SECURISEA · READINESS CHECKLIST

PCI DSS Self-Assessment Questionnaire Checklist

A requirement-by-requirement readiness review for SAQ-eligible merchants and service providers, aligned to PCI DSS v4.0.1.

How to Use This Checklist

Work through each section in order. For every item, mark the checkbox if you can answer yes with evidence to back it up. If you cannot, leave it blank and treat it as an open gap.

Each section has its own running total. When you finish, add the section totals together and compare your final score to the readiness tier table at the end.

This checklist is universal across all nine PCI DSS v4.0.1 SAQs. Some items apply only to specific SAQ types. Where that is the case, the item names the SAQ or the requirement it applies to. If an item does not apply to your environment, do not check it, but note in the margin why it does not apply (so the entry holds up to acquirer scrutiny later).

Section 1: Confirm Your SAQ Type

Picking the wrong SAQ is one of the most common reasons submissions get rejected or revisited after a breach. The right SAQ is determined by your payment acceptance channel, your integration model, and whether you store account data, not by your size.

Section 1 items	Score: ____ / 10

☐	I have confirmed with my acquirer or payment brand that I am eligible to validate via an SAQ rather than a Report on Compliance (ROC).
☐	I have mapped every way my organization accepts payments: card-present, e-commerce, mail order/telephone order (MOTO), and any other channel.
☐	I have identified the integration model for each channel (fully outsourced redirect, iframe, hosted payment page, virtual terminal, integrated payment application, P2PE solution, or SPoC solution).
☐	I have confirmed whether any account data is stored electronically anywhere on my systems or premises (even briefly, even in logs).
☐	If I accept e-commerce, I have confirmed that all payment page elements delivered to the customer's browser originate directly from a PCI DSS-compliant third-party service provider (TPSP).

☐	If I accept e-commerce, I have confirmed that my site is not susceptible to script-based attacks (required for SAQ A eligibility as of 31 March 2025).
☐	If I use a P2PE or SPoC solution, I have verified the solution is on the official PCI SSC list of validated solutions (not just sold as P2PE-capable).
☐	I have compared my channel and integration profile against the eligibility criteria for each SAQ and selected the one that matches, rather than the shortest one.
☐	If I have more than one payment channel, I have confirmed whether a single SAQ covers them or whether SAQ D (the most comprehensive) is required.
☐	If I am a service provider, I have confirmed that SAQ D for Service Providers is the only SAQ available to me.

Section 2: Scope Your Cardholder Data Environment

Under-scoping is the single most common PCI DSS error. PCI DSS scope includes the systems, people, and processes that store, process, or transmit account data, plus any system that is connected to or could impact the security of the CDE.

Section 2 items	**Score: ____ / 7**

☐	I have identified every system component, person, and process that stores, processes, or transmits account data (cardholder data plus sensitive authentication data).
☐	I have identified every system component that is connected to the cardholder data environment (CDE), even if it does not itself touch account data.
☐	I have identified every system component that, if compromised, could impact the security of the CDE (for example, authentication servers, DNS, patch management, monitoring tools).
☐	I have documented the people in scope by role and the processes in scope by function, not just the servers.
☐	I have walked the scope with someone outside the payment team (security, IT operations, or a QSA) to challenge any assumption that something is out of scope.
☐	If I use network segmentation to reduce scope, I have segmentation controls in place and tested, and I can demonstrate they work.
☐	I have a list of every third-party service provider (TPSP) that stores, processes, or transmits account data on my behalf, or that could impact the security of my CDE.

Section 3: Account Data Flow and Documentation

If you cannot draw the flow, you cannot scope the environment. Diagrams and inventories are the foundation that every other answer rests on.

Section 3 items	Score: ____ / 6

☐	I have a current data-flow diagram that shows all account data flows across systems and networks, for every payment channel (PCI DSS Requirement 1.2.4).
☐	I have a current network diagram that shows all connections in and out of the CDE, including wireless networks (Requirement 1.2.3).
☐	Both diagrams reflect the environment as it is today, not as it was at last year's assessment.
☐	I have an inventory of all system components in scope, including hardware, software, virtual components, and cloud services (Requirement 12.5.1).
☐	I have written policies and procedures for every PCI DSS requirement that applies to my SAQ.
☐	I have evidence that the controls in my SAQ are operating, not just that they exist on paper.

Section 4: Supporting Documentation

The SAQ document contains the AOC as Sections 1 and 3. The questionnaire itself sits in Section 2. Most submissions that get returned are missing the supporting artifacts behind the answers, not the answers themselves.

