STARTING YOUR PCI COMPLIANCE JOURNEY
PCI Pal is a suite of secure payment solutions designed to descope your contact centre from the requirements of the Payment Card Industry Data Security Standard, but what is the PCI DSS and how can you ensure your organisation is compliant?

To further your understanding, our payment security experts have compiled this starter guide, covering the basics of PCI compliance and some key factors you need to be aware of. Whether you’re planning to go it alone or decide to work with a third-party solution provider, we hope you’ll find this information and expert insight helpful as you embark on your compliance journey.

If there are any questions we haven’t answered or you’d simply like to discuss your specific requirements in more detail, please get in touch. We’d love to hear from you!

GET IN TOUCH

+44 207 030 3770
+1 866 645 2903
info@pcipal.com
www.pcipal.com
Chapter 1
A Beginner’s Guide to PCI Compliance

If you work for a company or contact centre who takes card payments from customers over the phone, you are responsible for keeping that data as safe and secure as possible – not just to protect your customers but to protect your business as well.

Enter the Payment Card Industry Data Security Standard (or PCI DSS as we affectionately know it), a set of 12 binding requirements that are designed to ensure complete data protection for merchants who take card payments from the major card schemes, such as VISA, MasterCard, AMEX, Discover and JCB.

Whether you’ve been referred to us by your bank or you’re in charge of compliance for your contact centre, this is where you’ll find everything you need to know about PCI DSS, including how it works, who it affects, and why it’s so important.

What is PCI DSS?
Set up in 2004 by VISA and MasterCard, and now regulated by the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS is a set of 12 mandatory rules designed to protect data that is processed, transmitted and stored during manual or electronic payment transactions.

Who Does It Affect?
Any organisation that stores, processes or transmits cardholder data from the major card schemes must comply with PCI DSS requirements.
How Does It Work?

The PCI compliance standards work to protect against card fraud by ensuring every business that handles cardholder information does so in a way that keeps customer data secure and protected.

If a contact centre wants to handle card payments from any of the major schemes they must comply with the following 12 requirements:

1. Install and maintain a secure firewall
2. Use unique passwords (rather than defaults)
3. Encrypt stored data
4. Encrypt data during transmission
5. Keep anti-virus software current and updated
6. Regularly check systems and applications are secure
7. Ensure access is restricted to only those who need it
8. Make sure those with access have a unique user ID
9. Ensure physical access to data is restricted and controlled
10. Make sure access to network and data is tracked and monitored
11. Regularly test security systems and incident response plans
12. Have a clear information security policy

Adhering to each of these requirements will ensure PCI DSS compliance for your contact centre, but remember:

PCI compliance doesn’t automatically reduce risk or make you more secure.

Why is PCI Compliance Important?

The PCI DSS requirements are designed to combat card fraud by keeping cardholder data safe from hackers and other security breaches, but it’s not just your customers’ safety that is protected.

By ensuring your contact centre is PCI DSS compliant, you are also protecting your business – both financially and legally. A single data breach is now estimated to cost a company $3m on average, while the loss of connectivity caused by a breach or DDoS attack can prevent businesses operating for long periods of time.

Not only can this negatively affect or even ruin a company’s reputation, it also damages confidence in the industry as a whole.

While PCI DSS compliance is not a legal requirement, it does ensure compliance with the Data Protection Act – protecting you legally should the worst happen.

What are the Risks and Penalties of Non-Compliance?

As mentioned above, PCI DSS compliance is not a legal requirement, but it is mandatory if your contact centre wants to process transactions with the major card schemes.

If a system is compromised and the company is found not to be PCI DSS compliant, the business could face severe penalties, such as brand damage, lawsuits and legal costs, share price drop, job losses, insurance claims, regulator fines, higher banking fees, and potentially, the loss of ability to accept card payments.

These, coupled with the fraud losses, the cost of replacing cards, loss of customer confidence, and the ensuing decrease in sales can all lead to a company suffering huge financial losses or even going out of business entirely.

