FORTRA™

Insider Insights for the PCI DSS 4.0 Transition

Introduction

Businesses of all types need to operate with the highest degree of security for their customers' data. Many businesses are covered under strict regulations about these expectations. For organizations that process payment card data, they also need to adhere to the strict standards set forth by the Payment Card Industry (PCI) Security Standards Council (SSC).

The formal Standard, known as the Payment Card Industry Data Security Standard (PCI DSS) has recently been updated to version 4.0, reflecting the contemporary changes in the security environment. The new version is slated for implementation by April 1, 2024, and some parts offer a further grace period, not requiring compliance until April 2025.

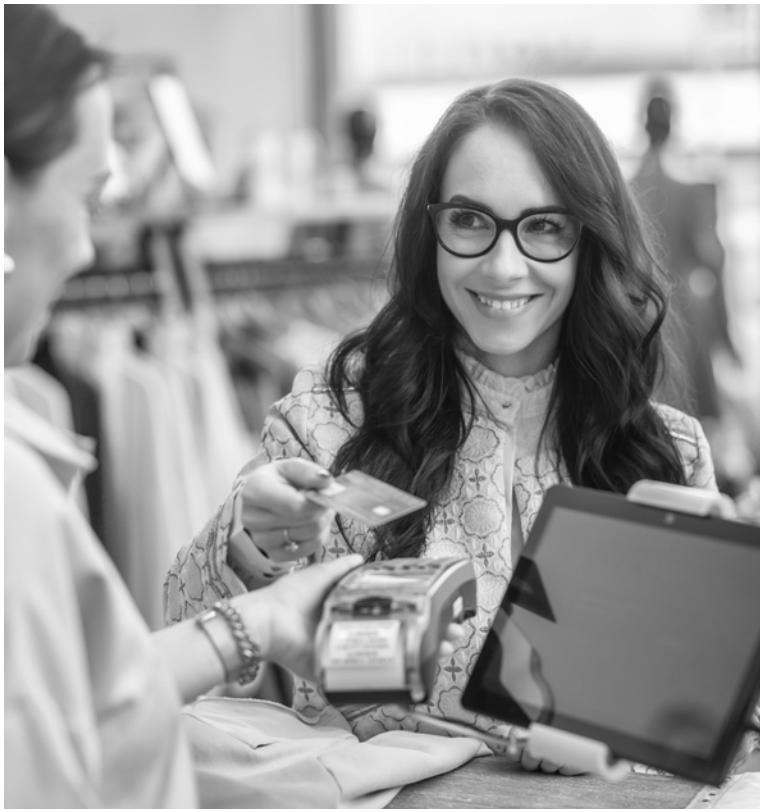
The most important part of PCI DSS compliance is the focus on protection of the Cardholder Data Environment (CDE). Whether it is the logical path that leads to the CDE, or even the physical access, any weakness that can allow unauthorized access to the CDE is assessed as a failure of compliance with the Standard.

Many organizations that process payment card data are already compliant with the previous version of the PCI Standard. This puts them in a solid position to transition to the new version. For organizations that are new to the payment card industry, the new Standard comes with comprehensive guidance, as well as supporting documentation to help with the implementation. Many of the requirements are also good for general security hygiene throughout an organization.

Is your organization ready for the new Standard? We assembled a group of experts who offer their guidance about some of the challenges of the new requirements, as well as some tips for making the path to compliance easier. This eBook covers all 12 requirements of the new Standard, and the insights offered by our panel amplify the salient points. Along with that, we have devised a quiz to help you assess your readiness for the new Standard.

We are confident that this will help with your journey to PCI DSS v.4.0 compliance.

David Bruce
Senior Product Manager, Fortra



Requirement 1
Install and Maintain Network Security Controls

Network security is only as strong as the controls that are in place to prevent unauthorized access. Requirement 1 aims to ensure full visibility of the entire CDE, including information about the physical hardware, as well as robust documentation concerning all aspects of the environment. **Jeff Man** offers the following:

> *Start with an up-to-date network diagram, as well as a data flow diagram that details all of the logical paths into and out of your CDE, and then follow the rules. The rules are not really new, they are merely more explicitly comprehensive to assure that you build and maintain a secure network.*

Jeff Man
Sr. Information Security Consultant

EXPERT INSIGHT FROM JEFF

The biggest change to Requirement 1 is the elimination of most references to legacy and archaic network devices, such as routers and switches, or references to 3-tier e-commerce architectures. This acknowledges that modern network devices provide all-in-one capabilities. There is also inclusion of cloud/container environments, and where security rule sets have replaced firewall rules.

