Cashflows

PCI DSS Guide for Merchants

Version 1.0 December 2023

Table of contents

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of mandatory requirements designed to safeguard cardholder data. PCI DSS compliance is mandatory for any business that processes credit and debit card transactions and vital for companies that want to keep their customers' data secure.

Each transaction your business processes will involve sensitive cardholder information. This data must be processed, stored, and transmitted securely to protect your customers and your business from the increasing threat of fraud**.** Cashflows works in partnership with VikingCloud (formally Sysnet) who provides Cashflows and its merchants with an online portal to streamline the process to make managing and maintaining your PCI DSS compliance easier.

How to become PCI DSS Compliant

Businesses need to validate their compliance on an annual basis and are expected to always maintain compliance.

For small or medium-sized businesses you must either complete a PCI DSS Self-assessment Questionnaire (SAQ) or have a Formal Onsite Assessment by a Qualified Security Assessor (QSA) to demonstrate compliance.

For larger or more complex businesses, the PCI Security Standards Council website provides a list of approved QSAs who can work with you to ensure that your business is PCI DSS compliant.

If you are a small or medium-sized business, we require you to report your PCI DSS compliance using the Cashflows PCI Portal. There are two options:

1. **Self-assessment**: Complete your own Self-Assessment Questionnaire (SAQ) available for download from the PCI Council website then upload your compliant SAQ or third-party certificate from a QSA onto our PCI DSS online portal. Cashflows does not charge a fee for this.

Instructions on how to access the portal will be provided once your Cashflows account has been opened.

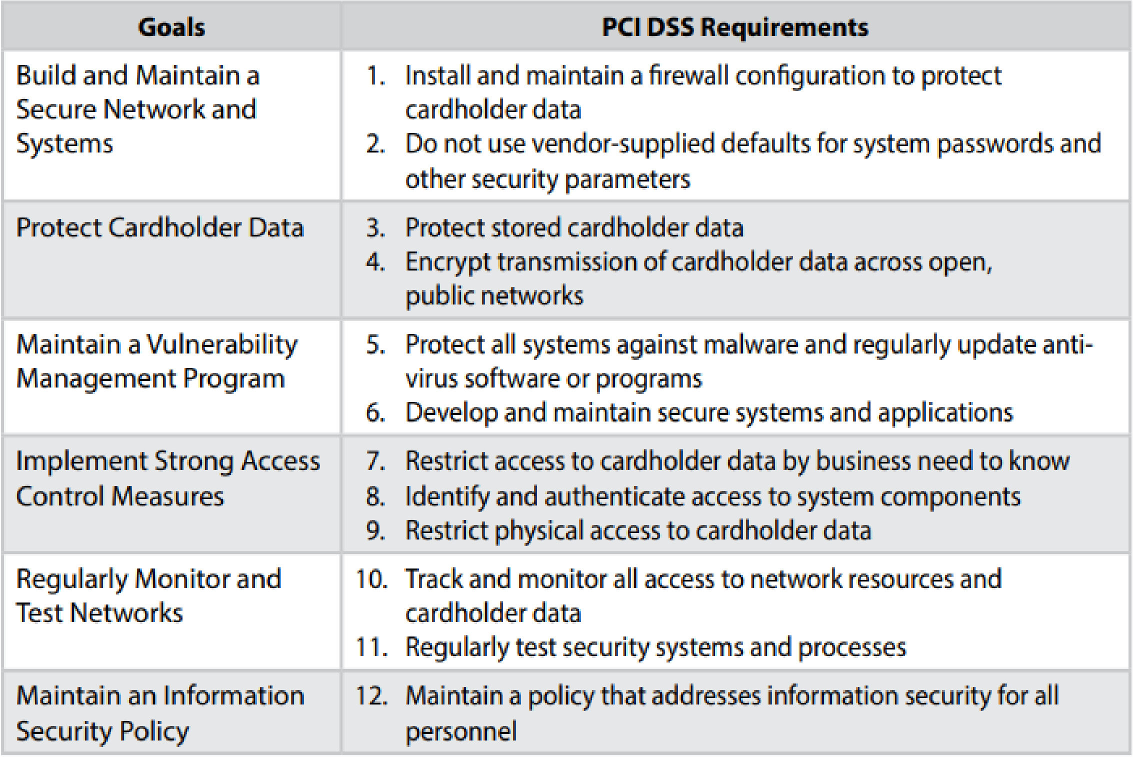
2. **Assisted online reporting service**: Manage, report, and maintain your compliance using our online service at https://complywithpci.com/ It provides assistance and information to help you to understand which requirements are appropriate to your business and guides you through your Self-Assessment Questionnaire (SAQ) step by step.

Benefits include:

- Access to the PCI Helpline and online chat.
- Task and revalidation reminders.
- Information Security Policy template.
- 'Security Measures for Your Business' checklist.
- Access to security information and advice.
- Inclusive Approved Scanning Vendor (ASV) vulnerability scans.

What are the requirements of PCI DSS:

PCI DSS compliance is based on 12 requirements. The specific requirements that apply to your business depend on how you process credit cards.