Rather worryingly, 9 out of 10 large organisations suffered a security breach last year; can you afford to be one of them?
Chapter 2
PCI DSS 3.2: What’s New?

Published earlier this year, PCI DSS 3.2 is the latest version of the standard we all know and love (well, know at least) and has been designed to ensure that security standards are developing and innovating at the same rate as the technology we use and the threats we face.

If you’re responsible for compliance at your contact centre, here’s everything you need to know about the changes...

So, What’s New?

Many of the changes found in PCI DSS 3.2 are simply extensions to, or expansions of, the requirements that were already featured in 3.1; however, there are some greater themes.

The biggest of these is making sure that organisations are working on PCI DSS compliance all year round, rather than only getting everything shipshape for their yearly assessment.

For example, new requirements state that organisations must provide quarterly reviews demonstrating that employees understand and are following the correct security procedures; that a change-management process must be implemented to ensure any changes to a system (such as new apps, programs or devices) are monitored and compliant; and that DESV requirements will now be incorporated into PCI DSS.

There is also a much bigger emphasis on ensuring service providers do not compromise the security of their customers and that their compliance can also be demonstrated on a regular basis. For example, service providers will now have to report system failures, establish a structured PCI DSS compliance programme (with defined responsibilities at executive management level) and perform penetration testing every six months at a minimum.

Lastly, one of the biggest changes from PCI DSS 3.1 is that multi-factor
authentication will now be a requirement for all non-console administrative personnel, rather than just those accessing data remotely.

**What is DESV?**

DESV, or Designated Entities Supplemental Validation, is like a more advanced version of PCI DSS that is sometimes required by payment brands or acquirers to ensure maximum data security on a regular basis (rather than just for PCI DSS assessments).

While DESV assessments will still only be necessary if requested by an acquirer or payment brand, incorporating the regulations into PCI DSS 3.2 is intended to encourage organisations to see whether the standards could be applied to their own systems, and to promote year-round vigilance.

**What is Multi-Factor Authentication?**

Multi-factor authentication is the process by which someone has to supply two or more examples of authorisation or identification in order to be granted access to sensitive material or systems. These can include passwords, security cards, fobs or biometrics.

In previous iterations of PCI DSS, personnel have been required to undergo two-factor authentication when acting remotely, but PCI DSS 3.2 now states that multi-factor authentication will be a requirement for all non-console personnel accessing data or changing systems from anywhere, including within their organisation's trusted network or data safe zone.

Changing the name from two-factor to multi-factor has been done to demonstrate that two levels of authentication are now the bare minimum.

**When is All This Happening?**

While the previous PCI DSS 3.1 officially retired on October 31st, the changes aren't as scary as that date might suggest; organisations have until February 1st 2018 to implement all 3.2 requirements and any changes will be considered ‘best practice’ until then (although the PCI Security Standards Council does recommend adopting the standard ASAP for your own security and peace of mind).

**What Do I Need to Do Now?**

The good news is that, if you’re already working with us here at PCI Pal, a large part of the work is done as we are already fully PCI DSS 3.2 compliant. If not, there’s no need to worry unduly; as we mentioned before, all organisations have until 1st February 2018 to make sure they’re compliant, so you have plenty of time to implement any necessary changes. We would, however, recommend getting started as soon as possible – partly because the new requirement for more regular monitoring and reporting will make upcoming PCI DSS assessments a lot easier.

It’s always good practice to make sure your security systems and procedures are as up-to-date as possible and functioning as they should be, so take this opportunity to review and reassess the way your contact centre handles and stores data and the way this data is accessed.

Reevaluate your security systems and start testing them regularly, both to get into the habit of compliance and to keep your data as secure as possible. If you do use third-party service providers, it’s also a good idea to check that they’re aware of and implementing the new regulations that apply to them, to ensure that they’re protecting your customers’ data as effectively as you are.
Chapter 3

What are Merchant Levels?

If you take card payments for goods or services via any of the 5 members of the PCI SSC (Payment Card Industry Security Standards Council), you will be required to meet one of four levels of compliance as part of your PCI DSS assessment.

