fime

PCI DSS

Business enabler,
not technical challenge.

June 2019

fime.com

> PCI DSS compliance is often seen as a challenge that needs to be overcome. But, if approached in the right way and with the right technologies, you can achieve so much more than just time and cost savings. In the right hands, PCI DSS compliance can be a trigger for digital transformation that delivers new kinds of value to your business and customer relationships.

Arnaud Crouzet

VP Security & Consulting at Fime

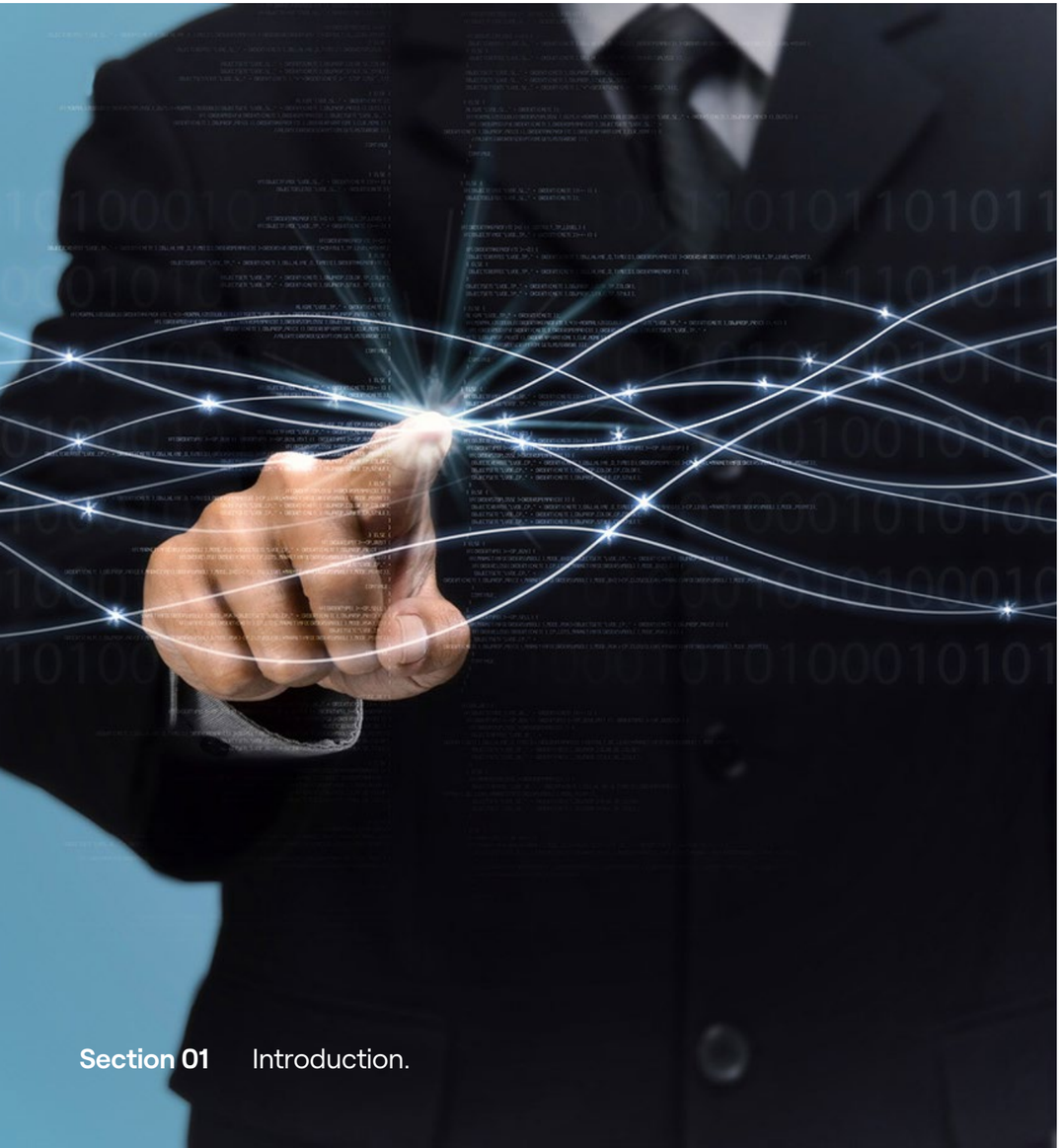
Contents

1. Introduction
2. What is PCS DSS?
3. Understanding the technical challenges
4. Protecting your business
5. Seizing the opportunity
6. Conclusion
7. Fime certification process

