making it easier to participate. Under the new process, the PCI SSC will also provide details back to the community on how specific feedback items will be addressed.

According to an official statement released through the PCI Standards Council blog: "The intent is to turn that feedback into action." [3]

RFC Timelines

Three RFC rounds were scheduled for PCI DSS v4.0:

- September – October 2019 (PCI recognized labs and PTS vendors only)
- October – November 2019
- December 2019 – January 2020

For the latest RFC information for PCI DSS v4.0, visit the PCI Security Standards RFC webpage

Preparing for PCI DSS 4.0

While the specifics of v4.0 are not yet set in stone, there are a number of things organizations can do to begin preparing for its release. We recommend all organizations take the following four steps:

Don't Bury Your Head In The Sand

We know that v4.0 will likely launch in late 2020 or early 2021. Given this — and the fact that a lot of information about the new standard is already available — organizations should be considering the possible implications of v4.0 during the coming months.

Allocate resources

Once an outline of the changes that are likely to be required has been developed, it would be sensible to allocate budgetary resources in advance. It's almost inevitable that some changes will be required, and having the resources in place early will ensure minimal disruption.

Review current and future projects

The changes proposed for PCI DSS v4.0 are significant and could affect any current or future projects that have a security, compliance, and payments technology focus. Depending on the likely impact of the proposed changes, it may be worth holding off on making major decisions until after the final RFC round.

Partner with an expert compliance assessor

An expert compliance assessor can help determine the likely impact of PCI DSS v4.0 for your organization, and bring security protocols into compliance as quickly as possible. Involving an expert partner early on in the process will also help to minimize cost and disruption during the transition.

Why Partner with MegaplanIT?

- **We're Not "Normal" Consultants**
  MegaplanIT's experienced QSAs are passionate about IT security, and have decades of experience building and maintaining effective security and compliance programs for organizations like yours.

- **Compliance Specialists**
  Compliance lies at the heart of all our security service offerings. If your organization needs support in any area to achieve PCI DSS compliance, we can help.

- **Year-Round Support**
  Got a question about compliance? Our customers are free to speak to our expert QSAs at any time and rely on us to help them solve their toughest compliance challenges.

- **Adapted to Your Needs**
  Unlike many of our competitors, our compliance services are customizable and matched to your organization's specific needs.

- **Trusted Partners**
  We build long-term relationships with our customers, and partner with them year after year. We understand their business and go beyond the contract to help them stay secure and compliant.

- **Full Range of Services**
  We take pride in being the one partner your organization needs for all its security and compliance requirements. In addition to our comprehensive compliance services, we also provide a full range of managed security, security testing, consulting, and training services.

- **100% US-Based**
  None of our services are outsourced or subcontracted. Everything is delivered directly from our headquarters in Scottsdale, Arizona.

Get Started Today

Choosing a security and compliance partner can be daunting. If you have any questions about what PCI DSS v4.0 means for your organization, or anything else to do with security or compliance, we can help.

Visit our website today to arrange a FREE consultation.

Sources

[1] PCI Security Standards Council, 3 Things to Know About PCI DSS V4.0 Development

[2] PCI Security Standards Council, 3 Things to Know About PCI DSS V4.0 Development

[3] PCI Security Standards Council, Understanding the RFC Process: New Guidance

Disclaimer

- Information provided is your company's opinion and does not represent the position of the PCI Security Standards Council. For information from the PCI Security Standards Council on PCI DSS V4.0, individuals should visit the PCI SSC website.
- Information about PCI DSS V4.0 is based on an early draft of the standard that will most likely change significantly over the several months

About MegaplanIT

At MegaplanIT, our expert security consultants and QSAs are fully certified and have decades of experience helping businesses like yours stay safe from cyber threats. We build long-term relationships with our customers and provide holistic services to meet all your security and compliance needs.

Every business has security and compliance challenges. Maybe you've had to repeatedly ask a compliance assessor to complete reports you could share with internal management, or your QSA was switched out halfway through an assessment. Maybe you've been sent a different security consultant every year, or your supplier surprises you with unplanned and unbudgeted extras to complete the project. Whatever the situation, the result is the same—the cost and level of effort required to stay secure and compliant never go down.

Most of all, with MegaplanIT everything is clear and above board. There are no hidden costs or surprises, and you'll never have to track down one of our consultants or assessors. That's our guarantee.