Known as “merchant levels”, your compliance requirements will vary depending on several factors, including the number of transactions you process annually and your history of processing transactions.

In this guide, we’ll be explaining what merchant levels are and which merchant levels apply to different types of business. But first, it’s time for a quick refresher...

What is the PCI SSC?

The PCI SSC is a regulatory body formed by and comprised of the world’s five biggest card payment providers; Visa, American Express, Discover Financial Services, JCB and MasterCard.

Working together in an independent capacity, these payment vendors collaborate in an effort to continually improve the PCI DSS (Payment Card Industry Data Security Standards), with the goal of protecting customer card data and reducing the potential for fraud and/or data breaches.

What are Merchant Levels?

Merchant levels are one of the tools the PCI SSC uses to improve safety and security when it comes to payments and customer data. Although compliance with the rules laid out by these merchant levels is not a legal requirement, any company (including contact centres) which accepts card payments from the big 5 will need to comply or risk potential financial penalties.

There are four different categories that your organisation may fall into, defined primarily by the number of transactions you process, but also by the security risks you might be facing. These criteria allow the PCI SSC
to determine the possible risks your customers might face when transacting with you, and thus, informs which level of security they need to enforce in order to improve their safety.

Which Merchant Level Does Your Contact Centre Fall Into?

The following guidelines will help you decide which merchant level applies to you and which steps you need to take to ensure PCI DSS compliance:

Merchant level 1

Merchant criteria:
- You process 6,000,000+ transactions annually
- You have been the victim of a data breach which compromised account data
- You have been identified by a card association as merchant level 1

Validation requirements:
- Undergo an annual on-site security assessment by a PCI SSC-accredited Qualified Security Assessor (QSA)
- Conduct annual penetration testing via an Approved Scan Vendor (ASV)
- Complete an attestation of compliance form

Merchant level 3

Merchant criteria:
- You process between 20,000 and 1,000,000 ecommerce transactions annually

Validation requirements:
- Undergo an annual Self-Assessment Questionnaire (SAQ)
- Conduct annual penetration testing via an Approved Scan Vendor (ASV)
- Complete an attestation of compliance form

Merchant level 4

Merchant criteria:
- You process fewer than 20,000 ecommerce transactions annually
- You process fewer than 1,000,000 non-ecommerce transactions annually

Validation requirements:
- Undergo an annual Self-Assessment Questionnaire (SAQ)
- Conduct annual penetration testing via an Approved Scan Vendor (ASV)
- Complete an attestation of compliance form

Merchant level 2

Merchant criteria:
- You process between 1,000,000-6,000,000 transactions annually

Validation requirements:
- Undergo an annual Self-Assessment Questionnaire (SAQ)
- Conduct annual penetration testing via an Approved Scan Vendor (ASV)
- Complete an attestation of compliance form
Chapter 4
Which Self-Assessment Questionnaire (SAQ) is Right for You?

If your business, organisation or contact centre processes fewer than 6 million transactions annually, you may be able to ensure PCI compliance via a Self-Assessment Questionnaire (SAQ).

The type of assessment you must undergo will vary according to your merchant level, but if you are at a level which allows for SAQ submission instead of a full, formal audit each year, you will need to deliver your SAQ and Attestation of Compliance (AoC) via a responsible party at your business – typically your chief financial officer (CFO).

Choosing the Right SAQ for Your Business

The very first step towards correct completion is to choose the right SAQ in the first place. Because organisations come in all shapes and sizes, one size doesn't fit all. This is why a range of SAQs has been developed to suit a variety of business types. So, which SAQ is right for you?

**SAQ A**

*Who is it for?*
"Card not present merchants" including contact centres, ecommerce businesses and mail order companies which outsource cardholder data processing functions to a PCI compliant 3rd party service provider. This means that these businesses never deal with cardholder data at any point.

*Actions required*
- Paper copies of cardholder data must be destroyed or protected.
- Details of 3rd party service providers must be kept.
- Compliance of 3rd party services must be monitored.

