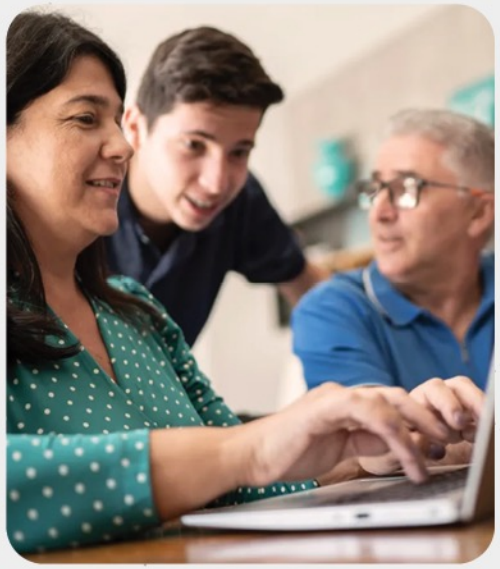
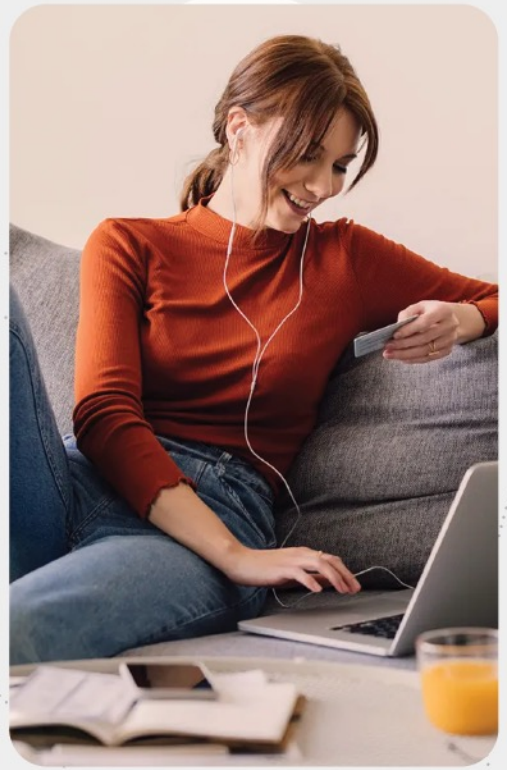
ClearAccept