...AND AN INSIDER TIP

The challenge of meeting Requirement 1 is to make sure you are knowledgeable about whatever network security controls you are utilizing. Adhering to the requirements, and making sure you are properly applying the protections to your CDE from even your own internal network, and not just the internet is of utmost importance. In this way, you can truly declare the rest of your network as “untrusted” from the perspective of PCI.

Requirement 2

Apply Secure Configurations to All System Components

One of the most dangerous vulnerabilities is a misconfiguration of a component. This is because misconfigurations can often go unnoticed, and are not fixed with patching or upgrades. Requirement 2 sets out to correct this by ensuring that configurations are carefully managed across the CDE. **Anthony Israel-Davis** makes the following observations:

> *Ensure you have a way to show that the configurations in your running environment conform to the policies that you have in place. Ideally, this is something that can be done on a regular basis to ensure there hasn't been any configuration drift or manual changes to the code-defined environment.*

Anthony Israel-Davis
Product Security Manager

EXPERT INSIGHT FROM ANTHONY

With any audit, consider how evidence will be provided for compliance. For this requirement, it's not enough to have the documents complete and up to date—you also need to show proof that what is documented is in use and known to team members responsible for implementation.

...AND AN INSIDER TIP

When documenting changes, it's important to note why a particular service or port is required. Not only will you know why the configuration was set that way, you will also be able to future-proof your audits if you ever need to provide a business justification for insecure services, protocols, or daemons.

Requirement 3
Protect Stored Account Data

One of the greatest challenges of many organizations is about how much data to save. While data can be seen as a treasure trove to help grow a business, it is also equally attractive to malicious actors. Requirement 3 aims to control not only how data should be protected, but how much data is reasonable to store. **Funso Richard** shares his advice on complying with this requirement:

> *Organizations will need to work with their Qualified Security Assessors (QSAs) to figure out what the new scoped environment should be. This is particularly important to ensure compliance and minimize unnecessary work.*

Funso Richard
Information Security Officer

EXPERT INSIGHT FROM FUNSO

One major consideration is for organizations to identify their business needs from the lens of the requirement. That is, don't begin with "we have to collect payment card information, so what do we need to do?" Rather, they should begin with the mindset of "this is what the requirement states, and what do we need to have in place to effectively build an Account Data environment?"

...AND AN INSIDER TIP

Treat your PCI compliance requirements as a program, rather than a project. Though a program incorporates elements of a project, it is an ongoing process that must be designed to remain adaptable to changes in the Standard.

Requirement 4

Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

When it comes to the ultimate method of protecting data, nothing compares to a solid implementation of industry-recognized cryptography. Requirement 4 contains only two main headings, but they are among the most powerful towards achieving data protection. **Nigel Sampson** is critical of the current language of the standard, believing that it leaves out an important consideration:

> *Use the Standard as a guide, but work to go beyond the minimum requirements. Use best practices and industry guidance to build a solid security program. Constantly monitor the program's maturity to ensure that it is ahead of the Standard.*

Nigel Sampson
Director of Cybersecurity

EXPERT INSIGHT FROM NIGEL

The challenge in the new Requirement 4 section is that organizations will not have a marker towards which they can work to ensure compliance, but also ensure secure transport of data. This weakens the Standard. By removing the prescriptive phrase "the latest version of SSL," or stating a minimum of TLS 1.2, means that if a new encryption version comes out, organizations will not be required to update encryption unless the Standard is amended.

...AND AN INSIDER TIP

This requirement is changing. It will change again. This is why staying ahead with industry best practices is a more efficient way of dealing with change. Rather than just meeting what the Standard is today, ensuring your cyber program is flexible, scalable, and agile is a must.

Requirement 5

Protect All Systems and Networks from Malicious Software

In today's environment, malware is one of the greatest threats, unleashing damages that have monetary consequences. Requirement 5 addresses the importance of combatting malware, from halting the software itself, to implementing anti-phishing technology as a method to prevent this most common attack technique. **Ian Thornton-Trump** expands on this with the following observations:

> *The updated PCI DSS version represents a profound shift in the evolution of the Standard, making it evident that the Council recognizes that compliance is far more of an organizational security challenge, and no longer just an endpoint, or malware problem. This moves proactive motion further ahead.*

Ian Thornton-Trump
Chief Information Security Officer

EXPERT INSIGHT FROM IAN

The PCI DSS changes seem to have now expanded to include the most common attack vectors, from phishing, to malware. I foresee profound impacts across many of the IT security, software development, asset management, and risk management functions of an organization as a result of the new updates.