1. Introduction.

PCI DSS has been around for a long time but, shockingly, some payments actors do not take it seriously and others do not even know if they fall under its scope. Achieving compliance can represent a significant technical burden but, with the right support, companies can align their compliance efforts with their business goals.

The result? Significantly reduced risk to their business and customers. A new technology infrastructure that operates far beyond security. It will enable you to add value to your business, customers and, ultimately, bottom line.



This eBook will offer a brief insight into the PCI DSS standards, outline the technical challenges actors face and highlight how compliance protects a range of businesses.

Importantly, though, the opportunity will also be explored, showing how compliance not only reduces your scope and risk, but can be a trigger for digital transformation and added value to future proof your business.

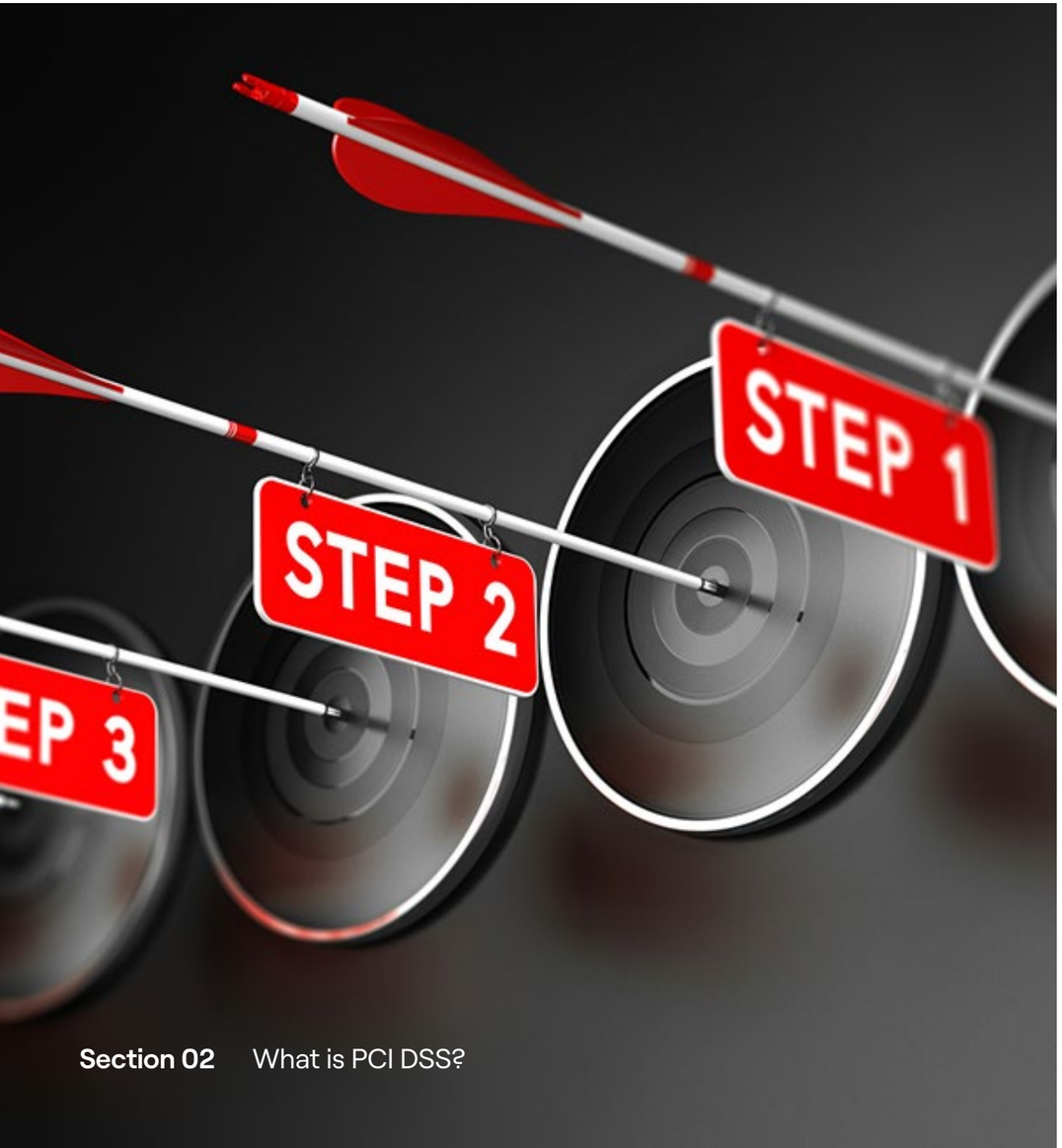
2. What is PCI DSS?

