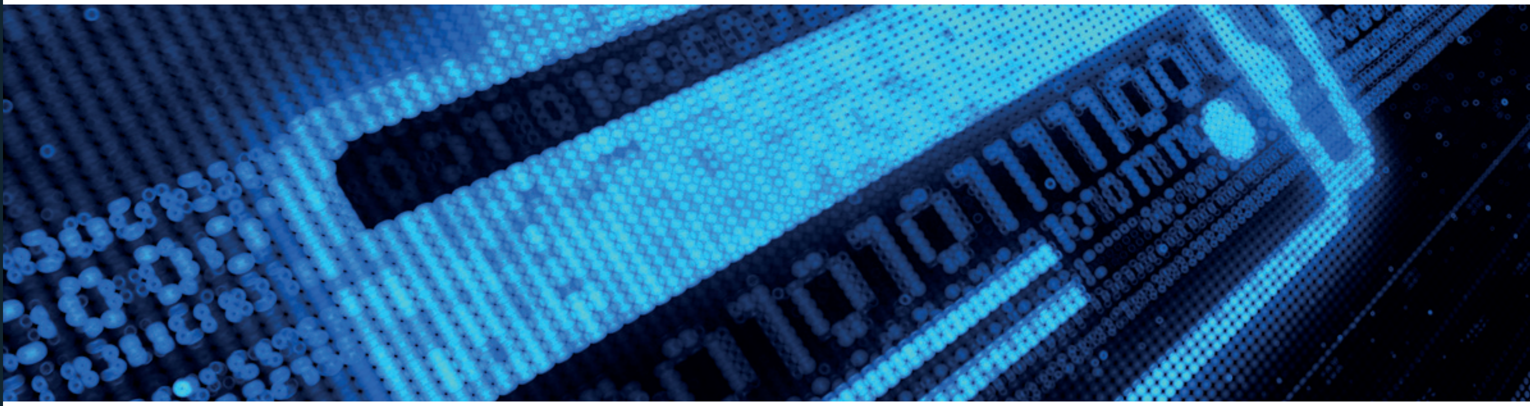
WHITE PAPER

CLOUD HOSTING. SECURED.

SECURITY FIRST:
CLARITY ON PCI COMPLIANCE

WWW.SERVERCHOICE.COM

SECURITY FIRST: CLARITY ON PCI COMPLIANCE



This Security First white paper provides an illustrated view of what has to happen in the end-to-end Payment Card Industry Data Security Standard (PCI DSS). Whilst the process may not be simple, it is clear and straight-forward. Regardless of claims to the contrary, PCI DSS compliance cannot be achieved by a single provider, nor is it simply a one-off exercise. The Payment Card Industry Data Security Standard (PCI DSS) is not considered to be a law on its own, rather it's a regulated set of controls that are mainly focused on cardholder data protection.

There is a fair bit of confusion surrounding this standard, thanks to a mixture of mindsets, resistance to change, and concerns around the cost and effort involved. Much of this confusion stems from varying interpretations, all of which need to cater for a range of factors involved in each specific situation and for each specific business.

> *"PCI DSS is an extremely capable and useful set of minimum requirements that has so far successfully adapted to the changing landscape."*

The truth, though, is simple: the controls are as much business process-related as they are technical, and like all forms of security, much of it comes down to the people within the business. Also true is that PCI DSS is one of the few standards that evolves over time and does not stick with out-dated practices. Though standards can never be perfect, PCI DSS is an extremely capable and useful set of minimum requirements that has so far successfully adapted to the changing landscape.

The proof is also simple: according to a Verizon report of 2015, breached organisations were less compliant with PCI DSS than un-breached organisations.

COMPLIANCE IS AN ON-GOING PROCESS

PCI DSS compliance is an on-going process of three primary functions; assessment, remediation and reporting. While achieving compliance is a significant milestone for any business, the reality includes end-to-end responsibility to maintain all processes, mechanisms and resources to ensure that the business stays compliant.

As illustrated to the right, there are actually a number of recurring elements within those three functions.

