securityMETRICS®

PCI DSS 4.0

What You Need to Know

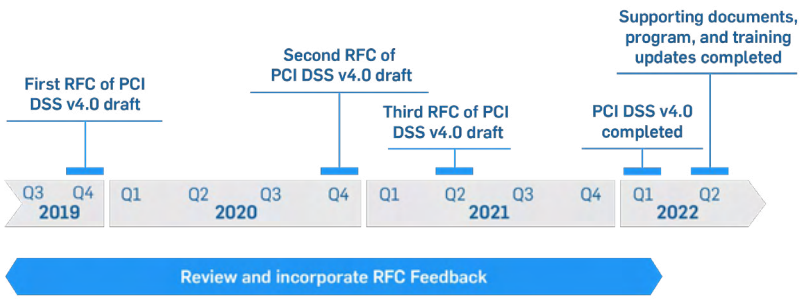
Contents

PCI DSS 4.0 Development and Implementation Timeline

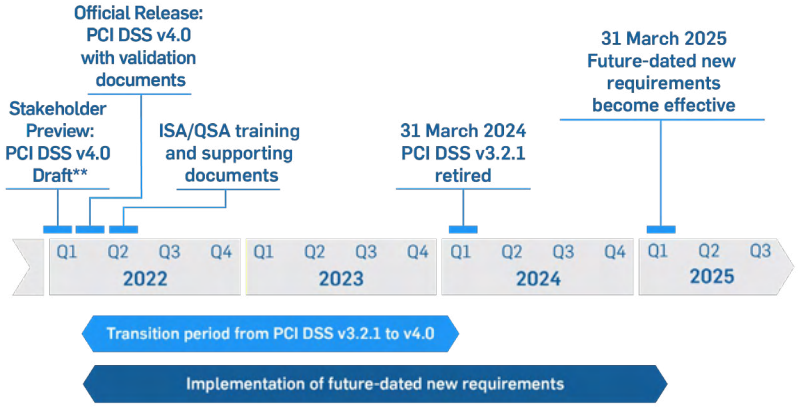
The adoption of PCI DSS version 4.0 includes an overlapping sunset date for PCI DSS version 3.2.1 to make the transition between versions smoother for businesses. The adjacent diagrams show PCI DSS 4.0 development and transition timelines. You can see that ample time has been provided for the transition from PCI DSS 3.2.1 to PCI DSS 4.0.

In addition, many new requirements in the standard are future-dated to allow new processes to be developed before they are enforced. We have included this section to give you a quick introduction to PCI DSS 4.0 and some of the larger changes. So, remain calm and keep progressing in your compliance efforts with the current version of the standard while you take some time to read and plan for PCI DSS 4.0.

PCI DSS v4.0 Development Timeline*



PCI DSS v4.0 Implementation Timeline*



* All dates based on current projections and subject to change.

** Preview available to Participating Organizations, QSAs, and ASVs.

The Goal of PCI DSS 4.0

Why did the PCI Council make a major rewrite of the PCI DSS when it is considered to be a fairly mature standard?

There are four major reasons for the changes:

- Ensure the standard continues to meet the security needs of the payments industry
- Promote security as a continuous process
- Enhance validation methods and procedures
- Add flexibility and support of additional methodologies to achieve security

1. ENSURE THE STANDARD CONTINUES TO MEET THE SECURITY NEEDS OF THE PAYMENTS INDUSTRY

As time moves on, technology changes and so do the attack vectors of bad actors trying to compromise systems.

It is important to keep up with this changing technology. PCI DSS 4.0 addresses these changes, from scoping to cloud computing. The following table shows some of the areas of further guidance and definition. This is not an exhaustive list but will give you some ideas of what has changed.

Areas of PCI DSS 4.0 evolution to stay current and relevant:

EVOLUTION AREA	COMMENTS
Scoping	Scoping guidance will be a more integral part of the standard itself by providing more detail on requirements for scoping validation. New requirements include tasks for organizations to verify their PCI DSS scope and some additional requirements for service providers.
Protection of Cardholder Data Transmissions	Included are continued enhancements to requirements for the protection of cardholder data in motion throughout the network.
Anti-Phishing and Social Engineering	The Council recognizes that phishing and social engineering are becoming bigger attack vectors. These are addressed in the PCI DSS 4.0 standard.
Risk Assessments	Requirements for performing risk assessments have been in PCI DSS for years; in version 4.0 these requirements expand and provide more detail for risk management as a whole. Additional requirements have been added to clarify the risk assessment process mentioned in section 12 of the standard.
Authentication	The Council aligned more closely with some industry best practices in authentication, such as addressing password length, periodic change guidelines, and multi-factor authentication enhancements. These revisions to password requirements help to accommodate different authentication options.
Cloud Considerations	PCI DSS 4.0 now addresses cloud technology where it may apply in the standard. The Council has also reviewed Appendix A, which contains requirements for shared hosting providers, in order to update it with cloud technologies in mind.