PCI Basics for E-Commerce Merchants



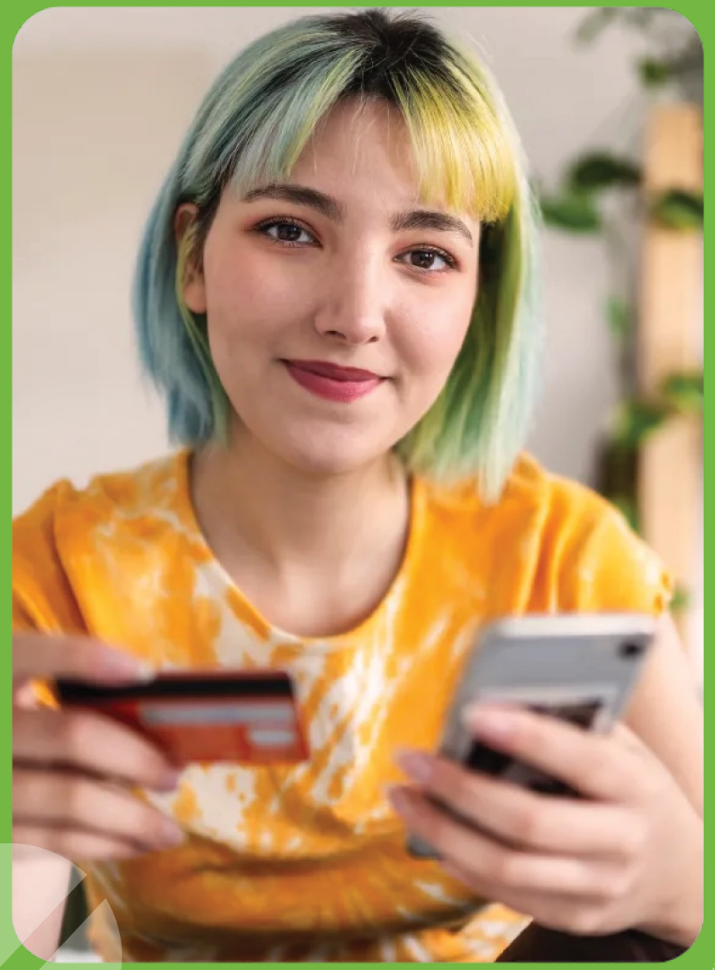


clearaccept.com

This presentation is applicable for merchants who accept online payments

We suggest reading the presentation
What is PCI? How does it apply to my business?
before proceeding with the details of this presentation.

Contents



ClearAccept

What does e-commerce mean?

Roughly speaking it is when you receive the card data electronically.

- Customer interacts with your web shop.
- Customer uses a mobile application that sends data to systems controlled by you.

If you have outsourced your e-commerce platforms, you are still responsible for being PCI compliant.

- The third party you engage may already be PCI compliant themselves.
- If they are not, then everything they do is included in your assessment.

If you have a website, then there are many ways this can be managed.

- You control the hardware and website.
- You use a service provider to create and manage your website for you.
- You have a web shop on one of the many “marketplaces”.

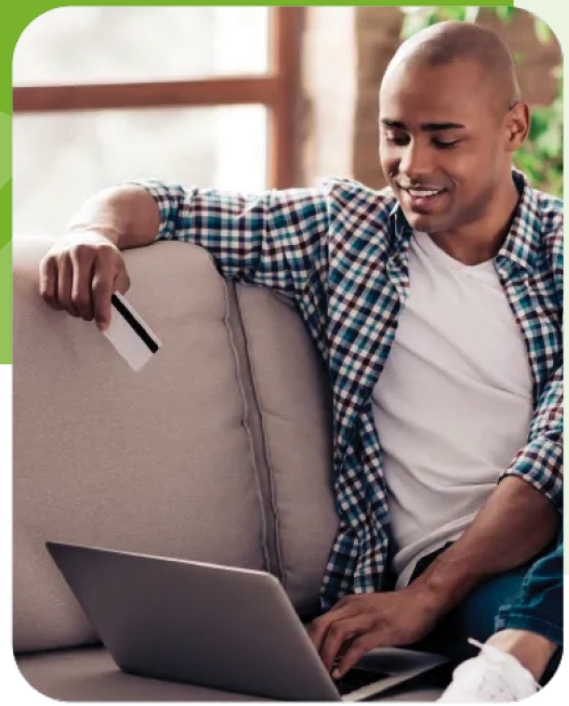
Payments can be processed in several ways.

- Your website processes the transaction and then sends the details on to the acquirer.
- Your website doesn’t store the data but accepts it and then sends it on to be processed by the acquirer.
- Your website doesn’t accept the card data itself, when the customer makes a payment, your site redirects the input to the acquirer for processing. Your site has no interaction with card data in any way.

ClearAccept

What do I have to do as a merchant?

If you are not compliant with PCI, **you may be liable to penalties imposed by the card brands,** and we **may no longer be able to process payments** on your behalf as you have not validated your security regarding payments.



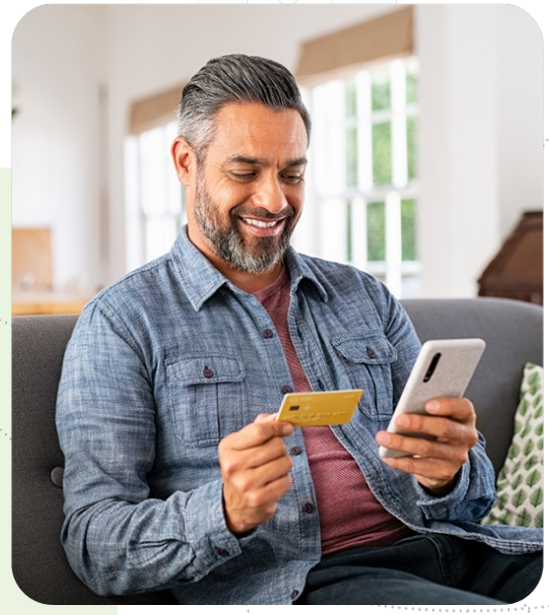
- PCI DSS has several hundred requirements as it covers every possible activity that is in scope for assessment.
- For those requirements that apply to your business you need a 100% pass mark.
- The same standard applies to everyone, the individual requirements can be marked “Not applicable” if there are grounds to do so, but these must be justified.
- The annual assessment is a validation of compliance. However, you need to be compliant all the time.
- Larger entities (processing over 1 million transactions per year) may be required to have their annual assessment performed by an ISA or a QSA.
- Smaller entities may be able to self assess without needing an ISA or QSA.