PCS DSS compliance is a requirement for any entity storing, processing or transmitting customer cardholder data.

Whenever a card payment is made – in-store, online or over the phone – the acceptance and processing infrastructure needs to be secure.

To restrict the opportunity for fraud, the major payment brands* created the Payment Card Industry Data Security Standard, known as PCI DSS.

*American Express, Discover, JCB, Mastercard and Visa



Control objectives.

The PCI DSS specifies twelve requirements for compliance, organized into six logically related groups called “control objectives”:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

The birth of PCI DSS

Source : Worldpay

1988-1998

Visa and Mastercard lost $750 million due to credit card fraud program.

2001

Visa is the first to act, publishing the Cardholder Information Security Program.

Early 2000s

Online payments became more common and security breaches increased rapidly.

2004

Major credit card companies create a comprehensive set of security standards for merchants: PCI DSS 1.0 was born.

But why is it important?

Fundamentally, it helps to prevent fraud for both consumers and businesses. This is why compliance should not be viewed as just another box to tick, but as a benefit to your business.

At its most basic level, aligning with the PCI DSS requirements significantly reduces the risk of cardholder data being compromised.

What is ‘cardholder data’?

Cardholder data refers to the full Primary Account Number (PAN) or the full PAN along with any of the following elements:

- Cardholder name
- Expiration date
- Service code

Sensitive Authentication Data, which must also be protected, includes full magnetic stripe data, CAV2/CVC2/CVV2/CID, PINs, PIN blocks and more.

While PCI DSS has been in place for many years, some merchants and other players do not yet comply with the standard. This leaves them open to data breaches that can incur significant negative consequences:

- Funds stolen from customers
- Customer identity theft
- Financial fines to your business
- Reputational damage and loss of customer trust

But it is not all doom and gloom. Yes, achieving compliance can be complex, but by effectively understanding the technical challenges and plotting the right route to compliance, you can:

1. Protect your business and open up opportunities for cost savings
2. Offer added value to customers
3. Develop new services to increase revenues

PCI DSS is a business enabler, not just a technical challenge.

3. Understanding the technical challenges.

When effectively implemented, the PCI DSS requirements combine to deliver layered, nuanced security, making it much more difficult for an attacker to gain access to sensitive data.

The first step to realize PCI DSS as a business enabler is to understand the technical challenges that the initiative represents.

Let’s get technical.

PCI DSS requirements are much more technical than other industry standards, like ISO 27001. Many companies are not used to managing the installation of security solutions, overseeing data encryption, defending systems against malware, developing secure software, and addressing the many other areas that need to be managed across a payment IT infrastructure.

Scope out the situation.

On top of this, defining (and hopefully reducing) the scope is one of the most important phases of PCI DSS compliance. This is where the organization defines the infrastructure that falls under the requirements of PCI DSS and what needs to be done to meet them.

To further complicate matters, PCI DSS also has different rating levels for companies seeking compliance, depending on the volume and types of data transactions performed in their environments.