2. PROMOTE SECURITY AS A CONTINUOUS PROCESS

From the beginning, PCI DSS requirements were created to help organizations develop security best practice habits that would be followed year-round, rather than only during an annual assessment period. Many organizations have been able to make this transition to a security mindset and lifestyle, while others are still focused on passing an assessment and moving on.

The release of the new 4.0 version may cause anxiety for those already familiar with the current PCI DSS requirements. Rest assured that the 12 core PCI DSS requirements remain fundamentally the same; version 4.0 is not a totally new standard.

3. ENHANCE VALIDATION METHODS AND PROCEDURES

The PCI Council has looked at validation methods and procedures to make sure they are meshing with the new PCI DSS 4.0 release. The SAQ and AOC processes and contents have been evaluated, enhanced, and released in April 2022. Note that the new customized approach methods are not supported in current SAQ validation methods.

4. ADD FLEXIBILITY AND SUPPORT OF ADDITIONAL METHODOLOGIES TO ACHIEVE SECURITY

QSAs sometimes get asked the question “our methods are secure, can't I meet this requirement another way?” The response had to be “We could look at defining a compensating control, but that is a solution used if you have a constraint or hardship that does not allow you to meet the requirement as stated. Compensating controls are often temporary until you can meet the requirement as defined."

Version 4.0 of the PCI standard will try to resolve this scenario by introducing the concept of validation of a security control using a customized approach. Companies that adequately meet the objective of a requirement with existing controls can continue to use these controls as a viable way to achieve compliance.

Past validation methodologies will now be known as a Defined Approach. This is essentially what we have been doing for the past 17 years. Either approach option can be used for a PCI DSS requirement and approaches can even be mixed up within a single Report on Compliance (RoC).

Customized Approach Milestones:

The Entity

Implements control(s) that meets the intent of the PCI DSS Requirement

Provides documentation that describes the customized implementation

- The who, what, where, when, and how of the controls
- Evidence to prove the controls meet the stated intent
- Evidence of how controls are maintained, and effectiveness is assured

The Assessor

Plans and conducts the assessment

- Reviews information provided by the entity
- Derives testing procedures based on information provided
- Documents details of testing procedures and results of testing in the ROC

Customized Approach Basics

PCI DSS 4.0 introduces the concept that not all security approaches are the same and that there may be many ways to achieve a security objective. Version 4.0 will allow customization of requirements and testing procedures in order to accommodate this.

Many companies have security solutions in place that may meet the intent of a security objective, but not meet a defined testing requirement. This approach could let entities show how their specific solution meets the intent of the security objective and addresses the risk, and therefore provides an alternative way to meet the requirement.

The PCI Council has stated that "unlike compensating controls, customized validation will not require a business or technical justification for meeting the requirements using alternative methods, as the requirements will now be outcome-based."

Sounds simple, right? Well, maybe. This new validation method will most likely result in more assessment work initially for the entity in order to prepare documentation and risk assessment data for a QSA to evaluate. It will then require specialized testing procedures to be developed by the QSA and agreed upon by the entity (*see adjacent chart*).

The Customized Approach will not be for everyone and will be most suited for entities with mature security and risk assessment processes in place. The custom process provides the advantage of defining a more permanent solution for compliance validation of specialized security controls. This is different from compensating controls , where you have to document a justification for the control with a business or technical constraint.

Relying on a security implementation you already have in place may save on new capital expenses, but it will require more work on your part. You will need to thoroughly document, test, and conduct risk analysis efforts to present to your QSA. The QSA then has to review your information to develop custom testing procedures–a process which will require more reporting from the entity.

Therefore, an assessment using the Customized Approach is not for every business and will likely require more resources than an assessment using the defined approach, but it may be a more cost effective method when all aspects are considered. Be sure to look for a QSA with the depth and years of experience necessary to validate custom controls and develop appropriate testing procedures.

The Customized Approach method shouldn't be a way to disengage from your assessment. Rather, utilizing the Customized Approach should encourage working closely with your QSA.

Customized Approach and Risk Assesments

As mentioned in the previous section, the Customized Approach is now available. However, before jumping right in, larger organizations and risk assessment teams may want to look at the Defined Approach and Customized Approach so that they understand the differences between the two and can make the right decisions for their organization.

A lot of people are excited about the Customized Approach because it sounds easier to get compliant. In reality, it's going to be a pretty heavy lift. The Customized Approach requires a lot of work and effort to define what the actual requirements are and how to measure the requirements.

One of the biggest adjustments to PCI 4.0 is the increased use of risk assessments within the Customized and Defined Approaches. Risk assessments for a Customized Approach are a big part of the new standard. These risk assessments will not be a simple 15-minute process, organizations will need to follow a very structured formalized risk assessment process.

In the past, people weren't certain about what risk assessments were or the associated requirements. We'd often ask questions like "have you had a meeting, or have you written a document, or have you done something that shows that you've thought about the risks in your system?"

Now, the expectation is that if you make a significant change in your environment (e.g., adding a new firewall), you need to do a risk assessment on that change.