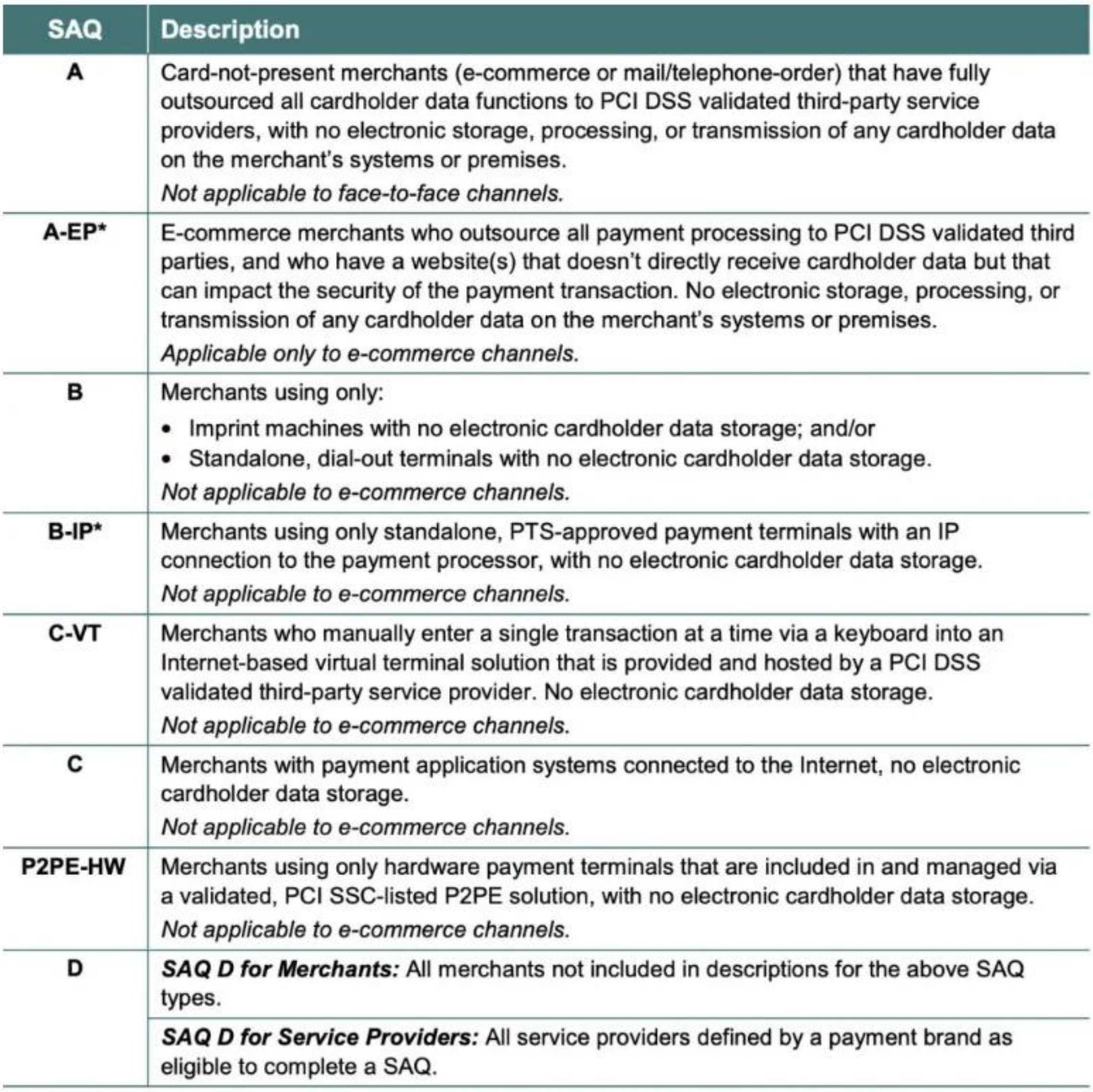
Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Which SAQ type is applicable is by business:

The “SAQ” is a validation tool for merchants and service providers to report the results of their PCI DSS self-assessment. The SAQ includes a series of yes-or-no questions for each applicable PCI DSS requirement. If an answer is no, then Cashflows may require you to state the future remediation date and associated actions. There are different SAQs available to meet different merchant environments. If you are not sure which SAQ would apply to you, contact Cashflows or VikingCloud for assistance.

How you process credit cards and handle cardholder data determines which SAQ your business needs to fill out. For example, if you don’t have a face-to-face shop and all your products are sold online through a third party, you probably qualify for SAQ A or SAQ A-EP. If you do have a face-to-face shop that processes credit cards through the Internet and you also store customer credit card data, you’re probably an SAQ D merchant.

There are 8 different SAQ types, each for different types of organisations that handle PCI information. The 8 different types can be found below:



SAQ	Description
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. *Not applicable to face-to-face channels.*
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. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Choosing the right PCI DSS SAQ is very important in self-assessment. Often businesses will find that they do not meet all the eligibility criteria for the SAQ they want to complete and that they are imposed on all PCI DSS requirements.

Before choosing the appropriate SAQ for your business, creating a network card data flow diagram, and system inventory for PCI DSS compliance will make the SAQ selection process much more manageable.

For more information, visit the PCI Security Standards website.

Cashflows

+44 (0)1223 550920
support@cashflows.com
cashflows.com