The initial compliance assessment required for your company is the first step towards an efficient validation process. Defining a narrow scope can bring huge benefits but has to be done without putting payment card data at risk through thorough segregation and compartmentation.
On the other hand, scoping beyond what is necessary raises the total cost and duration of the project.

All of this can be hard to achieve alone.
Few companies have the internal resources or expertise to meet the requirements in an efficient way. Additionally, this project should not be approached with the mindset of simply achieving compliance.

With the right approach and partner, companies can seek to:

- Significantly reduce the scope
- Introduce new technologies and methodologies to increase efficiency
- Deliver new innovative value-added services

4. Protecting your business.

Cyber thieves seek out basic mistakes such as weak passwords, misconfigured technologies and uneducated employees. PCI DSS mitigates these, and other areas of weakness, to protect your business.

In this section

a. Merchants.
b. Public Transport Operators.
c. Processors.
d. Banks.

It may be tempting to just “check the boxes” of the compliance requirements and move on rather than dedicate the required time. But this should be considered as a business concern at the highest levels as the impact of non-compliance could be significant.

And the responsibility does not just sit with merchants. Every entity touched by cardholder data has a role to play: ensuring the security and integrity of their systems to protect cardholder data.

PCI DSS splits companies, not just merchants, into four levels by the volume of transactions per year. These are used to determine fraud risk and to outline the appropriate level of security for their businesses.

a. Merchants.

To ensure that they’re doing everything necessary to meet the compliance requirements, merchants need to verify their transaction volumes from the past 52 weeks with the assistance of their acquiring banks. Merchants at every level must also be sure they’re following all the PCI requirements for their particular levels. Merchants may also need the help of approved vendors or payment processing partners to conduct the validation, since these can also fall inside the scope.

b. Public Transport Operators (PTOs).

Previously, most transport networks used closed-loop systems. With many operators now looking to accept open loop payments, the risk and challenge of managing transactions has increased. Automated Fare Collection (AFC) systems need to store, process and transmit cardholder data in line with the same requirements as any other payment. This is a completely new set of requirements for many operators.

Finding the right partners and technologies will be key to the successful implementation of a smart ticketing scheme, as any loss of trust in the system by users would damage passenger acceptance.

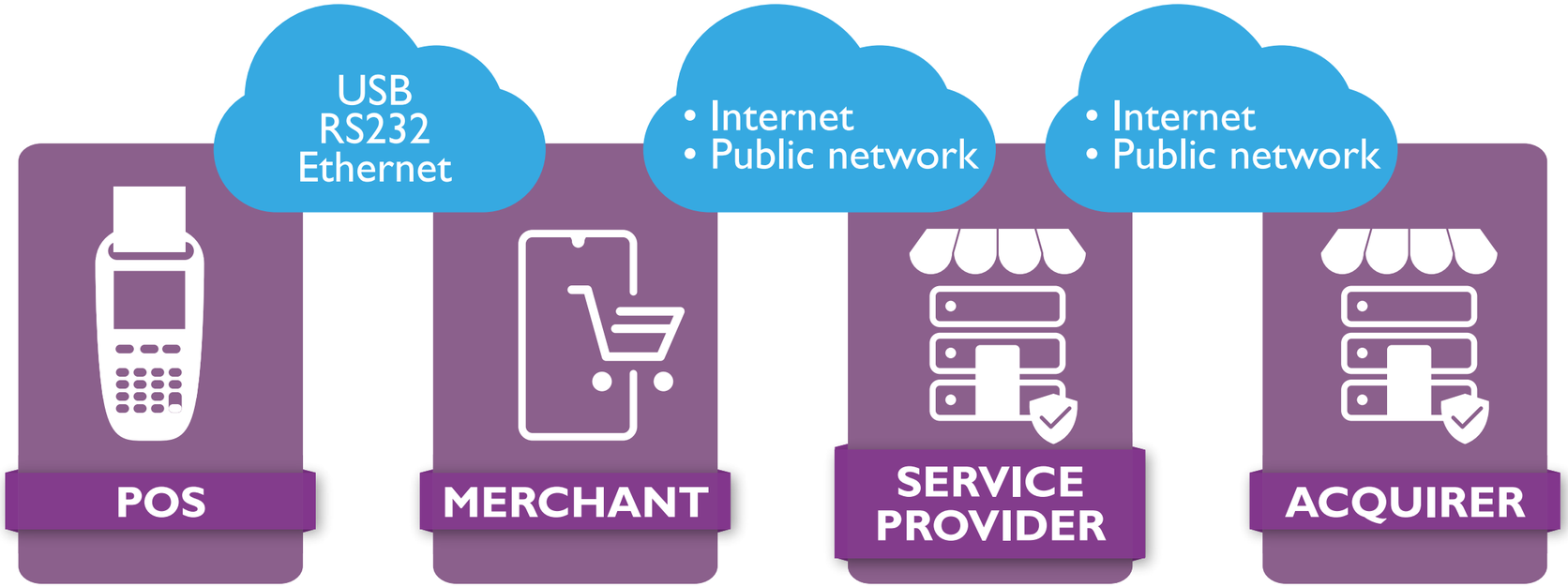
c. Processors.