> *"PCI DSS compliance is an on-going process of the three primary functions of assessment, remediation and reporting."*

Networks Secured & Controlled

- Managed firewalls
- Strong processes
- Systems hardened

Data Secured & Protected

- Secure and protected storage
- Encrypted transmission

Vulnerabilities Managed Rigorously

- Malware mitigation
- Systems and applications developed and maintained

Access Thoroughly Controlled

- Restricted to need to know
- Unique identifiers
- Regulated physical access

Measures Tested & Monitored

- Constant tracking, monitoring and alerts of resources & data
- Regular system & process testing

Policies Updated & Enforced

- Current, published, communicated
- On-going quality assurance & maintenance

RESPONSIBILITY IS NOT OUTSOURCED

Any business that collects, stores, processes, transmits or otherwise handles cardholder data has the responsibility to provide the proper levels of care to their customers and to adhere to all regulations related to their actions. This includes:

- **Where data enters an organisation**
- **Where data is stored**
- **What data is used for**
- **How data exits the organisation**

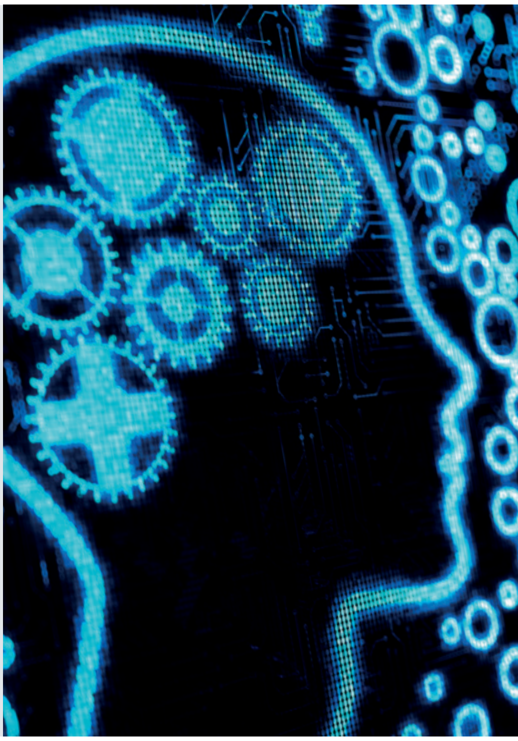
The critical word that crosses each of these is ‘responsibility’. It is generally agreed that outsourcing e-commerce transactions and data management to a payment services provider is often an ideal answer for small and medium-sized business. However, it is important to note that this does not transfer responsibility for PCI DSS compliance, which remains firmly with the business.

> *“The truth, though, is simple: the controls are as much business process-related as they are technical and like all forms of security, much of it comes down to the people within the business.”*

WHY THE CONCERN?

From the clear costs of fines, which can be staggering, through to the impact of a damaged brand or reputation, other consequences of data breaches include:

- **Legal costs from civil litigation**
- **Significant chargeback risks**
- **Negative media coverage**
- **Fines and increased transaction fees from credit card companies**
- **Loss of financial reputation and position**
- **Ultimately, loss of business**



