COMPLIANCE CHECKLIST

PCI DSS 4.0.1 compliance checklist

Payment Card Industry Data Security Standard 4.0.1

Jurisdiction: Global - any entity handling payment card data

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who PCI DSS 4.0.1 applies to

Merchants, payment service providers, and any entity that stores, processes, or transmits cardholder data - globally, contractually enforced by the card brands.

PCI DSS 4.0.1 checklist

- [ ] STEP 1
  Identify and isolate the cardholder data environment (CDE) to minimise scope.
- [ ] STEP 2
  Determine your merchant level (1-4) based on annual card-transaction volume.
- [ ] STEP 3
  Identify the applicable Self-Assessment Questionnaire (SAQ) type (A, A-EP, B, C, D, P2PE).
- [ ] STEP 4
  Implement and document the 12 PCI DSS requirements within scope.
- [ ] STEP 5
  Run quarterly external vulnerability scans by an Approved Scanning Vendor (ASV).
- [ ] STEP 6
  Run quarterly internal vulnerability scans.
- [ ] STEP 7
  Conduct annual penetration testing (network + application).
- [ ] STEP 8
  Maintain an inventory of all CDE system components, software, and personnel.
- [ ] STEP 9
  Document and review user access controls, change management, and incident response procedures.

STEP 10

- [ ] Complete and submit the Attestation of Compliance (AOC) to your acquirer or card brand.

FAQ

What is the difference between PCI DSS 3.2.1 and 4.0?

PCI DSS 4.0.1 is the current version. v4.0 (effective 31 March 2024) was retired on 31 December 2024 and replaced by v4.0.1 (published 11 June 2024) - a minor errata release. The 51 future-dated requirements introduced in v4.0 became mandatory on 31 March 2025. v4.0.1 introduces the customised-approach option, expanded multi-factor authentication, and more granular requirements for service providers. PCI DSS 3.2.1 was retired with the v4.0 transition.

Do I need a QSA?

Merchants Levels 2-4 generally self-assess via SAQ. Level 1 merchants and most service providers require an annual Report on Compliance (ROC) prepared by a Qualified Security Assessor (QSA). Card brands and acquirers can impose stricter requirements based on history.

How does scope reduction help?

Every system that stores, processes, or transmits cardholder data - or is connected to one that does - is in scope. Network segmentation, tokenisation, and P2PE all reduce the in-scope footprint, which directly reduces the cost and risk of compliance. SAQ-A (e-commerce with all card data handled by a PCI-validated third party) is dramatically simpler than SAQ-D.

How often do I need a penetration test?

External and internal penetration testing at least annually, and after any significant change to the CDE. Service providers have an additional obligation under PCI DSS Requirement 11.4.6: penetration testing on segmentation controls every 6 months (not general internal pen testing - specifically the controls that isolate the CDE from other networks).

Source: https://ba-copilot.com/compliance/pci-compliance-checklist. Tick each item as it is completed and add the named owner.