**SAQ A-EP**

*Who is it for?*
Ecommerce merchants which partially outsource payment processing to
a PCI-compliant 3rd party service provider. Depending on the merchant’s payment process (for example, if some parts of the payment form are completed on the merchant’s site before the customer is redirected to a 3rd party payment gateway) this type of SAQ may be applicable.

Actions required
Any ecommerce merchant formerly using SAQ A should read guidelines to identify whether they should now complete the new SAQ A-EP form instead.

SAQ B

Who is it for?
Merchants processing payments via standalone terminals or imprint-only machines who do not use electronic cardholder data storage.

Actions required
Completion of SAQ B form, particularly to ensure terminals (which can now connect via Bluetooth, Ethernet and GSM/LTE) are isolated from networks and therefore not putting cardholder data at risk.

SAQ C

Who is it for?
Merchants without electronic cardholder data storage who take payment via an internet connected application. These are usually widely used pieces of software connected to a standalone machine, operated by small, “bricks and mortar” businesses.

Actions required
Completion of SAQ C form, particularly to ensure the technology used to enter cardholder details is isolated from other networks and is strongly protected.

SAQ P2P E

Who is it for?
Merchants processing card data via PCI SSC-listed, P2PE (Point-to-Point Encryption) payment terminals. This can include physical and remote transactions.

Actions required
• Completion of SAQ P2PE form.
• All data must be entered via a validated P2PE hardware device.

SAQ D

Who is it for?
Service providers and merchants who do not meet the criteria for any of the above questionnaires.

Actions required
Completion of SAQ D which includes all 200 PCI DSS requirements, marking non-applicable sections with caution.
Chapter 5
What is a Qualified Security Assessor (QSA)?

A Qualified Security Assessor (QSA) is an impartial third party hired by a merchant to conduct an assessment and offer advice on how it can become compliant with the Payment Card Industry Data Security Standard (PCI DSS).

What Does a QSA Do?

The involvement the security assessor has in the process depends on the ‘level’ a merchant has been assigned. All merchants fall into one of four merchant levels based on their Visa transaction volume over a 12-month period. Level 3 and 4 merchants, which are typically small-to-medium sized businesses, will not necessarily need the assistance of a QSA to be PCI compliant.

Level 1 and 2 merchants will require an onsite assessment and an annual Report on Compliance (ROC) completed by a QSA. During the PCI assessment, the QSA will determine whether the organisation has met the 12 PCI DSS requirements before completing an ROC.

How Does Someone Become a QSA?

To qualify as a QSA, an individual must meet information security education requirements and receive appropriate training from the PCI Security Standards Council. They must also be full-time employees of an approved PCI security and auditing firm and be re-certified annually.

Because the quality of PCI DSS validation assessments can have a significant impact on the application of the security measures and controls, the qualification requirements they must meet are demanding and detailed. Once an applicant has been accepted by the PCI SSC, they then have to complete the two-day QSA training course and pass an open-book exam. They will then receive official certification.
How Do They Interact with Internal Security Assessors?

Internal Security Assessor (ISA) sponsor companies are organisations that have been qualified by the PCI SCC. The council runs an Internal Security Assessor Programme, which gives employees of ISA sponsor companies the opportunity to receive training and earn a qualification.

The aim of this training is to improve the organisation’s understanding of PCI DSS and the requirements they must meet to be compliant. It will also help to improve an organisation’s interactions with Qualified Security Assessors and enhance the reliability, quality and consistency of PCI DSS self-assessments. The result is the proper and consistent application of PCI DSS measures and controls.

How Should You Choose a QSA?

As in any profession, there can be considerable differences between the technical skills of individual QSAs, so ultimately the security of your card payments is only as good as your assessor.

There are three questions you should ask to give your organisation the best chance of hiring a reputable and thorough Qualified Security Assessor (QSA):

1. **What type of organisations have they performed PCI DSS assessments for?**

The type of organisation a QSA has worked for in the past is important because the payment card processing equipment and applications tend to vary from sector to sector. Using an assessor with prior experience in your industry can improve the level of security guidance provided.