SETTING THE SCOPE

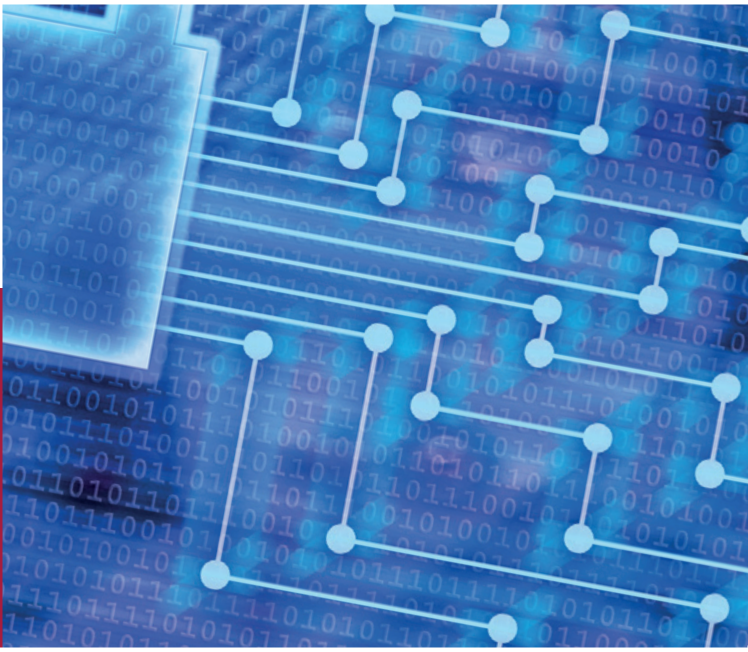
The effort and expense of achieving compliance varies depending on the Self-Assessment Questionnaire (SAQ) you are required to fill in, with the number of controls varying from a few up to 300. See the section **Getting To Grips with SAQs** for more information. The key to requiring a simpler SAQ is defining the right scope: a smaller scope means less time and effort has to be put in, drastically lowering the cost of achieving PCI compliance. Here are some tips for reducing the scope of your PCI compliance.

Firstly, identify all locations where cardholder data exists. This includes systems and processes that comprise the cardholder data, as well as those that provide services to the cardholder data environment (CDE). This defines your scope. Now we can implement a few measures to reduce the scope, making it as small as possible. Segmentation and segregation is a good place to start, effective implementation of which can result in:

- **A reduced surface area that could be attacked thus lowering the risk of a breach**
- **A reduced workload needed to achieve and maintain compliance**
- **Reduced costs for any hardware, software and management support needed**

> *"Even though segmentation is not strictly a PCI requirement, it is a great shortcut to cutting down your scope."*

Even though segmentation is not strictly a PCI requirement, it is a great shortcut to cutting down your scope. There are different segmentation and segregation techniques, one of which is partitioning the underlying network. This typically involves VLANs, firewalls, and IP/port restrictions in addition to access control policies and procedures. Sometimes the whole CDE is zoned, though this can involve redesigning the boundaries of the environment. Through a bit of work up-front, you can save a lot of time and money further on down the line.



UNDERSTANDING THE 12 PCI REQUIREMENTS

Here's an overview of the 12 PCI DSS requirements as laid out by the PCI Security Council, with some helpful information on what they mean in practical terms.

1 **Install and maintain a firewall configuration to protect cardholder data.**
This means that the firewalls and routers within your network infrastructure must be appropriately implemented, tested and managed.

2 **Do not use vendor-supplied defaults for system passwords and other security parameters.**
You must harden your infrastructure by addressing known vulnerabilities and using industry-accepted practices. The infrastructure must also have its functionality limited to only what is necessary.

3 **Protect stored cardholder data.**
If you don't have to store cardholder data then don't! You'll save yourself a lot of work. If you do, then it must be protected according to various legal, regulatory and compliance requirements.

4 **Encrypt transmission of cardholder data across open, public networks.**
Cardholder data travelling across the Internet must be encrypted using strong cryptographic protocols. There's no place for weak cryptography here.

5 **Use and regularly update anti-virus software.**
In-scope systems must be protected by anti-virus and anti-malware tools. These must be actively running, kept current, and regularly evaluated for efficiency as the threat landscape evolves.

6 **Develop and maintain secure systems and applications.**
This includes on-going development and maintenance of your secure applications and systems. You must follow best practices and use change-management processes.

7 **Restrict access to cardholder data by business need-to-know.**
Access to cardholder data and its underlying systems and processes must be limited to only those that need to know. Appropriate access control measures must be put in place.

8 **Assign a unique ID to each person with computer access.**
Every action must be tracked by a person's unique identifier, supported by password management best practices.

9 **Restrict physical access to cardholder data.**
The physical infrastructure that supports your cardholder data must reside in a physically secure and controlled environment.