ClearAccept

Which core principals of the standards apply to me?

For smaller merchants, the PCI Council have created a set of Self-Assessment Questionnaires (SAQs) which are targeted at specific business models.

There are two alternatives for **merchants with e-commerce systems**:



1)SAQ A: Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.

2) SAQ A-EP: E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.

If neither of these describe the exact situation, then the merchant must use SAQ D.

ClearAccept

More about the individual SAQs for e-commerce merchants.

SAQ A.
If you meet the criteria to complete an SAQ A, then the below applies to your business:

CRITERIA FOR SAQ A:

- Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
- When the payment stage is reached in a transaction your website does not perform any of the functions – it either redirects the card holder to your payment processor or a payment processor iFrame is displayed and all transaction data is restricted to this frame.

EXAMPLES OF REQUIREMENT FOR SAQ A:

- No electronic storage of card data.
- Systems are secured and kept up to date.
- Scripts loaded and executed in the card holder's browser during the payment process are managed, controlled and authorized.
- External vulnerability scans ("ASV") conducted at least quarterly.
- Critical system files on the merchant systems are monitored and alerts are raised and responded to if any change is detected.

ClearAccept

More about the individual SAQs for e-commerce merchants

SAQ A-EP.
If you meet the criteria to complete an SAQ A-EP, then the below applies to your business:

CRITERIA FOR SAQ A-EP:

- E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
- Merchant web site controls the payment page, but the web site does not perform any processing, all data is sent to the payment processor (direct POST for example).

EXAMPLES OF REQUIREMENT FOR SAQ A-EP:

- No electronic storage of card data.
- Systems are secured and kept up to date.
- Anti virus is implemented where appropriate.
- Software is developed and patched securely.
- Scripts loaded and executed in the card holder's browser during the payment process are managed, controlled and authorized.
- From 2024: A technical method of detecting and preventing web-based attacks is implemented.
- Access to systems is restricted and secured.
- User activity and system events are logged and retained.
- External vulnerability scans ("ASV") conducted at least quarterly.
- Penetration testing is performed at least annually.
- Intrusion Detection/Prevention systems are implemented to alert and/ or prevent unauthorized access.
- Critical system files on the merchant systems are monitored and alerts are raised and responded to if any change is detected – File Integrity Monitoring ("FIM").

ClearAccept

More about the individual SAQs for e-commerce merchants

SAQ D.

If you don't meet the criteria to all other SAQs then SAQ D and the below applies to your business:

CRITERIA FOR SAQ D:

- Merchants that don't store account data electronically but that do not meet the criteria of another SAQ type.
- Merchants with a site that receives inbound transactions via electronic channels, processes them and then forwards the data to a payment processor.
- Merchants with multiple payment acceptance channels.
- Merchants with electronic storage of account data.
- No other SAQs eligible.

REQUIREMENT FOR SAQ D:

- SAQ D includes the majority of the requirements and may require the assistance of an Internal or External resource to adequately assess.

ClearAccept

What requirements are there?