Processors are directly impacted by PCI DSS and must be compliant. Firstly, it is essential that they effectively protect their own business. In aggregating a huge number of transactions, the impact of fraud could be significant. Secondly, approaching PCI DSS in the right way can be a business differentiator.

Compliance is not just a way to give customers more confidence. In becoming PCI experts processors can offer advice and added value to their merchants, helping them to simplify their own certifications.

d. Acquirers.

Acquiring banks need to support their merchant partners in their security and compliance efforts as the whole payment chain needs to be secured.*

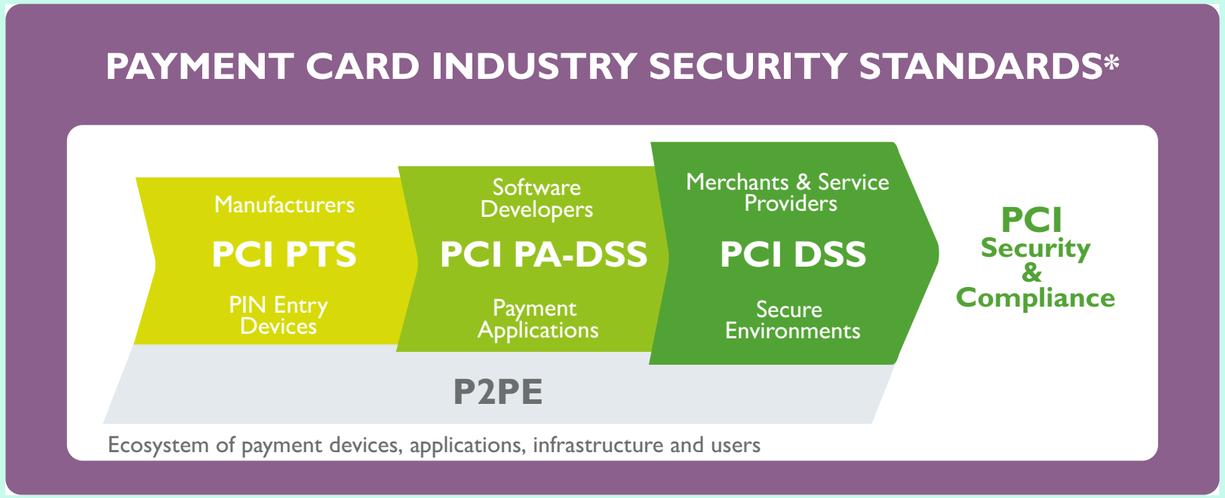


* PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1

At times, acquirers are unsure if they have to be compliant. But banks need to be proactive to protect their business and support customers. They will be initially responsible to the schemes if there is a security issue, before deciding the level of liability to pass to their merchants.

