PCI DSS 4.0 Self■Assessment Questionnaire (SAQ) Comparison

SAQ Type	Typical Merchant Scenario	Scope	Effort	Key Controls
SAQ A	Fully outsourced processing; merchant systems do not store, process, or transmit cardholder data (CHD).	Minimal scope; only verification of outsourcing and website security if applicable.	Lowest effort (~24 questions).	Confirm provider PCI compliance, secure redirection (HTTPS), and ensure no CHD storage.
SAQ B	Standalone payment terminals or imprint machines; no electronic CHD storage.	Terminals are isolated with limited connectivity; no electronic CHD storage.	Low effort (~59 questions).	Secure terminals; ensure no CHD stored electronically; avoid IP connectivity.
SAQ C	Internet-connected payment application without CHD storage.	Internet-exposed systems; network and application in scope but no CHD storage.	Moderate effort (~84 questions).	Maintain firewalls, patch management, vulnerability scans, and segmentation.
SAQ D	Merchant stores, processes, or transmits CHD electronically or operates a complex environment.	Full PCI DSS scope; includes all systems, people, and processes handling CHD.	Highest effort (300+ questions).	Comply with all PCI DSS requirements: encryption, access control, monitoring, and testing.

Key Differences & Considerations

• Electronic storage of cardholder data (CHD) determines the SAQ type—storage requires SAQ D.
• Payment channel type matters (e■commerce vs. face■to■face vs. mail/telephone order).
• Connectivity (internet/IP) drives more controls; isolated systems may qualify for SAQ B.
• Complexity of environment correlates with the number of required controls.
• PCI 4.0 emphasizes continuous monitoring, script integrity, and customized testing.
• Acquiring banks confirm SAQ eligibility; self■assessment must be validated.

Operational Implications

Operations teams should align payment architecture to minimize PCI scope. Outsourcing (SAQ A) and isolating payment systems (SAQ B/C) reduce compliance costs. SAQ D environments require dedicated resources, monitoring, and ongoing policy enforcement under PCI DSS 4.0.

Quick Decision Flow

1. Do you store cardholder data electronically? → Yes: SAQ D.
2. Are payment terminals internet■connected? → Yes: SAQ C.
3. Fully outsourced to PCI■compliant provider (no CHD handled)? → Yes: SAQ A.
4. Confirm SAQ with your acquiring bank or payment brand.