2. **What is their background?**

The experience and background of the QSA you should look for depends on the particular aspects of PCI DSS compliance you wish to improve. Firms with considerable experience of information security might be more expensive, but you generally get what you pay for.

3. **Who will be carrying out the work?**

It can be the case that you have discussions with a particular QSA to ascertain their suitability for the work, only for a different QSA to carry out the work. Make sure the assessor you have been talking to is the same assessor who arrives on site.
Chapter 6
What is Multi-Factor Authentication?

Before PCI DSS 3.1 expired in October last year, multi-factor authentication (MFA) was only required for remote access to any cardholder data environment (CDE). With the introduction of the new PCI DSS 3.2 however, multi-factor authentication is now required for any personnel with non-console administrative access, as part of Requirement 8.

With these measures becoming such an important part of CDE security, here’s everything you need to know about multi-factor authentication.

So, What is MFA?

Multi-factor authentication is simply a security system that requires more than one type of identification or authentication before allowing user access. The term can refer to two-factor authentication or higher. The forms of authentication required usually encompass knowledge, possession and inherence, i.e. something the user knows, something they possess and something they are.

Examples of these include:

**Knowledge** – a password, login number, username or PIN.

**Possession** – a physical object, such as a key, swipe card or token.

**Inherence** – biometric identifications, such as fingerprints, iris scans or voice recognition.
**Why is MFA Useful?**

The idea behind multi-factor authentication is pretty uncomplicated; it simply makes accessing sensitive data more difficult, providing potential hackers with more barriers than just a simple password. By requiring several, separate identification factors, the system is less easily compromised, making cardholder data environments safer from unauthorised access.

**Protection of Authentication Factors** – to meet validation requirements for PCI DSS 3.2 Requirement 8, each factor of authentication needs to be protected. This simply means passwords should be secure and difficult to guess, while hardware or biometric data should be kept private and safe from unauthorised replication. Factors should also not be verified on a step-by-step basis as this could allow unauthorised users to determine the validity of individual factors over time.

**Laws and Regulations** – it’s important to keep your local laws and regulations in mind as well as the requirements made by PCI DSS 3.2. For example, both the European Union Directive on Payment Services and the Federal Financial Institutions Examination Council have additional requirements when it comes to consumer payments authentication or high-risk transactions.

**When Do I Need to Use MFA?**

According to the new PCI DSS 3.2 requirements, all organisations will need to implement multi-factor authentication systems for any non-console administrative access. This means any access to your system over a network, even if this is a non-remote on-site network that is already considered ‘safe’.

While PCI DSS 3.2 is effective now, businesses will have until February 2018 to implement any new MFA systems.

**What are Some Key MFA Best Practices?**

Guidance recently released by the PCI Security Standards Council states a few simple ideas for MFA best practice. Here are some to keep in mind:

**Independence of Authentication Mechanisms** – organisations need to make sure that the mechanisms used to authenticate different factors are independent from one another and cannot compromise one another.
Chapter 7

What is Point-to-Point Encryption (P2PE)?

If you’re responsible for PCI DSS compliance at your company, the idea of being able to reduce the lengthy and complicated self-assessment process, as well as your costs and accountability for data breaches, no doubt sounds too good to be true.

Fortunately, such a possibility does exist and it comes in the shape of Point-to-Point Encryption or P2PE. If you’d like to find out more about P2PE (whether it’s right for your contact centre and how it might be able to descope and reduce the cost of your PCI DSS assessments), here’s our handy guide...

What is P2PE?

Point-to-Point Encryption is a standard set of requirements created by the PCI Security Standards Council to ensure maximum security for payment card data. It involves the secure and undecipherable encryption of data from the moment a card is swiped or payment details taken, to the moment the relevant banking service receives those details.

The standard is intended to be met by a P2PE solution, a comprehensive service providing devices, secure software and everything else that is needed to meet P2PE requirements. Solutions are delivered by specialist P2PE providers – third parties responsible for designing, supplying and maintaining a validated P2PE service.