...AND AN INSIDER TIP

Seek a third-party audit against this new standard as soon as possible in order to build in the updates of the new Standard.

Requirement 6
Develop and Maintain Secure Systems and Software

There is a legal doctrine that speaks of the Fruit of the Rotten Tree. When thinking of securing the CDE, if the systems and software are not secure, there is little that can be done to prevent exploitation of the data that grows out of those systems. Requirement 6 stresses this point. **Tyler Reguly** has years of first-hand knowledge, as well as academic experience teaching others, about the best ways to achieve this goal:

> *Do not rely on a standard to dictate your security policies or programs. Instead, develop your own, and ensure they encompass the requirements of the security standard you are looking to implement.*

Tyler Reguly
Senior Manager, Security R&D

EXPERT INSIGHT FROM TYLER

Secure development training is key. Then, turning that training into a well-defined secure software development lifecycle will help you address these requirements.

... AND AN INSIDER TIP

It is important to note that only one part of this requirement applies to internal software development. The remainder applies to your systems and how they are used, configured, and managed. It really is a broad collection of mixed requirements that should be carefully delegated to provide the most complete coverage.

Requirement 7

Restrict Access to System Components and Cardholder Data by Business Need to Know

In many organizations, the phrase "need to know" generates a lot of confusion. Requirement 7 makes this previously fuzzy concept very clear by offering two definitions: "Need to know" refers to providing access to only the least amount of data needed to perform a job. "Least privileges" refers to providing only the minimum level of privileges needed to perform a job. **Ben Rothke** sheds further light on the importance of this requirement:

> *It all comes down to the fundamental business, as well as information security principles of need to know, and least privilege. A user, process, or system should only have access to the specific data, resources, and applications needed to complete a required task. Following these principles improves security, lessens the chance of a data breach, and is essential to PCI compliance.*

Ben Rothke
Senior Information Security Manager

EXPERT INSIGHT FROM BEN

The QSA would typically ask something like, "based on your current and up-to-date network diagrams and cardholder data (CHD) flows, please show me how you restrict access to the Cardholder Data Environment (CDE) and CHD." Part of the reason so many people have challenges with Requirement 7 is that they don't understand where their CHD resides and the systems involved in processing it.

...AND AN INSIDER TIP

Companies need to know precisely what their PCI scope is. Only when a firm knows its scope can it ensure that it is PCI compliant, particularly with Requirement 7. The Qualified Security Assessor (QSA) must sign off on their scope. Too many firms significantly underestimate their scope, and that is a surefire method to ensure they fail a PCI audit.

Requirement 8

Identify Users and Authenticate Access to System Components

One of the heftiest responsibilities of the security team is keeping a firm awareness of all the users on a system, and appropriately controlling the authentication mechanisms for each. One oversight can allow an unauthorized person into the system. Requirement 8 seeks to address this important responsibility. **Dr. Andrea Simmons, PhD**, is deeply familiar with this task, and provides valuable vision to meet this task:

> *It is vital that we have fully documented who has access to what. Making sure there are supporting processes for identifying and authenticating all those who are on those systems still appears to be challenging, even though system access precision has been a long-time focus in the computing industry.*

Dr. Andrea Simmons, PhD
Managing Consultant

EXPERT INSIGHT FROM ANDREA

Keep up to date with all of your tasks, including the administrative ones. Maintaining documentation and updating lists is vital. Ensure that your People Management (HR) folks are updating joiners, movers, and leavers (JML) information on a regular basis so that your authentication records align with your employee (and third party/ contractor) population.

...AND AN INSIDER TIP

For anything that you know will appear misaligned during an audit, if Requirement 8 can be shown to be "in place with remediation," then no further investigation will be required. Remediation includes the proactive use of Plan of Action and Milestones (POAM) documents (templates), as these, in particular, can show who is responsible for what action, by when. Your QSA relies heavily on documentation to "show and tell" the story of your compliance.