If you don't have a lot of experience with a formal risk assessment, or don't have a risk department as part of your company, you may need initial help from a third party to get you going and learn how to do these things.

Formal risk assessments may not seem like a big change based on some of the other future dated requirements that have been added to the standard, but this change in PCI DSS 4.0 may result in additional effort in the transition process.

NEW PCI DSS 4.0 REQUIREMENTS

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
REQUIREMENT 2: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS				
2.1.2	■		■	
REQUIREMENT 3: PROTECT STORED ACCOUNT DATA				
3.1.2	■		■	
3.2.1	■			■
3.3.2	■			■
3.3.3		■		■
3.4.2	■			■
3.5.1.1	■			■
3.5.1.2	■			■
3.6.1.1		■		■

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
REQUIREMENT 4: PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHY DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS				
4.1.2	■		■	
4.2.1	■			■
4.2.1.1	■			■
REQUIREMENT 5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE				
5.1.2	■		■	
5.2.3.1	■			■
5.3.2.1	■			■
5.3.3	■			■
5.4.1	■			■
REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE				
6.1.2	■		■	
6.3.2	■			■
6.4.2	■			■
6.4.3	■			■

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
REQUIREMENT 7: RESTRICT ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA BY BUSINESS NEED TO KNOW				
7.1.2	■		■	
7.2.4	■			■
7.2.5	■			■
7.2.5.1	■			■
REQUIREMENT 8: IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS				
8.1.2	■		■	
8.3.6	■			■
8.3.10.1		■		■
8.4.2	■			■
8.5.1	■			■
8.6.1	■			■
8.6.2	■			■
8.6.3	■			■

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA				
9.1.2	■		■	
9.5.1.2.1	■			■
REQUIREMENT 10: LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA				
10.1.2	■		■	
10.4.1.1	■			■
10.4.2.1	■			■
10.7.2	■			■
10.7.3	■			
REQUIREMENT 11: TEST SECURITY OF SYSTEMS AND NETWORKS REGULARLY				
11.1.2	■		■	
11.3.1.1	■			■
11.3.1.2	■			■
11.4.7		■		■

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
11.5.1.1		■		■
11.6.1	■			■
REQUIREMENT 12: SUPPORT INFORMATION SECURITY WITH ORGANIZATIONAL POLICIES AND PROGRAMS				
12.3.1	■			■
12.3.2	■		■	
12.3.3	■			■
12.3.4	■			■
12.5.2	■		■	
12.5.2.1		■		■
12.5.3		■		■
12.6.2	■			■
12.6.3.1	■			■
12.6.3.2	■			■
12.9.2		■	■	
12.10.4.1	■			■
12.10.5	■			■

NEW REQUIREMENT	APPLICABLE TO		EFFECTIVE DATE	
	All Entities	Service Providers Only	Immediately for All v4.0 Assessments	31 March 2025
12.10.7	■			■
APPENDIX A1: ADDITIONAL PCI DSS REQUIREMENTS FOR MULTI-TENANT SERVICE PROVIDERS				
A1.1.1		■		■
A1.1.4		■		■
A1.2.3		■		■
APPENDIX A3: DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION (DESV)				
A3.3.1	■			■
TOTALS	53	11	13	51

GRAND TOTAL: 64

Key PCI DSS 4.0 Requirement Updates

Here's a quick overview of some key new requirement changes in each section of PCI DSS 4.0:

REQUIREMENT 1

There were no significant changes in this section.

REQUIREMENT 2

There were no significant changes in this section (beyond documentation updates).

REQUIREMENT 3

Requirement 3.2.1 (March 31, 2025)

In the past, if you stored sensitive authentication data before authorization, it was recommended that you should try to encrypt or protect it, but it wasn't required. Now, it is required.

Requirement 3.3.3 (March 31, 2025)

Issuers now must encrypt the sensitive authentication data that they may be storing. This may not be a big deal for most issuers at this point, but may be difficult for some legacy systems where encryption software is not readily available.

Requirement 3.4.2 (March 31, 2025)

If you're using remote access technology to access the cardholder data environment (CDE), then you must prevent the copy and relocation of PAN data. This has been mentioned before, but now it will be a requirement.

Previously, you could just have a policy addressing this, but now it needs to be enforced by some technology. There may be settings in your remote access software that have ways of preventing access to certain functions. Depending on what resources you have and your current processes, this requirement may or may not be difficult to implement.

Requirement 3.5.1.2 (March 31, 2025)

This requirement discusses the removal of disk-level encryption as an option to protect card data. Now it can only be used for removable media (e.g., a USB drive, an external SSD). You can't use it anymore on your computer's hard drive or any kind of non-removable media. If you're using disk-level encryption for protection, you will need to make some changes.

Requirement 3.5.5.1 (March 31, 2025)

PCI DSS 4.0 also changes the security required on hashing functionality if your system is using a hash method for protecting card data.

Organizations will need to use a keyed cryptographic hash method, which is different from most common hash algorithms in use. So you may need to change your hashing algorithm to something like HMAC, CMAC, or GMAC, with an effective cryptographic strength of at least 128-bits. A code change of this kind could take some effort so you may want to focus on this earlier rather than later.

