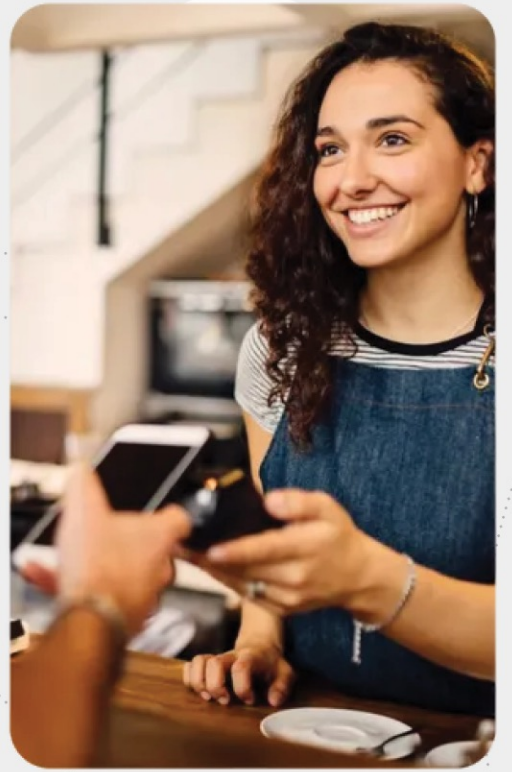
ClearAccept

What is PCI?

How does it apply to my business?



clearaccept.com

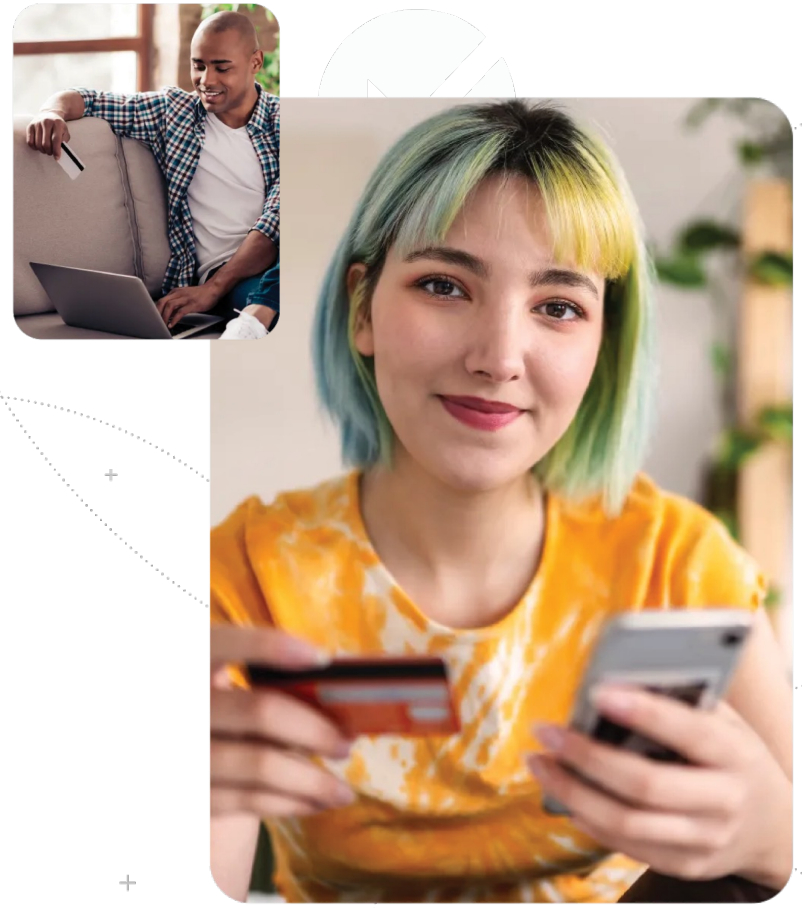
Contents

1. About PCI and its standards
2. What am I required to do as a merchant?
3. Self-Assessment Questionnaires in PCI DSS
4. What requirements are there?
5. Where can I find more information?

ClearAccept

About PCI and its standards

PCI stands for Payment Card Industry which itself is just short for Payment Card Industry Security Standards Council (PCI SSC). This organisation manages a number of standards covering the payment industry.



1) PCI SSC is owned by some of the major payment brands and was created to establish and manage security standards covering a wide range of activities related to the processing of card payments.
2) The most important standards for your business are:

Data Security Standard (PCI DSS): Often the term PCI is used to refer to this standard. It covers the environments and systems of entities that store, process or transmit card data – which includes all merchants.

Pin Transaction Security (PCI PTS): Standard that covers hardware used to take face-to-face card payments. Merchants can only use payment terminals that are certified under PTS.

Point to Point Encryption (P2PE): Covers solutions used by face-to-face merchants which can considerably reduce the users PCI compliance requirements.

Approved Scanning Vendor (ASV): Entities that provide vulnerability scanning services.

What am I required to do as a merchant?

The standard that everyone has to comply with is DSS (PCI DSS, “Payment Card Industry Data Security Standard”)

1. You are required to be compliant 24/7/365.
2. You are required to validate your compliance annually.
3. You must validate your compliance even if you have outsourced all your activity to a third party.
4. If you outsource any part of your activity that is in scope for the assessment, then your assessment either:
    - Extends to cover the activity the third party perform *or*
    - The third party has their own assessment done and provides you with proof it covered everything they do for you.