How Does P2PE Work?

P2PE works by encrypting card information from the moment it is taken (known as the point of interaction or POI), using an algorithm that turns the data into unreadable codes. These codes are then transferred directly to the processor where they are decrypted automatically using a secure key, before being passed onto the relevant bank.
Since the decryption is carried out electronically, the merchant or processor does not have to decrypt data manually nor do they need access to the secure key; therefore, they never have access to their customer's personal card data. The P2PE solution will even supply a token to the merchant with each transaction, helping them to identify and refund or rectify a payment at a later date, without ever revealing the card information.

Isn’t That Just End-to-End Encryption?

While many E2E and P2P solutions are similar, P2PE only refers to encryption solutions that specifically meet the PCI Security Standards Council’s requirements. Many E2E solutions don’t meet the standard because they include other systems between the POI and the point of processing, elevating the risk of fraud or hacking.

P2PE transfers data directly from the point of interaction to the point of processing, with no other systems in between – hence the name Point-to-Point – making it a much more secure (and much quicker) process.

P2PE is also an assessable, validatable standard, whereas E2E has no standards or requirements protecting data once it has been taken.

How Can P2PE Help Descope & Reduce PCI DSS Assessment Costs?

The best thing about a P2PE solution from a contact centre’s perspective is that all accountability for PCI DSS compliance is automatically the solution provider’s responsibility. It’s down to the solution provider to ensure all the requirements of the standard are met and that they are providing a complete and secure system.

If fraud or a data breach does occur, the P2PE solution provider will be held accountable for any ensuing fines or penalties, rather than the merchant.

This passed-on accountability also makes PCI DSS assessments much easier for a merchant using a P2PE solution. For example, on the PCI DSS compliance self-assessment questionnaire (SAQ), an organisation responsible for their own encryption has to go through 12 sections and 329 questions, whereas those using a P2PE solution provider only have to cover four sections and 35 questions.

Reducing this lengthy assessment process not only saves time but also money.

Where Can I Find PCI-Validated P2PE Solution Providers?

When it comes to choosing a P2PE solution provider, there are some big names that you will have already heard of. MasterCard, WorldPay and Verifone are all well-known examples of PCI-validated P2PE solution providers, but for a more comprehensive selection you can also check out the PCI Security Standards Council’s directory of Point-to-Point Encryption Solutions.
Chapter 8

What is Tokenisation?

PCI DSS (Payment Card Industry Data Security Standards) are no walk in the park for organisations and contact centres to comply with. Yet these standards are absolutely critical for businesses that want to process payments with any member of the PCI SSC (Security Standards Council), including Visa, MasterCard, American Express, Discover Financial Services and JCB.

PCI compliance is also essential for businesses that appreciate how important it is to protect customer data and their own security, particularly when it comes to preserving customer trust and the brand’s reputation.

Ultimately, adhering to these standards is difficult, but it’s also a huge priority which must be handled carefully and effectively. But there are solutions which can make the whole process simpler...

Choosing a PCI Solution

If you’ve been searching for a PCI compliance solution which takes the burden away from your business, you’ll no doubt have come across reams of information, acronyms, technical terms and options.

Many of these solutions apply only to specific types of business (i.e. ecommerce merchants or small, bricks and mortar enterprises), others require varying amounts of input and co-operation with your business, making it tricky to know which route is right for you.

Introducing Tokenisation

In this quick guide we’ll be taking a closer look at one potential solution, which is becoming increasingly prevalent amongst organisations that process payments over the phone; tokenisation.
What is Tokenisation?

Tokenisation is a process which helps businesses who process telephone payments to reduce the burden of PCI DSS compliance by allowing them to store less cardholder data on their systems. When no data of this type is stored, the amount of compliance which needs to be conducted is greatly reduced.

The process replaces Primary Account Numbers (PANs) and other sensitive data (i.e. credit card numbers) with a “token” when they are shared via a telephone transaction. Each token is a randomly assigned replacement value, which ensures it cannot be reverse-engineered. As it is not an encryption or code, it also cannot be broken by hackers to give access to customer details.