REQUIREMENT 4

Requirement 4.2.1 (March 31, 2025)

A new requirement in this section will be to carefully document, track, and inventory SSL and TLS certificates in use for the transmission of sensitive data across public networks. Increased tracking will help ensure the certificates' continued strength and validity. So, it's just a new process and tracking that needs to be implemented.

REQUIREMENT 5

Requirement 5.3.3 (March 31, 2025)

Organizations will need to scan removable media used in the CDE. Since most antivirus solutions do this or have the capability, it may just require some configuration setting changes. Review the capabilities of the malware solution you are using to see if they have these capabilities.

Requirement 5.4.1 (March 31, 2025)

One of the bigger changes is that a requirement to have automatic process mechanisms in place to detect and protect personnel against email phishing attacks has been added.

If you're doing your email in house, you may or may not have had all the controls in place for this yet. If you've outsourced emails, confirm with your provider and see what sort of protections they have against phishing attacks.

REQUIREMENT 6

Requirement 6.4.2 (March 31, 2025)

In PCI DSS 3.2.1, a web application firewall or a process to do code reviews was required to protect web applications developed by a company. In March 2025, organizations will need to have a web application firewall in place for any web applications exposed to the Internet.

This standard has been a long time coming and shouldn't be surprising. There are many solutions, including cloud-based solutions, that can help with this requirement.

Requirement 6.4.3 (March 31, 2025)

To reduce the possibility of malicious scripts making it onto payment pages, organizations need an inventory of all the known scripts used on those pages. This inventory must be documented and tracked to ensure that all the scripts used are authorized, and that the integrity has been validated. Review the guidance column for further information on this requirement.

REQUIREMENT 7

Requirements 7.2.4, 7.2.5, 7.2.5.1 (March 31, 2025)

Not much has changed in this section. It's the basic, role-based access control requirements, and most of the changes are just tightening account reviews and processes around reviews for systems, users, and applications.

REQUIREMENT 8

Requirement 8.3.6 (March 31, 2025)

To strengthen passwords, the minimum length of passwords is moving from 7 to 12 alpha and numeric characters.

Depending on your applications, this could be a simple fix or it may require some code changes. So, start checking now to see if there are any systems in use in your CDE that would have difficulty with this future dated requirement.

Requirement 8.3.10.1 (March 31, 2025)

Another change in section eight around passwords pertains to service providers. Customers of service providers will now have to change their passwords every 90 days if you're using just a password for authentication (i.e., you are not using a multi-factor authentication).

Requirement 8.4.2 (March 31, 2025)

Multi-factor authentication will be required for all access to the CDE, not just from external locations. So this then would apply for internal administrative access to servers, firewalls, networking gear, etc.

Requirement 8.5.1 (March 31, 2025)

PCI DSS 4.0 adds a new detail to MFA requirements that might be a bit tricky. Success of all the factors has to happen before authentication, and it can't be known from the process which factor has failed.

Presently, most systems ask for a username and password (i.e., something you know) and only move on to the second factor if you have the correct username/password. This will no longer be allowed.

Both factors will have to be presented and entered without revealing any information about which factor might have been wrong if authentication fails.

Requirement 8.6.2 (March 31, 2025)

All application and system passwords that could be used for interactive login have additional approval and tracking controls on their use, and can no longer reside in a script or a file.

PCI DSS 4.0 SECTION 9

There were no significant changes in this section.

PCI DSS 4.0 SECTION 10

Requirement 10.4.1.1 (March 31, 2025)

Organizations can no longer review their logs manually.

Few, if any, companies are manually reviewing logs anymore as it's just too much data to effectively review manually. There are many log review tools out there, so it shouldn't be difficult to implement a solution. Manual review of logs is time-consuming and easy to do poorly, so this is a good change.

Requirement 10.7.2 (March 31, 2025)

All organizations must now detect, alert, and promptly address failures of critical security control systems. This used to be only required for service providers, but has now been extended to everyone.

This means that if you had a firewall or IDS system that went down for some reason, you would have to detect it, generate an alert, and respond to that alert. This update will require additional procedures for merchants to implement. We recommend that you start now to look for solutions.

PCI DSS 4.0 SECTION 11

Requirement 11.3.1.2 (March 31, 2025)

Internal vulnerability scanning must now be authenticated. This means that it's not just a scan of ports and services; now, if a service is exposed that requires a credential to access it (e.g., a web app), you need to use those credentials to gain access and test the authenticated port or service.

An important part of this new requirement will be that the credentials used by the vulnerability assessment (VA) scanner must be entered in the system and stored securely. This will have to be a feature of the VA scanning solution and should be something you check with your vendor carefully on.

Requirement 11.5.1.1 (March 31, 2025)

Another requirement change was on IDS/IPS, so that systems detect and alert on any covert malware communication channels that are being used (i.e., DNS tunneling). This may represent a change to the IDS/IPS system that you are currently using.