10 **Track and monitor all access to network resources and cardholder data.**
All applications and systems must produce logs. These logs must be reviewed in order to prevent, detect and minimise any security incidents.

11 **Regularly test security systems and processes.**
The security you've put in place must be verified. This usually takes the form of external vulnerability scans, penetration tests and integrity checks. Your infrastructure must also be monitored using intrusion detection/prevention systems.

12 **Maintain a policy that addresses information security.**
Design, implement and communicate information security policies and procedures to all employees.

GETTING TO GRIPS WITH SAQs

The Self-Assessment Questionnaires (SAQs) are an integral part of the PCI compliance process. Knowing which SAQ to complete can be tricky, though your acquiring bank can advise you on which SAQ they expect you to complete.

We've translated the official definitions into something more understandable and explained them in the table below:

SAQ	Description
A	This SAQ is aimed at 'card-not-present' merchants: namely traders that have outsourced the transmission, processing and/or storage of all card data. To fit into this category, you basically have to ensure that you have nothing to do with the payment information your business takes.
A-EP	This is only for e-commerce traders that use a third party for payment processor such as SagePay or PayPal. You're still not permitted to store, process or transmit any card information yourself, but the link to a third party does put you into a different category and leaves you slightly more at risk.
B	SAQ B applies to merchants using only card imprint machines or dial-out payment terminals. If that all sounds a bit retro, that's because it is. Note that this one doesn't apply to e-commerce traders or those who store cardholder data.
B-IP	Almost exactly the same as SAQ B, except your payment terminals make use of a permanent connection. This doesn't apply to e-commerce traders or those who store cardholder data.
C-VT	Similar to B-IP, but applicable if you're instead manually entering transaction details into an internet-based solution provided by a third party, generally via a web browser. This doesn't apply to e-commerce traders or those who store cardholder data.
C	SAQ C is for companies that run integrated point of sale (POS) systems on a network that only connects to the Internet for authorisation. This doesn't apply to e-commerce traders or those who store cardholder data.
P2PE-HW	As the name suggests, if you are taking payments using hardware that is validated for Point to Point Encryption by PCI SSC, then you fall into this SAQ. This doesn't apply to e-commerce traders or those who store cardholder data.
D	SAQ D is the one to fill in if you store cardholder data. It's also a catch-all for organisations who don't fit into any of the above categories.

> *"Knowing which SAQ to complete can be tricky, though your acquiring bank can advise you on which SAQ they expect you to complete."*

PA-DSS – DO I NEED IT?

You might also have heard of PA-DSS. This is a framework for organisations who develop and maintain payment applications, applying equally to third parties and in-house teams. It can be thought of as an extra step in the PCI compliance process which becomes mandatory as soon as payment applications are used to handle cardholder data. If the development and maintenance of a payment application is outsourced, you must check that the organisation you're using is PA-DSS compliant.

Even if your organisation does not need PA-DSS compliance, the framework can be a useful tool to validate and provide assurance for your organisation's payment application. At its core, the PA-DSS framework will allow you to apply best practices and common sense practices that will strengthen your network and systems. You will get stricter access control, better visibility and, ultimately, lower risk.

WHAT'S NEW IN V3?

Version 3 of PCI requirements became mandatory as of 1st January 2015, replacing the older v2. Until then you had the option to achieve your compliance in either version of the PCI standard, and a few unaware businesses who gained compliance in v2 risk getting caught out. The step from version 2 to version 3 sees some significant changes.

Highlights

Penetration testing is now essential for all in-scope assets under v3. Think of all the hard work you put in to segregate, configure, harden, patch (and so on) your network infrastructure. Now imagine you can still be penetrated thanks to a simple human-error misconfiguration on your firewall. Well, no more: penetration must be done at least once a year and upon significant changes to your technology/environment. Testing is the best exercise of proving that your systems provide a sufficient level of security. Another key improvement is the due diligence that's being exercised to the service providers and third parties that provide any sort of service to your card data environment. So for those who outsource their website's payment application to a third-party development company, PCI is now a requirement for your service providers. If they can't prove compliance, then you are not compliant.