PCI defined security standards address the whole chain.*

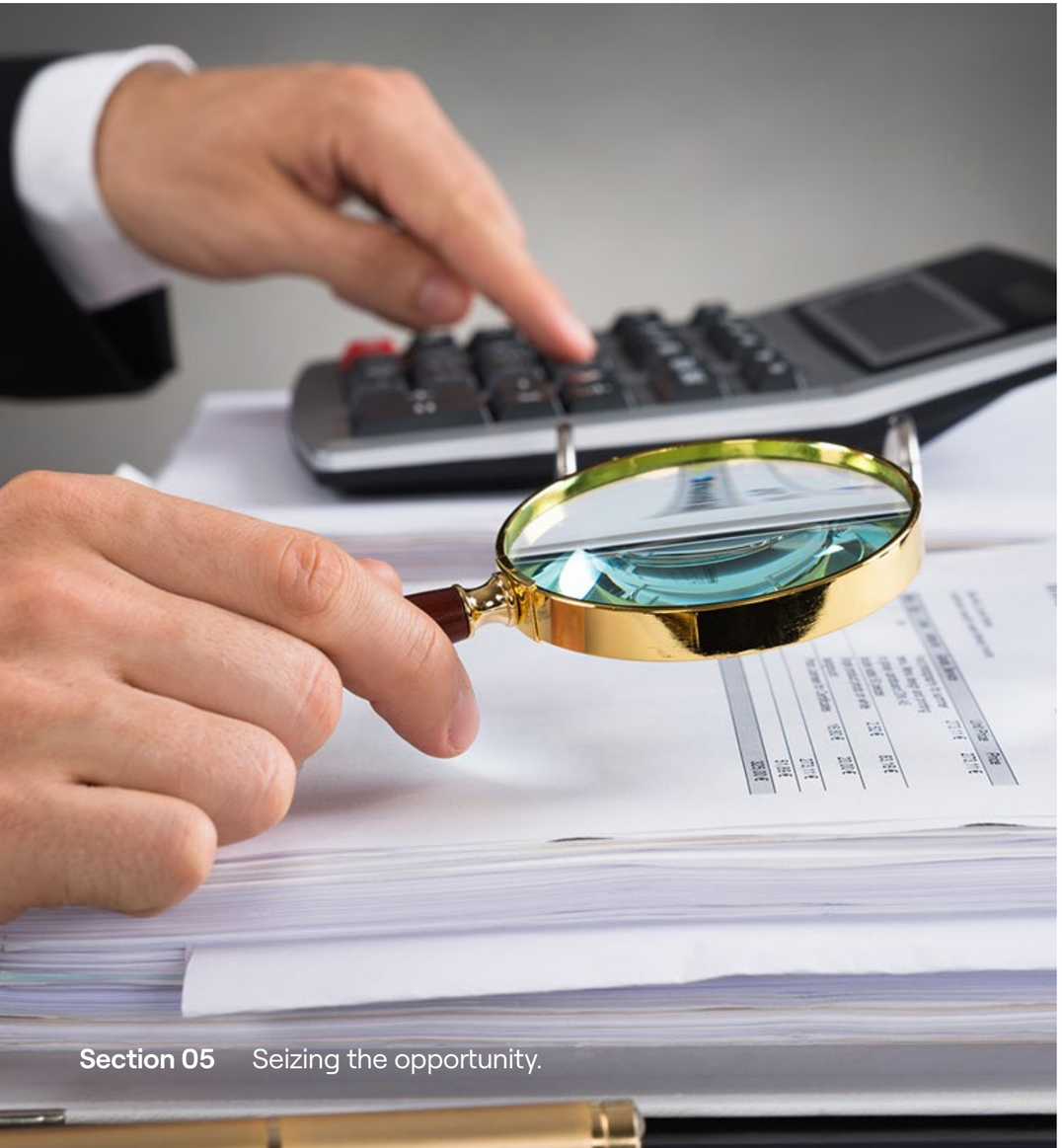
Everyone that is part of the payment transaction chain **has a role to play** when it comes to security.



* PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1

5. Seizing the opportunity.

You need a compliance framework that reinforces your business's objectives while meeting the latest security and privacy requirements.