Requirement 11.6.1 (March 31, 2025)

Probably one of the biggest things in section eleven was the addition of a requirement to implement a change and tamper detection mechanism for any payment pages. This requirement addition is a direct result of the increase in e-commerce skimming compromises seen on payment pages in recent years.

Before March 31, 2025, companies will have to deploy a solution that will detect changes to those pages (e.g., script additions, changes to known script and code).

> This is a great addition to the standard and is helpful in protecting e-commerce data.

PCI DSS 4.0 SECTION 12

Requirement 12.5.2 (Immediately Effective for 4.0 Assessments)

An annual scoping of your card data environment was mentioned in the initial discussion section of previous versions of PCI DSS, but now the Council has moved that into the requirements matrix under section 12 and made it a trackable requirement effective immediately for version 4.0.

So a documented scoping exercise will have to be done by merchants annually, or after any significant changes to the in-scope environment (e.g., people, systems, processes).

Requirement 12.5.2.1 (March 31, 2025)

New for service providers will be a future dated requirement to perform this scoping exercise at least every six months and after any organizational changes to the company.

Requirement 12.6.2 (March 31, 2025)

Organizations will need to enforce a more formal Security Awareness Program, where before you could get by with some basic security training.

Organizations will need to document and update their Security Awareness Program at least once every 12 months and as needed to address any new threats and vulnerabilities that may impact the security of their CDE or information provided to personnel about their role in protecting cardholder data.

Requirement 12.6.3.1 (March 31, 2025)

The standard now expects a security training program to discuss specific threats and vulnerabilities in your environment, as well as acceptable use of end-user technologies.

For example, if phishing is a big deal for your environment, then you need to address phishing in your training. The training program will also need to be reviewed and updated at least annually.

Requirement 12.10.7 (March 31, 2025)

Incident response procedures will need to be initiated if stored Payment Account Numbers (PAN) is detected anywhere it is not expected. This means that you are always on the watch for new or errant processes creating repositories of stored PAN outside of expected boundaries.

Periodic review of processes dealing with card data and running a good data discovery tool will be needed to fully say you have satisfied this future-dated requirement.

PCI DSS v. 4.0 Requirement FAQs

WHAT IS BEING DONE TO SIMPLIFY THE PCI PROCESS FOR SMALL BUSINESS MERCHANTS?

The PCI Council is really not the entity that is concerned with simplifying the SMB compliance processes. They want people to be able to use the standard and validate their compliance (through the SAQs), but they will not work on making that process any simpler than they have.

Merchant banks often use a portal provider for their merchants to validate PCI compliance through. Work with your merchant bank or call one of the portal providers for information.

For example, SecurityMetrics offers a portal for use by small merchants, which simplifies their PCI compliance efforts.

HOW HAVE THE REQUIREMENTS FOR RISK ASSESSMENTS CHANGED IN VERSION 4.0?

In version 3.2.1, the risk assessment had to be done annually, and it should be based on some industry-accepted risk assessment process. Outside of that, there wasn't really a lot of detail that was provided other than it had to happen at least once a year.

In version 4.0, they're relying on the risk assessment for a lot of the other requirements. Most requirements that state a task must be performed on a periodic basis will, in version 4.0, tie the decision on how often the task be performed to a targeted risk assessment.

One requirement that comes to mind for this is for merchants who perform card-present payment transactions using a terminal or device that physically interacts with the credit card. These merchants are required to have tamper prevention inspections on those on a periodic basis.

What does *periodic* mean? Your risk assessment should determine what periodic means for your organization.

There are many requirements tied back into that risk assessment requirement where you do have to do a risk assessment at least annually.

But those risk assessments should be looking at things like "how often am I performing tamper inspection reviews on my terminals?"

If you're currently doing a risk assessment for PCI in version 4.0, you should examine all these additional requirements that tie back to the risk assessment and make sure your risk assessment is covering all of these requirements.

HAVE REQUIREMENTS CHANGED SURROUNDING DOCUMENTATION?

There have been some changes to documentation. For example, at the beginning of each section, there's a requirement that states you have policies and procedures in place and staff members are aware of these policies.

For example, Requirement 1 addresses firewalls and network devices. At the very beginning, there is a requirement that discusses having policies and procedures in place, and documentation about what staff members or which groups within our organization are responsible for maintaining the security of these devices. These people need to have a copy of our policies and procedures surrounding network device security. You'll see similar requirements in every section.

Another example: Requirement 3 addresses how organizations protect credit card data at rest. For this requirement, you need to show that you have policies and procedures in place that define how stored cardholder data is protected. Also, someone is put in charge of making sure that data at rest is protected, and that they have a copy of these policies and procedures.

FOR THE REQUIREMENT 11.6.1, WHAT IS THIS REQUIREMENT, AND WHICH SAQ TYPES NEED TO WORRY ABOUT THIS?

PCI requirement 11.6.1 deals with protecting payment pages from malicious scripts that can even tease data out of third-party iframes used to collect cardholder data. So, if you have a payment page or reference a payment page via an iFrame on your e-commerce website, this will affect you.