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

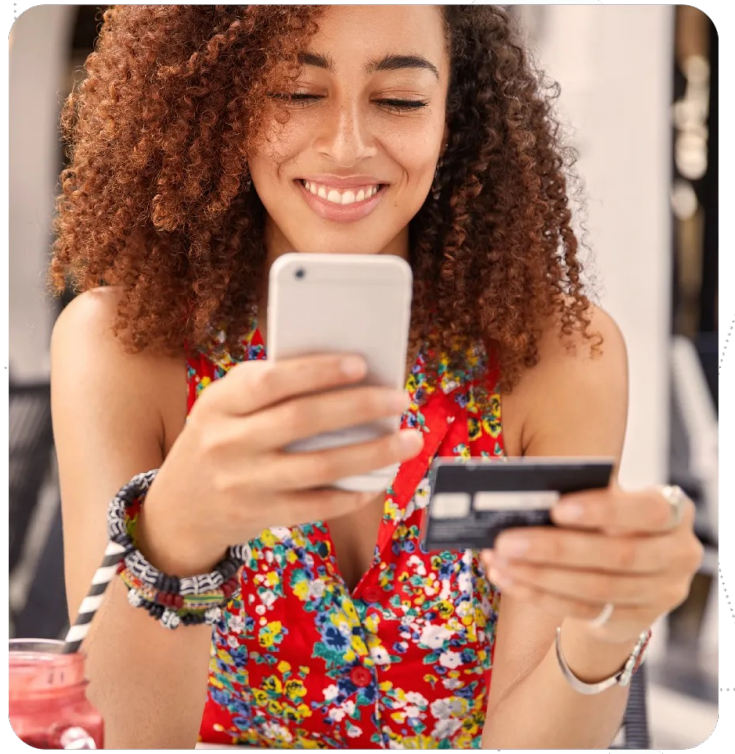
- The twelve sections of the standard below always stay the same, but each SAQ has its predetermined number of requirements.
- The individual requirements are the same no matter what reporting template is used, the Report on Compliance (“ROC”) used by larger merchants (processing over 6 million transactions 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 organizational 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

ASV scanning, Penetration Testing, Intrusion Detection/ Prevention and File Integrity Monitoring

One or more of these may be required for the assessment depending on the reporting template used. These are all fundamentally different activities as explained below.

- **ASV:** As part of the PCI DSS requirements, any entity having internet (public facing) IP addresses must undergo a security scan at least quarterly and the scan must be performed by an approved ASV Scanning Vendor. To pass the scan there cannot be any security issues (vulnerabilities) identified by the scan that have not been addressed.

  Note: This is NOT an in-depth penetration test – it simply looks for known software and configuration issues as a base line security check.

- **Penetration Testing:** An experienced tester will perform scanning to identify any potential weaknesses in the systems just like an ASV scan but will then go further and attempt to exploit those vulnerabilities. This is one step further than ASV scanning, but ASV scanning is still required.

  Note: ASV scanning must be performed by an approved vendor listed on the PCI Council web site. Penetration testers are not listed by the PCI Council, but they must be skilled and experienced in the activities.

- **Intrusion Detection/Prevention Systems ("IDS/IPS"):** These are systems within your environment that monitor network traffic in a similar manner to the way Anti-Virus software monitors programs and data. The systems are able to identify known "bad" traffic and either alert or block depending on the implementation. These systems are "always on", and need to be continually updated to ensure they have the latest threat data to be able to identify bad activity.

- **File Integrity Monitoring ("FIM"):** Monitors files on your system and raises an alert if they have changed from the known "good" version. This identifies any malicious changes to the critical files on your systems.

ClearAccept

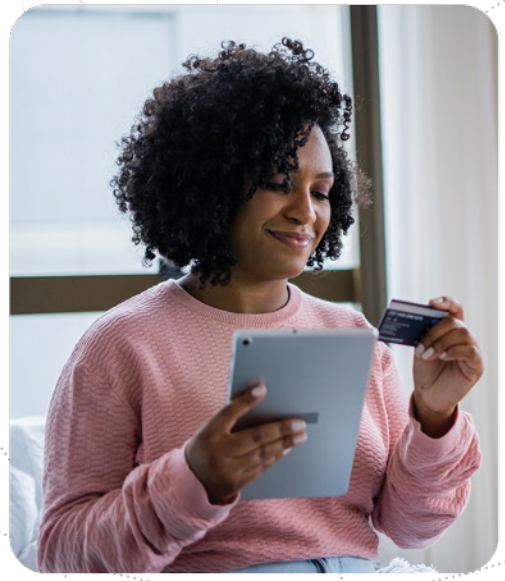
Where can I find more information?

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