Yes, PCI DSS compliance can be complex, time consuming and costly. But done in the right way, significant time and money can be saved by reducing the scope and speeding up future compliance efforts.

This is a limited viewpoint: it is far better to look for the opportunities that PCI DSS can deliver.

Scope reduction.

Firstly, let’s focus on scope reduction as it is fundamental to a successful PCI DSS compliance project. Is there a way to reduce the number of systems that fall under the scope and therefore need to be secured?

Think about insuring your house. Without any locks on the doors or windows, your premiums will be high. But, by considering all of the entry points and securing them effectively, you can reduce the risk.

Taking this one step further, by permanently blocking an unused entrance you can change the characteristics of the house to reduce risk (and your insurance premiums!) without impacting the overall house.

This is the pragmatic approach that should be applied to payment infrastructures. Following the PCI DSS rules blindly and attempting to secure the infrastructure that has always been in place can be costly, complex and, in some cases, impossible. The rules need to be applied intelligently, using new methodologies and technologies to do things in different, better ways.

Digital transformation.

Once your payment infrastructure is in place, it can be difficult to both critically assess your own systems and challenge the different parts of the chain (e.g. processors and acquirers). It is very easy to say “It works, so why touch it?”

PCI DSS compliance is the trigger to ask “why do we do it this way? Can we be more secure? Can we be more efficient? How can we do better?”. The resulting systems, approaches and technologies can then be put to work to enable new services.

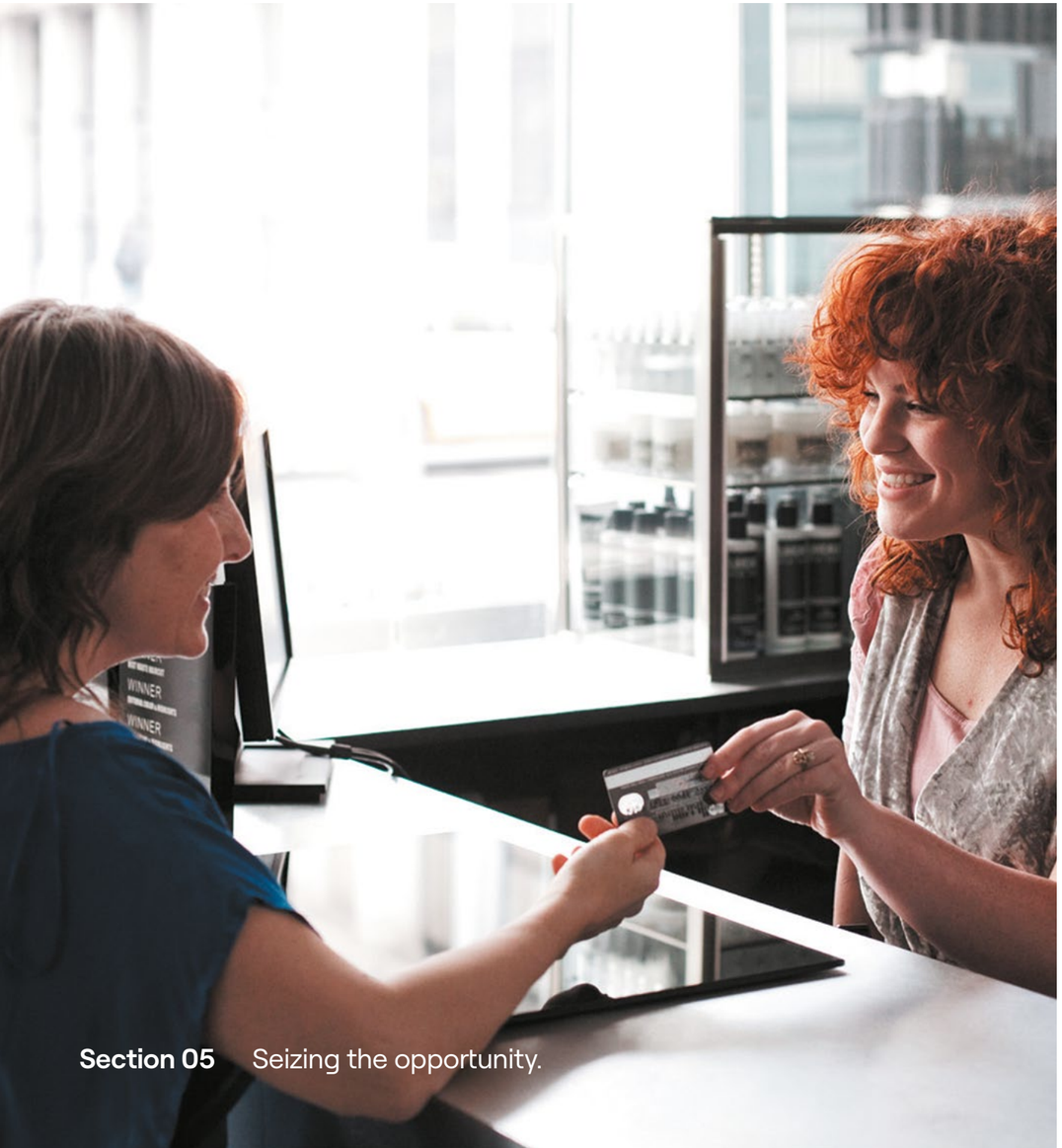
Added value.