This requirement has been included in the SAQ A, the SAQ A-EP, and the SAQ D.

To meet this requirement, you will need to monitor all payment pages or pages that reference payment pages at least every 7 days looking for unexpected scripts or behaviors.

There are some recommendations that the PCI Council gives in the PCI DSS documentation for how to become compliant with requirement 11.6.1, but this is mostly going to affect e-commerce merchant types.

PCI DSS Version 4.0 Preparation FAQs

WHEN SHOULD YOU START WORKING ON 4.0?

It doesn't hurt to start looking at it now. Merchants have until March 31, 2024 before they will no longer be able to validate their compliance using version 3.2.1 of the SAQs.

For many of the SAQ types, very few changes have been made, so moving to PCI version 4.0 may be quite simple. However, some of the SAQ types (e.g., SAQ A) have several newly added requirements that may take time to implement in a merchant's environment.

If this is the case for your organization, continue to validate your compliance using version 3.2.1 but begin now to implement any missing controls that would be required to validate to version 4.0.

IF AN ORGANIZATION HASN'T REACHED COMPLIANCE WITH V. 3.2.1, SHOULD THEY FOCUS ON GETTING COMPLIANT TO V. 4.0?

That is not an easy answer.

It may depend on the layout of your systems, how close you are to security compliance, and how soon you have to validate compliance (if soon, stick to 3.2.1).

But if you are brand new and have some time, it's recommended to go through version 4.0. Remember that you can work on the future dated requirements (some harder) over three years. If you would fall under an SAQ for compliance validation, you'll have to wait for a bit still to see what those look like.

WHAT ARE SOME BEST PRACTICES TO STARTING PCI 4.0?

First, it's all about the amount of time it's going to take to accurately fill out your SAQ. If you get started as soon as it's available to you, you will have time to implement new security practices.

The transition from PCI version 3.2.1 to version 4.0 seems a lot simpler than one might think, just for the reduction of questions alone. If it is available to you, take it and run with it.

One caveat would be for the following SAQ types:

- SAQ A
- SAQ A-EP
- SAQ C
- SAQ C-VT

These SAQs have added some of the existing PCI requirements, which are not future-dated. So, if you look through the version 4.0 SAQ and it contains some newly added requirements (that are not future-dated), realize that these must be in place to successfully validate your compliance using that SAQ.

Look through the PCI DSS version 4.0 SAQ that fits your environment and ask yourself, "how would performing an SAQ 4.0 affect me? Are there any security controls that need to be in place now that I currently don't have in place?" If there are, go ahead and take the opportunity to continue using version 3.2.1 while it's still here. But start working now on being fully compliant with all requirements listed in the PCI v.4.0 SAQ.

PCI DSS v. 4.0 SAQ FAQs

CAN THE VARIOUS SAQ TYPES USE THE CUSTOMIZED APPROACH? (E.G., SAQ A)

No, the Customized Approach can only be used for ROC-based assessments. It is only meant for large organizations that have a mature security setup. Organizations can use the Customized Approach to show they are meeting the intent of a PCI requirement that differs from the Defined Approach in the PCI DSS.

Organizations performing a Customized Approach assessment will need to work with their QSA to define testing procedures that will validate the intent of the requirement has been met.

DOES THE SAQ DOCUMENT LOOK DIFFERENT IN PCI 4.0 VS. 3.2.1?

It's going to look a little bit different, but not substantially different. There's still the Qualifying Criteria section and a place where you put your contact information. The formatting is a little bit different but not substantially so.

With the exception of the SAQ A, there are fewer checkboxes in the PCI DSS version 4.0 SAQs. They've consolidated some of the requirements all into one box, whereas in the past, there were multiple boxes you needed to check. If you are familiar with or had performed a self-assessment in PCI DSS version 3.2.1, version 4.0 is not that big of a stretch.

IF YOU SUBMIT A PCI V4.0 SAQ, DO YOU HAVE TO FOLLOW THOSE FUTURE-DATED REQUIREMENTS?

Future-dated requirements don't need to be implemented until March 31, 2025. These future-dated requirements are considered best practices until that time.

So, you should have those in place or be working on those. If you don't have them in place, you're still compliant even if they're not in place until 2025. The main newly added requirements that are immediately required for 4.0 assessments are requirements on documentation (requirements 2.1.2, 3.1.2, 4.1.2, 5.1.2, 7.1.2, 8.1.2, 9.1.2, 10.1.2, 11.1.2), risk assessments (requirement 12.3.2), and scoping (requirement 12.5.2), as well as service providers' requirements around third-party service providers (TPSPs) (requirement 12.9.2).

WHEN WILL THE SAQS CHANGE AGAIN?

The short answer is that we never really know. From version 3.0 to 3.2 to 3.2.1, there were several fairly quick changes that were made to deal with some newly discovered vulnerabilities surrounding transmission encryption (e.g., vulnerabilities in TLS and SSL). So, there have been some significant changes to come out quickly in the past.