Evolution of existing requirements

The new framework is evolutionary rather than revolutionary, but it's certainly mature, and not a lot of new requirements were expected. What is really beneficial is the direction version 3 of the PCI standard has taken: it has remained flexible enough to be driven by an organisation's current risks and assessments. People and organisations are typically poor at understanding risks, even when experienced in our day-to-day lives. PCI makes the risk management process simple. Why is this important? Good risk management can sustain your business in the market, whilst a bad or non-existent risk management can remove it from the market. It is as simple as that.

PCI MYTHS

There are many examples of myths that organisations believe in order to avoid achieving full PCI DSS compliance. Here, we've presented a selection of the most commonly heard myths and, crucially, explained why they're not to be believed.

As a small merchant who takes a few cards, I don't need PCI compliance

If you are a merchant and are set up to take credit cards by any mechanism, then you need to be PCI compliant.

This can wait until my business grows

The PCI standard applies to all sizes of business and waiting could be costly. Should you be compromised and not be PCI compliant, the fines and the compensation requirements by the banks could be substantial.

> *"Many vendors offer an array of software and services for PCI compliance but, regardless of their marketing material, no single product can fully address all twelve requirements of the PCI DSS standard."*

My bank hasn't mentioned it yet, so I must still have time

The dates for merchants to be PCI compliant are long past and your business is responsible for making sure that it is in compliance with the PCI DSS standard.

We have a provider who will make us compliant

Many vendors offer an array of software and services for PCI compliance but, regardless of their marketing material, no single product can fully addresses all twelve requirements of the PCI DSS standard.

The PCI Security Standards Council urges merchants and processors to avoid focusing on products for PCI security and compliance. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the 'big picture' related to the intent of PCI DSS requirements.

Outsourcing card processing makes us compliant

Whilst outsourcing can simplify payment card processing, it does not provide automatic compliance. Policies and procedures for cardholder transactions and data processing must be in place and being followed by your business. You must protect cardholder data whenever you receive it.

Additionally, you must also ensure that applications and card payment terminals from your provider comply with all respective PCI standards, and that you do not store sensitive cardholder data. You should also expect an annual attestation of compliance.

> *"You must protect cardholder data whenever you receive it."*

Compliance equals certification

There is a significant difference between being PCI compliant and PCI certified. It's fairly easy to achieve PCI compliance: all that's required is the completion of a self-assessment questionnaire, which usually takes about a half day of effort. Certification against the PCI DSS is a comprehensive process involving a full-scale audit by a qualified security assessor (QSA). It covers almost 300 control points and includes how software is developed and how engineers were trained, as well as daily reviews of more than 200 different streams of audit events. The process typically takes six months.

Essentially, it's best to think of compliance as a claim, and certification as proof.

Compliance is a technical problem

Many businesses believe that PCI issues can be managed as a purely technical matter, using tools and features such as anti-virus and encryption. In reality, compliance is more related to people, policies and processes than to the tools that assist. Retail organisations who fail a PCI audit, for example, typically find the reason wasn't poorly-written code, rather it was code that was poorly documented. The ability to become and stay compliant with PCI requirements starts and finishes with the people following your policies and procedures. The technical aspects are probably simpler than you have been led to believe.