As mentioned, the new technologies implemented to intelligently achieve compliance can then be used in supplementary ways to add value and develop new services. For example, payment tokenization technology is used to encrypt cardholder data end-to-end and significantly reduce the scope of your compliance.

On top of this, tokens can also be used to identify customers across omni-channel retail environments to automate loyalty programs without (or alongside) a separate loyalty card. This simplifies life for the consumer and maximizes your investment.

Future proofing.

PCI DSS are currently only applied to transactions routed by the PCI member payment schemes. But they are increasingly considered as a strong benchmark for the universal protection of payment systems and customer data. We can therefore also look to apply the rules to protect instant payment, credit transfers, P2P payments, IBANs and much more.



If your company is already applying PCI DSS for card payments, it can be extended to cover ‘transactions’ generally bringing peace of mind and trust to your business and customers.

6. Conclusion.

It is true that PCI DSS compliance can be complex, time consuming and expensive. But viewing it as a tick-box exercise for your business is short-sighted and risky. In not approaching compliance in the right way, your business could put data at risk while exponentially increasing the cost and time required to become certified. This is without considering the devastating impact that fraud could have.

Look past the technical challenge of PCI DSS to identify the business opportunities.

With a deep understanding of the ecosystem and the nuances of PCI DSS, the rules can be applied intelligently to reduce the scope of your compliance, and consequently the time and cost investment. All of this, while reducing risk. What's more, the right partner can help you to put new technologies and infrastructure to work, adding value to your business and customers.

By working with a strategic partner merchants, PTOs, processors and acquirers can turn certification nightmares into business enablers.

7. Fime certification process.

Fime is an independent payments expert that supports merchants, PTOs, processors and acquirers throughout every stage of PCI DSS certification projects.

We help companies to understand, from business and technical perspectives, what they need to do and how they can make PCI DSS work for their business.

We are a PCI Council participating organisation, and we have a deep knowledge of the PCI rules. Nevertheless we are not a PCI auditors (QSA) checking the boxes.

We want to maintain independence to bring together the right technologies, experts and partners to solve your problems and create business opportunities.

1. Scope identification.
2. Scope reduction.
3. Gap analysis.
4. Corrective action plan.

5. **Implementation support.**

6. **White audit / pre audit.**

7. **Self-assessment questionnaire assistance.** If applicable.

8. **Ongoing support.** Post-audit.

9. **Security compliance audit / Support during the official QSA audit.**
   Official compliance audit.

10. **ASV scans.**
    Internal and external network vulnerability scans.

11. **WiFi Scan.**

12. **Internal and external penetration testing.**

13. **Compensating controls assessment.**

Discover more about how Fime can help your business.

Making innovation possible.

To learn more about how
Fime can help your business:

visit fime.com

or contact sales@fime.com