However, the Council likely is not expecting any significant changes to happen anytime soon, but the fact that organizations still have two years before 3.2.1 is officially retired, and another year before new 4.0 requirements are required. A lot can change in that period.

So, if there are significant changes to the risk landscape, the PCI Council will likely come out with new requirements to address that additional risk. It all depends on the risks merchants are facing and if the PCI SSC addresses these risks.

If the risk to merchant environments stays fairly static, there's probably not a desire to make significant changes to the standard. The Council probably feels comfortable with where the standard is now and expects version 4.0 will be with us for quite some time. But we really don't know; we'll have to see.

WHAT ARE SOME OF THE BIGGEST CHANGES IN PCI VERSION 4.0 FOR SERVICE PROVIDERS?

The biggest change for service providers is the fact that instead of just checking a box, you will also need to write in your SAQ what steps you took to verify that each required security control was in place. This will be a much more intensive exercise for our service providers.

After marking that various controls are in place, they have to go in and say, "these are the systems and the settings I looked at to verify that this control is in place in my environment." So, it is going to be a lot more work for a service provider to fill out an SAQ D version 4.0 than it was in 3.2.1.

What's the best way to explain the difference between a merchant and a service provider?

Knowing who counts as a service provider really deals with who holds the merchant account. If you're selling shoes, and when someone purchases your shoes and pays with a credit card, that money goes directly into your bank account, you are a merchant.

If you're helping merchants perform those operations, then you are a service provider. For example, if you help merchants by managing their firewalls or e-commerce servers, but the money from the customer doesn't go into your bank account, it's going into your customer's bank account, then you're a service provider.

You can be both a merchant and a service provider.

WHERE IS MORE INFORMATION ABOUT SAQ UPDATES?

The first place to go is the PCI Council's website itself. If you go into the document library, you can download all the guidelines and documentation. The Council also has a blog that discusses PCI DSS updates.

Here's a list of the various SAQ documents from the PCI Council:

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- SAQ D Service Provider
- SAQ P2PE

The next place to look is SecurityMetrics, where there are numerous articles about the new PCI DSS standard and how it will affect different types of merchants.

Again, the PCI Council's website is usually the best place to go to see the document quickly, and then look for other answers on SecurityMetrics' blogs, white papers, podcasts, and webinars.

SAQ OVERVIEW		V. 3.2.1	V. 3.2.1	V. 4.0	V. 4.0
SAQ	DESCRIPTION	# OF ?S	VULN. SCAN	# OF ?S	VULN. SCAN
A	**E-commerce website (third party)** • Fully outsourced card acceptance and processing • Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor • Merchant can't impact the security of the payment transaction	24	No	31	Yes
A-EP	**E-commerce website (direct post)** • Merchant website accepts payment using direct post or transparent redirect service	191	Yes	151	Yes
B	**Processes cards via:** • Analog phone, fax, or stand-alone terminal • Cellular phone (voice) or stand-alone terminal • Knuckle buster/imprint machine	41	No	27	No
B-IP	**Processes cards via:** • Internet-based stand-alone terminal isolated from other devices on the network	86	Yes	48	Yes
C	**Payment application systems connected to the Internet:** • Virtual terminal (Not C-VT eligible) • IP terminal (Not B-IP eligible) • Mobile device (smartphone/tablet) with a card processing application or swipe device • View or handle cardholder data via the Internet • POS with tokenization	160	Yes	131	Yes
C-VT	**Processes cards:** • One at a time via keyboard into a virtual terminal • On an isolated network at one location • No swipe device	83	No	54	No
P2PE	**Point-to-point encryption** • Validated PCI P2PE hardware payment terminal solution only • Merchant specifies they qualify for the P2PE questionnaire	33	No	21	No
D-MER	**E-commerce website** • Merchant website accepts payment and does not use a direct post or transparent redirect service **Electronic storage of card data** • POS system not utilizing tokenization or P2PE • Merchant stores card data electronically (e.g., email, e-fax, recorded calls, etc.)	329*	Yes	251*	Yes
D-SP	**Service provider** • Handles card data on behalf of another business • Provides managed firewalls in another entity's cardholder data environment • Hosts a business's e-commerce environment/ website or controls the flow of e-commerce data	354**	Yes	267**	Yes

**Additional controls in Appendix A2*

***Additional controls in Appendix A1 and A2*

securityMETRICS®

Takeaways

What are the most important things to focus on right now?

First, read the PCI DSS version 4.0 standard and get familiar with the bigger changes that could impact your compliance process. Then start formulating your plans right now to implement changes for version 4.0.