Section 4 items	Score: ____ / 7

☐	I have completed Sections 1 and 3 of the SAQ document, which together form the Attestation of Compliance (AOC), and the AOC has been signed by an authorized officer.
☐	I have current ASV scan reports (passing) for every external-facing system in scope, if my SAQ requires quarterly external scans under Requirement 11.3.2.
☐	I have current internal vulnerability scan results, if my SAQ requires internal scans under Requirement 11.3.1.
☐	I have a current penetration test report, if my SAQ requires one (typically SAQ D).
☐	I have collected an AOC from every TPSP that handles account data on my behalf, confirming their PCI DSS compliance (Requirement 12.8).

☐	If I rely on any compensating controls, I have a completed Compensating Controls Worksheet (CCW) for each one, documenting the constraint, the objective, the identified risk, the control itself, validation, and maintenance.
☐	I have evidence of the targeted risk analyses required under Requirement 12.3.1 for any requirement where I am setting the frequency myself, reviewed within the last 12 months.

Section 5: Common Pitfalls to Verify Against

These are the patterns QSAs see year after year. Each item is phrased as the right behavior, so a checked box means you have avoided the pitfall.

Section 5 items	Score: ____ / 7

☐	I have not scoped my environment based only on systems that obviously touch account data; I have included connected-to and security-impacting systems.
☐	I have not selected an SAQ type based on my organization's size or transaction volume; I have selected based on how account data actually flows.
☐	I have not picked the shortest SAQ available; I have picked the one that matches my eligibility.
☐	I have not left any section of the SAQ marked 'In Place' without performing the testing the SAQ asks for.
☐	I have not marked any requirement 'Not Applicable' without documenting why it does not apply.
☐	I have not signed the AOC without completing the questionnaire and gathering the supporting documentation behind every answer.
☐	I have not treated last year's SAQ as still valid; I have reassessed whether the same SAQ type still applies after any change to my payment environment.

Section 6: Ongoing Compliance Activities

PCI DSS is a continuous program. Annual validation is the visible part, but the controls behind it have to operate year-round for the validation to hold up.

Section 6 items	Score: ____ / 6

☐	I treat PCI DSS as a continuous business-as-usual program, not a once-a-year project.

☐	I have a calendar of recurring activities (quarterly ASV scans, internal scans at the required frequency, annual penetration testing where required, annual policy reviews, annual targeted risk analyses).
☐	I review my SAQ eligibility every year, before I submit, in case my payment environment has changed.
☐	I have a process to reassess scope whenever a significant change happens to my environment (new application, new TPSP, new network segment, new payment channel).
☐	I know who at my organization owns the AOC sign-off, and they are aware of what they are attesting to.
☐	I know when my SAQ is due to my acquirer or payment brand, and I have built in enough time to remediate any gaps I find while completing it.

Your Readiness Score

Add up the checked items across all six sections. There are 43 total items.

Section 1: Confirm your SAQ type	_____ / 10
Section 2: Scope your cardholder data environment	_____ / 7
Section 3: Account data flow and documentation	_____ / 6
Section 4: Supporting documentation	_____ / 7
Section 5: Common pitfalls to verify against	_____ / 7
Section 6: Ongoing compliance activities	_____ / 6
Total	**_____ / 43**

Readiness tier

Score	Readiness tier	What it means
0 – 21	**Not Ready**	More than half of the items are open. Submitting an SAQ in this state is likely to be rejected by your acquirer or to surface gaps during the next breach review. Close foundational items (scope, data flows, SAQ selection) first.
22 – 35	**Approaching**	You have the core building blocks but real gaps remain. Most often these sit in supporting documentation, compensating controls, or ongoing activities. Closing them before submission is a much smaller lift than discovering them mid-assessment.
36 – 43	**Ready**	You are positioned to complete and submit your SAQ and AOC with confidence. Any remaining items are likely minor. This is a good point to bring in a QSA for a final review before sign-off.

Ready to Move Beyond the Checklist?

The checklist helps you prepare, but the SAQ itself is how SAQ-eligible entities validate and report their PCI DSS compliance. If your score landed in Approaching or Not Ready, the gaps are easier to close before you submit than after.

Securisea is a PCI SSC-qualified QSA Company and a member of the PCI SSC's Global Executive Assessor Roundtable (GEAR). Our QSAs work across all merchant levels and can support you from scoping and readiness through final validation.

Talk with us: securisea.com/contact-us