- PCI DSS has several hundred requirements as it covers every possible activity that is in scope for assessment.
- For those requirements that apply to your business you need a 100% pass mark.
- The same standard applies to everyone, the individual requirements can be marked “Not applicable” if there are grounds to do so, but these must be justified.
- Failure to demonstrate compliance can result in financial penalties being levied by the card brands, which will be passed on to you.
- Larger entities (processing over 1 million transactions per year) may be required to have their annual assessment performed by a certified assessor (Internal Security Assessor (“ISA”) or an external one (“QSA”).
- Smaller entities may be able to self assess without needing an ISA or QSA.
- The annual assessment is a validation of compliance requirements that you must fulfil 365 days/year.

ClearAccept

Self-Assessment Questionnaires in PCI DSS

The PCI Council (PCI SSC) recognises that there are a number of use cases where only a limited sub-set of the requirements apply.

- The same sub-set of requirements applies to all entities that only take payments through a certified terminal connected to the internet in a face-to-face transaction.
- A different sub-set of the requirements applies to entities that have a website but have outsourced all their payment functions to a PCI certified third party.

There are a set of Self-Assessment Questionnaires ("SAQ's") provided by the PCI SSC that include only those requirements that would apply to a number of given situations.

Additional information about the different types of SAQ's in the PCI SSC guidelines (page 4-5)

How to handle SAQ's?

- Simply identify which SAQ description exactly matches your card processing or handling activity.
- Open the document.
- Answer the questions.
- To pass the assessment you must respond to all the requirements (either it is "In Place" or you have a legitimate reason to say it is not applicable).
- Complete the attestation document and provide it to your acquirer.

Important for you acquirer:

1. Continue to meet the requirements every day for the next 12 months.
2. Renew your assessment and go to step 1 again.

ClearAccept

What requirements are there?

The standard is structured in 12 sections, each covering a specific aspect of the requirements.

- The twelve sections of the standard below always stay the same, but each SAQ has its predetermined number of requirements.
- The individual requirements are the same no matter what reporting template is used, the Report on Compliance (“ROC”) used by larger merchants (processing over 6 million transactions per year) includes all of them, SAQ D contains most of them, SAQ P2PE contains very few.

CORE PRINCIPALS	SECTIONS OF THE STANDARD
Build and maintain a secure network and systems	1. Install and maintain network security controls. 2. Apply secure configuration to all system components.
Protect account data	3. Protect stored account data. 4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a vulnerability management program	5. Protect all systems and networks from malicious software. 6. Develop and maintain secure systems and software.
Implement strong access control measures	7. Restrict access to system components and cardholder data by business Need to Know. 8. Identify users and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data. 11. Test security of systems and networks regularly.
Maintain an information security policy	12. Support information security with organisational policies and programs.

ClearAccept

What requirements are there? (cont.)

1. SAQs simply require that the merchant indicates whether the requirement is in place or not.
2. The merchant “attests” that they are compliant through an AOC (“Attestation of Compliance”).
3. If you use a service provider to perform some of the functions in scope for the assessment, then you should obtain a copy of their AOC to prove they are compliant as you cannot claim to be compliant if they are not.
4. An AOC is valid for one year. You should complete (not start) your renewal assessment by the date the last one expires.
5. Some assessments require a vulnerability scans done by an ASV vendor that should be contracted by your company.
    - Passing scans must be obtained at least quarterly.
    - The final stage of an ASV scan is you “attesting” it – if you do not do this you have not completed the scan.

PCI is primarily intended to protect card data. You are strongly advised to implement similar security controls to protect your other business assets and systems.

ClearAccept

Where can I find more information?

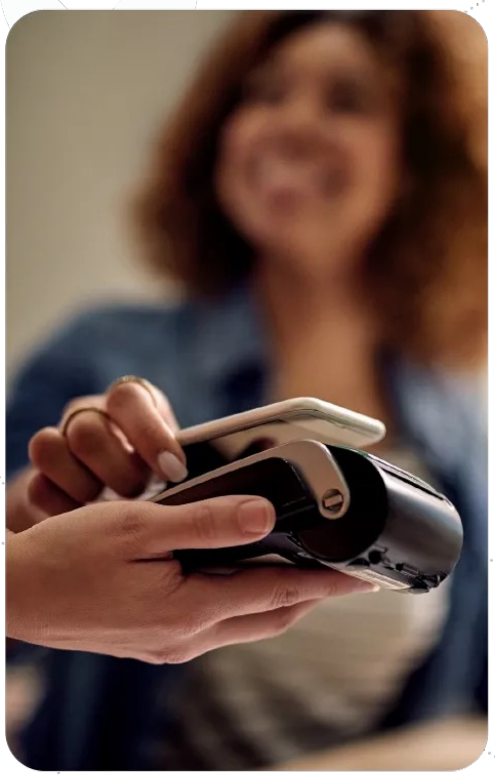
All the standards are maintained by the PCI Security Standards Council.

Official PCI Security Standards Council Site

What you can find in the council website

- Downloadable copies of the guidance on SAQ types
- Actual SAQ's
- Frequently Asked Questions
- Guidance for Merchants
- Listings of vendors/products that have been certified under various PCI Standards: PTS, ASV, P2PE
- And more…

At ClearAccept we **ensure and support our merchants to be PCI DSS compliant** with the card schemes requirements and regulations.



Thank you

clearaccept.com