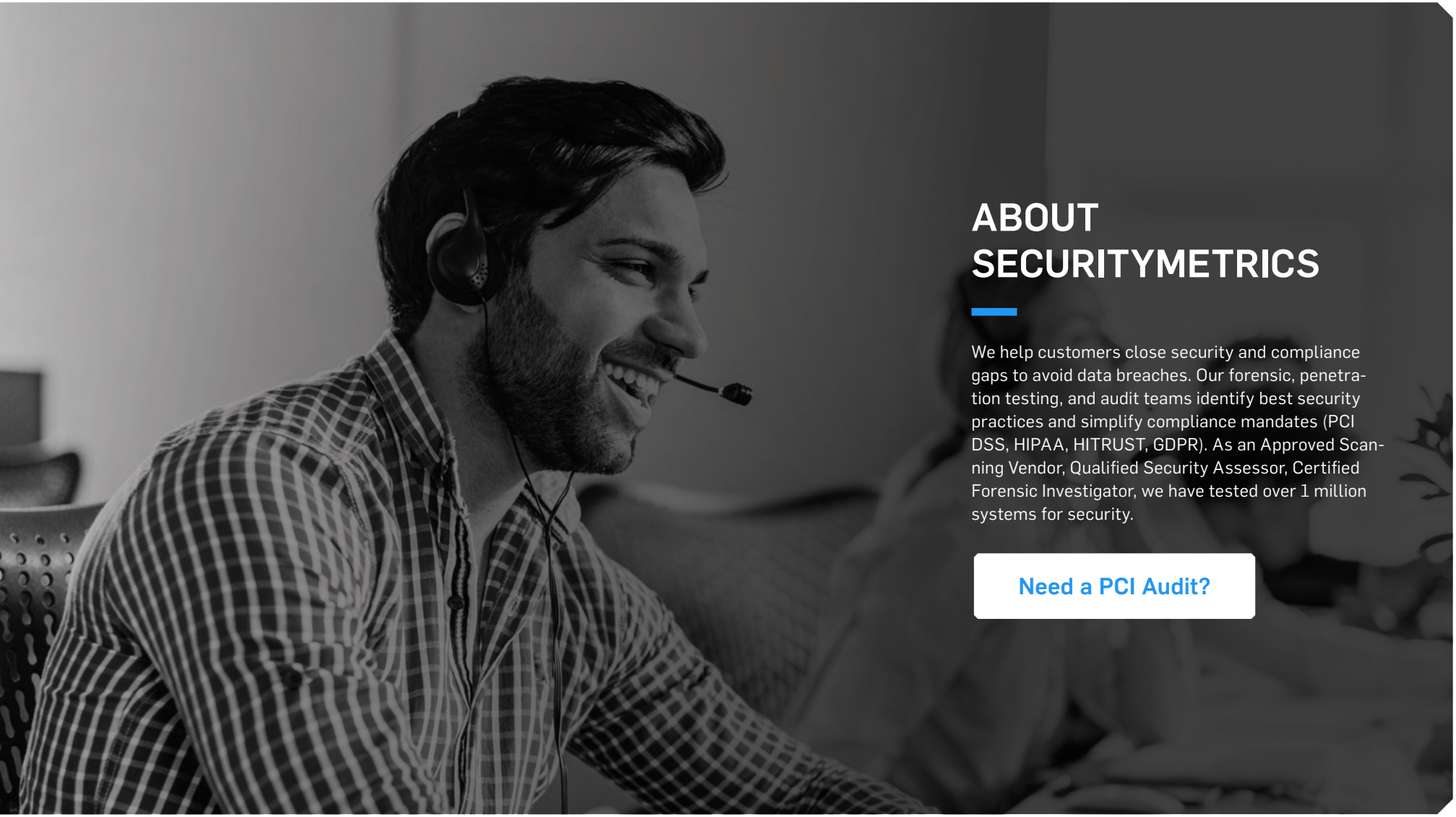
There is plenty of time, so start early and you will not have problems making the transition. During this planning process don't forget to keep working hard to keep your current efforts going to be compliant to PCI DSS version 3.2.1.

Second, start thinking about how you are conducting your risk assessments. More formal risk assessment processes are required in version 4.0 and most organizations will have to add processes and gain skills to do this correctly. Start doing google searches on formal risk assessment and refer to the industry standards out there like NIST 800-30 and OCTAVE to begin getting familiar with them. It may be a good idea to consult with a QSA as you develop these processes.

QSA's will not be able to conduct a PCI DSS 4.0 assessment until after they have been formally trained by the PCI Council (expected mid-Summer 2022), so it is a bit too early to actually start on a formal assessment to PCI DSS version 4.0, but QSA's are happy to start consulting on questions you may have as you begin working on your version 4.0 compliance.

Finally, don't wait until 2024 to begin switching over to PCI DSS 4.0. Spread your efforts across the next couple of years and you will be just fine with the new requirements.

PCI DSS version 4.0 may seem daunting, but is actually an improved way to counteract the techniques used by threat actors. Preparing for compliance to version 4.0 is straightforward if you are already working towards or maintaining compliance to PCI DSS 3.2.1.



ABOUT SECURITYMETRICS

We help customers close security and compliance gaps to avoid data breaches. Our forensic, penetration testing, and audit teams identify best security practices and simplify compliance mandates (PCI DSS, HIPAA, HITRUST, GDPR). As an Approved Scanning Vendor, Qualified Security Assessor, Certified Forensic Investigator, we have tested over 1 million systems for security.

Need a PCI Audit?