WHICH SELF-ASSESSMENT QUESTIONNAIRE (SAQ) IS RIGHT FOR YOU?

BACKGROUND

Every organisation that accepts, transmits and stores payments must complete one or more Self-Assessment Questionnaires (SAQ) to evidence PCI compliance.

A range of SAQs has been developed to suit a variety of business types, since organisations come in all shapes and sizes.

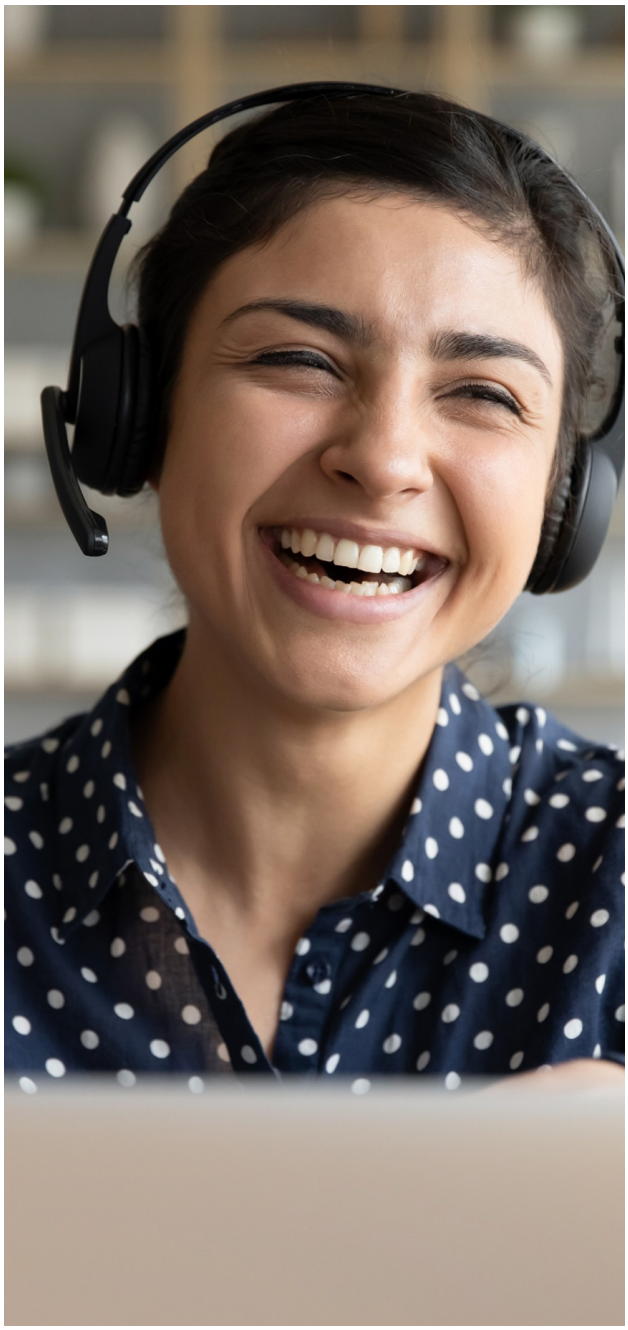
The very first step towards correct completion is to identify which SAQs are applicable to your organisation.

Use our chart to see which SAQs are correct for you.

SAQ TYPE	WHO IT'S FOR	ACTIONS REQUIRED
SAQ A	Cardholder-Not-Present (CNP) merchants 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.	• Paper copies of cardholder data must be destroyed or protected • Details of Third-party service providers must be kept • Compliance of third-party services must be monitored • Completion of SAQ A (22 questions)
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.	• Any e-commerce merchant formerly using SAQ A should read guidelines to identify whether they should now complete the new SAQ A-EP form instead • Completion of SAQ A-EP (193 questions)
SAQ B	Merchants using only imprint machines with no electronic cardholder data storage; and/or standalone, dial-out terminals with no electronic cardholder data storage.	• Ensure terminals (which can now connect via BlueTooth, Ethernet and GSM/LTE) are isolated from networks an therefore not putting cardholder data at risk • Completion of SAQ B (41 questions)
SAQ B-IP	Merchants without electronic cardholder data storage who process payments via standalone PTS-approved point-of-interaction (POI) devices which have IP connections to payment processors. This type of transaction can take place in person or via MOTO.	• Ensure POI devices are isolated from other networks • Paper merchant receipts must be the only type of cardholder data retained. • Completion of SAQ B-IP form (84 questions)
SAQ C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.	• Ensure the technology used to enter cardholder details is isolated from other networks and is strongly protected • Completion of SAQ C (162 Questions)
SAQ 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.	• Ensure the technology used to enter cardholder details is isolated from other networks and is strongly protected • Completion of SAQ C (162 Questions)

Continued on back.

SAQ TYPE	WHO IT'S FOR	ACTIONS REQUIRED
SAQ 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.	• All data must be entered via a validated P2PE hardware device. No vulnerability scan or penetration testing required • Completion of SAQ P2PE-HW (33 questions)
SAQ D (For merchants)	All merchants not included in descriptions for the above SAQ types.	• Vulnerability scans and penetration testing required • Completion of SAQ D which includes all 329 PCI DSS requirements, marking non-applicable sections with caution
SAQ D (For service providers)	All service providers defined by a payment brand as being SAQ-eligible, processing fewer than 300,000 transactions per year.	• Vulnerability scans and penetration testing required • Completion of SAQ D which includes all 329 PCI DSS requirements, marking non applicable sections with caution. • Additional 'Service Provider Only' requirements are identified within the PCI DSS



NEXT STEPS

Now that you know which SAQ is right for your organisation, enhance your PCI compliance strategy to ensure you score well. Our team at PCI Pal is ready to help. Our pioneering Level 1 PCI DSS certified solutions are built around your contact centre and processes, so your customer service operation will remain exactly as you want it to be. Customisable, scalable and reliable, with 24/7 global support. Contact us to get started.

OUR ACCREDITATIONS

pci WINNER Awards for Excellence 2020

Card & Payments Awards 2021 CATEGORY FINALIST Best Technology Initiative

DATA SECURITY SOLUTION PROVIDER OF THE YEAR

London Stock Exchange

UKAS ISO 27001

QMS ISO 27001 ISO 22301 REGISTERED

QMS ISO 9001 ISO 14001 REGISTERED

PCI Security Standards Council PARTICIPATING ORGANIZATION

GET IN TOUCH

+61 02 7202 0294

info@pcipal.com