Requirement 9
Restrict Physical Access to Cardholder Data

Few things could be more embarrassing than putting monumental technical efforts into protecting the CDE, only to be undone by something as simple a physical security oversight. Requirement 9 seeks to ensure that physical access to the CDE is properly maintained. **Shubhra Deo** explains the importance of this requirement:

> *A security principle that must be adhered to is that physical access log reviews should be performed by a person with no conflict of interest. For example, IT administrators cannot review logs of the data center. Each organization is different, hence, due diligence should be conducted while assigning this task.*

Shubhra Deo
Head of Data Privacy and Security

EXPERT INSIGHT FROM SHUBHRA

To establish a good physical security program, organizations must manage the legitimate movement of assets and people to ensure the safety of the CDE. If we look at the practical implementation of this control in an organization, it would mean providing either color-coded plastic cards, or access badges, or a printout containing the visitor's picture and escort name. If the visitor can be distinguished from an employee with their badge or any other identification, this would meet the intent of this specific area of the requirement.

...AND AN INSIDER TIP

For sensitive areas in the CDE, an organization should have access control for exit gates, and should not rely only on a push button for the exit. Whereas, if the organization is using video cameras, it should capture the face of the person exiting the area. Another tricky part to ponder is that sensitive areas should be enclosed with hard walls, and not glass partitions.

Requirement 10

Log and Monitor All Access to System Components and Cardholder Data

One of the most valuable methods of keeping watch over the entire environment is through monitoring the activity that takes place. Requirement 10 directs the careful curation, review, and storage of system logs, as well as the importance of corrective attention if log mechanisms fail. **Ross Moore** offers keen insight about this requirement:

> *A major challenge of Requirement 10, is losing sight of the security goal, which is to regularly monitor and test networks for the purpose of keeping customer data safe. Getting into the weeds of requirements is challenging enough, but when the "Why are we doing this?" answer is lost, then that can quickly diminish the reason for the details.*

Ross Moore
Cybersecurity Analyst and Writer

EXPERT INSIGHT FROM ROSS

Demonstrate how a multi-departmental effort will help to achieve compliance. For example, some ways to build a strong case towards improved efficiencies is through graphs and charts that demonstrate latency, the need for extra storage for log retention, and the business need for obtaining other pertinent resources, such as regulatory experts, security, and IT.

...AND AN INSIDER TIP

Tie monitoring and alerting into other aspects of the business, such as DevSecOps, and IT Infrastructure. Any other business units where it can be integrated could help in procuring the right solutions and assistance in implementation and maintenance.

Requirement 11
Test Security of Systems and Networks Regularly

Setting all the security necessary to give the appearance of PCI DSS compliance only goes so far. Requirement 11 puts all of the settings, configurations, and controls to the real-world test. This enables an organization to see if their defenses are as good as the Standard requires. **Angus Macrae** understands how important this requirement is, and offers the following:

All well run organizations, regardless if they are seeking or claiming PCI DSS compliance or not, should by now already have formalized processes, technology, and capabilities in place for identifying and addressing system vulnerabilities. This must include a way of regularly scanning their systems to ensure this is being appropriately managed. By ensuring that you assess and manage all risks, and vulnerabilities, rather than just the high and critical ones, meeting these evolving requirements should simply align with your existing responsibilities.

Angus Macrae
Head of Cyber Security

EXPERT INSIGHT FROM ANGUS

It is quite inevitable that the savvier and digitally capable criminals seeking card data will increasingly direct their efforts to inserting script based browser "skimmers" on websites. It's a tactic also likely to yield far greater returns. After all, even a very active physical card payment device may only process a few hundred or less transactions a day, whereas a busy, international e-commerce website selling desirable goods may process thousands of card details before the rogue code has been detected and removed. For this reason, Requirement 11.6 now mandates that an automated "change- and tamper-detection mechanism" be in place to alert the system owner of any unauthorized changes to their payment pages, or to pages that redirect to fraudulent payment pages. All websites that accept card payments would be advised to start implementing such controls as soon as possible, if they have not done so already.

...AND AN INSIDER TIP

Whilst it is directed under Requirement 11 to conduct internal vulnerability scans at least every three months or upon key changes to the environment, it is not prescribed that you have to use an external QSA or ASV. In fact, the standard categorically states that internal vulnerability scans can be performed by qualified, internal staff so long as they are "reasonably independent" of the system component being scanned.