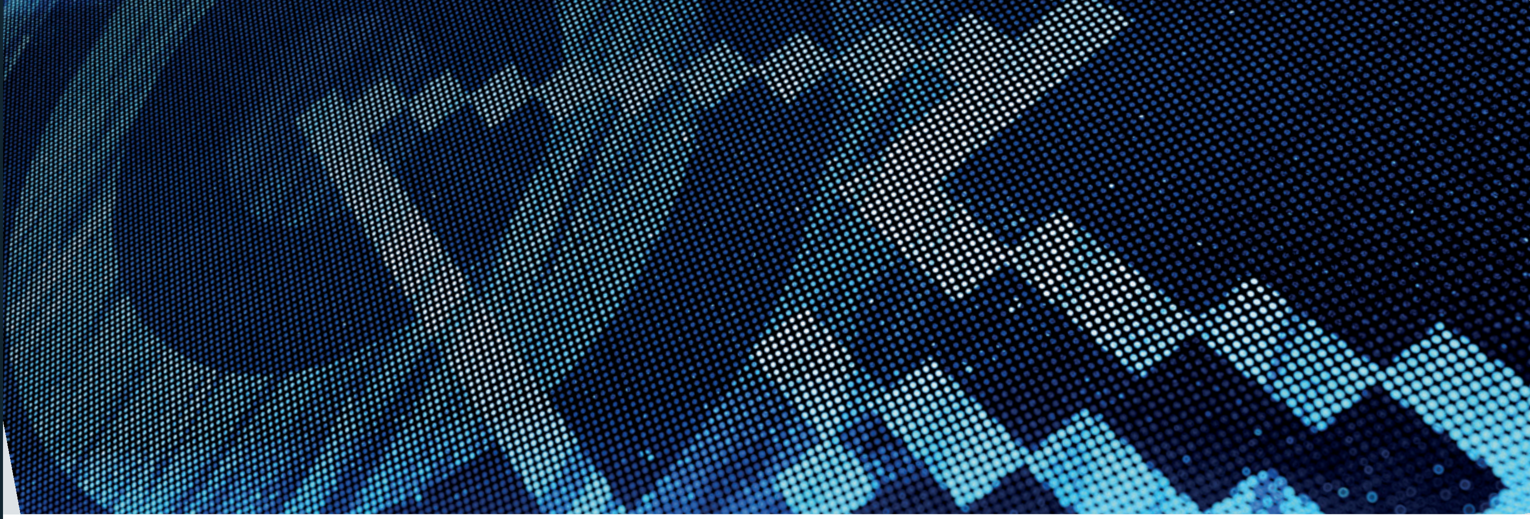
Compliance is forever

PCI compliance is not like a driving licence where you pass the test once: threats are evolving on a day-to-day basis and the PCI compliance targets themselves need regular updates and amendments as a result. As such, PCI compliance should always be viewed as an on-going objective; a process of continuous improvement.

Compliance is easier to manage in-house

External parties who specialise in PCI DSS compliance have already made the significant investments in time, infrastructure and expertise. Outsourcing to them is a much wiser investment than committing to an already-overtasked in-house IT department. Look for a hosting company that's also a Level 1 Service Provider and you'll see that much of the work has been done for you. Plus, they can help get your policies and procedures in-line with stringent PCI requirements.

"ServerChoice follow every single PCI DSS regulation down to the letter."



SUMMARY

PCI DSS compliance is not a simple process, but it is clear and well-defined. Cost is normally seen as a stumbling block, but the reality is that full compliance doesn't have to be expensive. If the time is taken upfront to correctly analyse your organisation and the Card Data Environment (CDE), the scope of compliance can be reduced to the minimum level required. And, much like insurance, PCI DSS compliance will certainly pay for itself in the long run. The most important points to make are that compliance is:

- **Not a choice**
- **Not a one-time operation**

Simply put, PCI compliance is an on-going, auditable process and is designed so auditors can make sure a company is managing all possible risks associated with collecting, storing, transmitting and processing cardholder information. It shouldn't be seen as a burden either: it is an excellent framework to help you stay secure, and ultimately is designed to protect both you and your customers.

> *"The reality is that full compliance doesn't have to be expensive... the scope of compliance can be reduced to the minimum level."*

Get in touch today to ensure that your business and your customers are protected:

+44 (0)1438 532 300

enquiries@ServerChoice.com

www.facebook.com/ServerChoiceUK

www.twitter.com/ServerChoice

CLOUD HOSTING. SECURED.

👤 +44 (0)1438 532 300

✉ enquiries@ServerChoice.com

www.facebook.com/ServerChoiceUK

www.twitter.com/ServerChoice

WWW.SERVERCHOICE.COM