The real data is then captured and securely stored in a data vault, typically operated by a PCI-approved third party service provider, removing the need for businesses to store vulnerable data which requires significant PCI protection on their systems.

What are the Benefits of Tokenisation?

When businesses process payments via telephone, customer data may be stored on their systems or it might be conveyed via keypad touch tones. Unfortunately, because contact centres and their ilk are typically part of large, sprawling and interconnected businesses, it is very difficult indeed to keep this data safe and inaccessible.

Tokenisation means that customer data never even reaches the company itself. Instead, companies store each identifying token, while a specialist third party provider takes care of processing the payment and storing the information securely.

This process doesn’t just keep customer data safe, protect the reputation of businesses and mitigate the impact of security breaches, it also relieves organisations of many of the PCI DSS compliance hoops they must jump through annually or even quarterly.
Chapter 9
Your Annual PCI Checklist

If you operate a contact centre that takes card payments from customers over the phone or via SMS and web chat, there are certain checks you must perform to ensure the security of cardholder data.

The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for organisations that handle card payments from the major card schemes, including Visa, MasterCard, American Express, Discovery and JCB.

To remain compliant, the following checks must be performed annually to maintain security and mitigate the risks of a compromise of card or personal data. It’s worth noting that if you’re using a hosted solution like PCI Pal then most of the PCI DSS requirements will already be met.

Although the Payment Card Industry Security Standards Council (PCI SSC) sets the security standards, each card provider also has its own programme for compliance, validation levels and enforcement.

Compliance is not enforced by the PCI SSC however, but rather by the individual card issuer or acquiring banks.

You can find more information about compliance for each card scheme from the following links:

- American Express – [americanexpress.com/datasecurity](http://americanexpress.com/datasecurity)
- Discover Financial Services – [discovernetwork.com/fraudsecurity/disc.html](http://discovernetwork.com/fraudsecurity/disc.html)
- Visa Inc – [visa.com/cisp](http://visa.com/cisp)
- Visa Europe – [visaeurope.com/ais](http://visaeurope.com/ais)
**What is the PCI Compliance 3-Step Process?**

There are three continuous steps that should be carried out to ensure PCI DSS requirements are met:

1. **Assess** – You must identify cardholder data and take an inventory of your IT assets and business processes for payment card processing, then assess them for vulnerabilities that could lead to a compromise of cardholder data.

2. **Remediate** – You must fix any vulnerabilities and not store any cardholder data that you do not need.

3. **Report** – The final step is to compile and submit compliance reports to the banks and card schemes you do business with, along with any remediation validation records if applicable.

**Which PCI Standards Do I Need to Maintain?**

Your merchant level dictates the standards you will need to maintain for PCI DSS compliance. There are four levels of merchant based on the number of transactions you process every year. This dictates whether you need an annual security assessment carried out by a PCI SSC-accredited qualified security assessor (QSA), or if you can complete a self-assessment questionnaire (SAQ).

**What Annual Checks Should I Perform in My Contact Centre?**

Regardless of the assessment method required, the following steps must be taken each year:

- Complete an annual risk assessment
- Ensure third parties that store, process and/or transmit card data have maintained their PCI DSS compliance and are still registered with the card schemes
- If you are using a third party application in your contact centre, make sure the product and particular version you are using is Payment Application Data Security Standard (PA DSS) compliant
- If you use an integrator to bring the products together, make sure they are certified to the required standard to do so
- Train your staff to follow PCI DSS procedures
- Make sure you only store data that is essential and that it is encrypted and/or masked
- Protect your data network and make sure you are using a firewall and up-to-date anti-virus software
- Perform network scans on a quarterly basis. These have to be performed by an approved scanning vendor (ASV)
- You should also discuss security with your web hosting provider to ensure they have secured their systems appropriately. Web and database servers should also be hardened to disable default settings and unnecessary services
- Annual pin entry device (PED) tests need to be run to identify any vulnerability
- Any software or hardware you use to process transactions should have approval from the Payment Card Industry Security Standards Council (PCI SSC)

**Reduce Your PCI Compliance Concerns**

If this all sounds like a lot to deal with, you might like to consider partnering with a hosted PCI solution provider. Our smart PCI solutions, like Agent Assist, can be seamlessly integrated with your contact centre operation to ensure compliance without compromising the customer experience.
Chapter 10

PCI Glossary

When it comes to PCI DSS jargon, are you A-OK or are you more “WTH?”?