Requirement 12

Support Information Security with Organizational Policies and Programs

The best security plans are those that do not take place in isolation. The more aware and informed everyone is within the organization, the greater the likelihood of the plans becoming part of the normal business operations. Requirement 12 aims to spread the knowledge so that the entire organization can be part of the security program. **Dimitris Georgiou** speaks concisely—and wisely—about this requirement:

> *Put forward risk-real, minimal, and easy to understand security policies. Maximalist, hyperbolic policy statements can cause control-fatigue, even to well-trained security teams, and can put your organization into dire-straits when scrutinized against the failures that lead to a security breach.*

Dimitris Georgiou
Chief Security Officer

EXPERT INSIGHT FROM DIMITRIS

Train your policy auditors not only to uphold policy, but to routinely challenge and revise it as best fit to your evolving organizational needs. Train the decision makers to accept policy as a business enabler. Train all personnel to appreciate their role as the strongest link in the security chain.

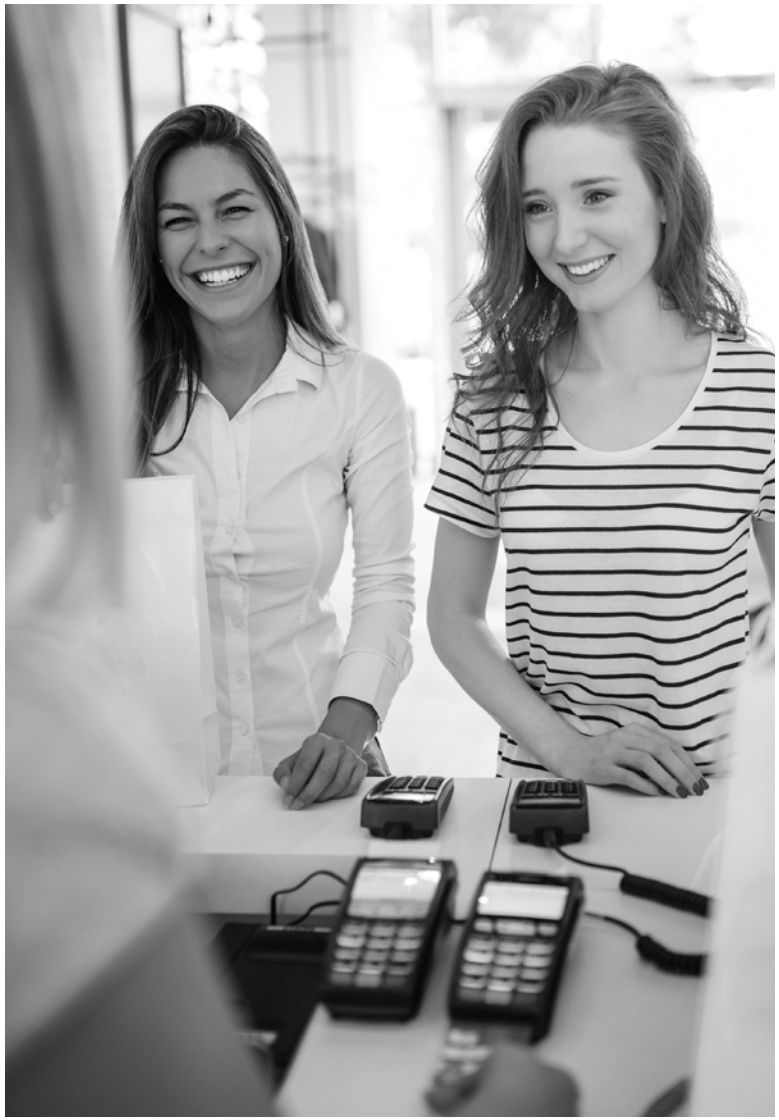
...AND AN INSIDER TIP

Foster risk management procedures designed to minimize exposure while being tailored to your operational and regulatory requirements.

Conclusion

The PCI DSS has a long history and has changed to reflect the need for greater security for payment card data. The latest version continues to emphasize many of best practices established in prior versions, and introduces many new concepts. The information contained in the PCI DSS is a valuable source of knowledge for any organization, not only those that work with payment cards—the Standard serves as a valuable tool to help provide sound security practices. We are confident that this eBook, as well as our self-assessment quiz can add to your tool set to help you confidently transition to PCI DSS version 4.0.

Want to learn more about how Fortra can help you meet your security needs? Visit us here.



FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

fta-tw-gd-0523-r1-hm