Whether you know your POS from your POI or you wouldn’t know a QSA if one bit you on the nose, our glossary of PCI terms is bound to come in handy at some point. Here are just a few of the terms you’re likely to come across on your PCI DSS compliance journey.

A PCI Glossary

**Acquirer** – The financial institution that processes your payment card transactions.

**Agent Assist** – A secure, PCI DSS compliant solution that uses DTMF masking to disguise a customer’s key tones when a contact centre agent takes a payment over the phone.

**AOC** – Attestation of Compliance – a form that allows you to attest to your PCI DSS assessment results.

**Audit Trail** – A sequential log of your system activities.

**CDE** – Cardholder Data Environment – The entire environment (personnel, software, and hardware) in which data is stored, processed, and/or transmitted.

**Console/Non-console Access** – Direct or indirect access to a mainframe, server, or system.

**CVSS** – Common Vulnerability Scoring System – A method of ranking the seriousness of system vulnerabilities.

**Data-flow Diagram** – A comprehensive diagram documenting the flow of sensitive data through your system or network.

**DESV** – Designated Entities Supplemental Validation – An extra level of security validation required by some payment brands or acquirers.
DPA – Data Protection Act – the Act and relevant legislation regarding data security in the UK.

DTMF – Dual-Tone Multi-Frequency signalling – the system that recognises and processes the key tones on your phone.

DTMF Masking – Disguises the key tones as a contact centre agent takes a payment over the phone by masking them with a monotone beep so that the agent has no way of accessing card information.

De-scope – To remove your contact centre from the scope of PCI DSS entirely by using a third party service provider to process, transmit and /or store all card data.

DoS – A denial-of-service attack in which a hacker disables a system by overloading it with requests.

E2E – End-to-End Encryption. An encryption solution that does not meet P2PE standards.

GDPR – General Data Protection Regulation – The EU’s new standard for data security.

ICO – The Information Commissioner’s Office – the UK’s data protection regulator.

IDS – Intrusion detection system.

IPS – Intrusion prevention system.

IVR – Interactive Voice Response – An automated system that allows a computer to recognise and process speech and DTMF tones.

Multi-factor Authentication – The requirement of two or more levels of authentication to gain access to sensitive data or systems.

OS – Operating system.

P2PE – Point-to-Point Encryption – A standard of encryption for the secure transmission of data from the POI to processing.

PCI DSS – Just testing!


PFI – PCI Forensic Investigator – The person who investigates system breaches to analyse when, how, and why they occurred.

POI – Point of Interaction – The point at which cardholder data is taken.

QSA – Qualified Security Assessor – A PCI SSC-qualified PCI DSS assessor.


SAQ – Self-Assessment Questionnaire – the self-assessment section of a PCI DSS assessment.

Service Provider – A third-party organisation that provides cardholder data processing, storage, or transmission services.

Tokenisation – The use of tokens to represent sensitive data so that data is never accessible by the merchant.

Please let us know if there are any other PCI terms you regularly come across, but don’t understand. We’ll give you a full explanation and will add them to our PCI glossary!
Thank you

We hope you found this eBook useful. If you have any further questions about PCI compliance or would like to find out how PCI Pal can help secure your contact centre without compromising your customer service experience, please visit our website or get in touch with our expert consultants today.

GET IN TOUCH

U.K. +44 207 030 3770
U.S. +1 866 645 2903
info@pcipal.com
www.pcipal.com
Secure contact centre technology from contact centre people.