
CYBER360 / SPECIALIST SERVICES

PCI DSS Compliance

A clear route to sustainable payment security.

Understand your payment environment, close control gaps and prepare the evidence for PCI DSS validation. Cyber360 connects practical security improvements with a compliance programme your teams can sustain.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | UK & Middle East

01 / SCOPE & FOCUS

The right question. A useful assessment.

Understand your payment environment, close control gaps and prepare the evidence for PCI DSS validation. Cyber360 connects practical security improvements with a compliance programme your teams can sustain.

Payment ecosystem & validation strategy

Merchant or service-provider role, payment channels, transaction volumes and acquirer obligations.

A compliance strategy and agreed validation assumptions.

Data discovery & scope reduction

Cardholder data flows, system inventories, connected systems, third-party dependencies and network boundaries.

CDE documentation and a justified scope-reduction plan.

Gap assessment & remediation planning

Applicable PCI DSS requirements, technical evidence, documents and operational practices.

A requirements matrix and prioritised roadmap with owners and milestones.

Technical safeguards & testing

Agreed network, access, encryption, hardening, logging and vulnerability-management controls.

Implementation guidance and an agreed testing and validation plan.

Policy, people & operational processes

Security policies, access reviews, change and patch management, awareness, supplier oversight and incident response.

Tailored documentation, responsibility assignments and role-based awareness materials.

Evidence & continuous compliance

Evidence collection, SAQ completion support or ROC preparation, assessor liaison and compliance maintenance.

An assessment-readiness pack and ongoing compliance calendar.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Confirm the route

Agree objectives, stakeholders, payment channels and acquirer or payment-brand validation expectations.

Map the environment

Document payment flows, assets, suppliers and the boundaries of the cardholder data environment.

Assess the gaps

Review applicable requirements and available evidence; prioritise weaknesses by risk and dependency.

Implement improvements

Agree remediation work packages, strengthen controls and develop practical policies and procedures.

Prepare validation

Support SAQ completion or ROC readiness and coordinate with the appointed QSA or ASV where needed.

Maintain the programme

Establish review cycles, evidence ownership, training and monitoring of material changes.

WHAT YOU RECEIVE

For leadership & programme owners

- Diagnostic assessment and compliance strategy.
- Prioritised remediation roadmap with responsibilities and milestones.
- Scope-reduction recommendations and key delivery dependencies.
- Continuous compliance calendar and governance framework.

For technical & assessment teams

- Payment data-flow diagrams, asset inventory and CDE documentation.
- Requirements matrix, tailored policies and implementation guidance.
- Evidence repository structure and testing records for agreed controls.
- SAQ support or ROC preparation materials and assessor liaison.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Payment environment

- List payment channels, business entities and processors.
- Share existing diagrams, inventories and previous assessment results.

Validation expectations

- Provide acquirer or payment-brand instructions and deadlines.
- Confirm merchant or service-provider role and any appointed assessor.

Evidence & owners

- Nominate payment, IT, security, business and supplier contacts.
- Agree secure access to relevant documentation and configuration evidence.

Delivery boundaries

- Confirm implementation, testing and third-party work to be included.
- Agree change windows, responsibilities, dependencies and acceptance criteria.

PRACTICAL QUESTIONS

Who needs to consider PCI DSS?

PCI DSS applies to entities that store, process or transmit payment account data, and entities that can affect the security of the cardholder data environment. Your payment arrangements and role determine the scope and validation obligations.

Do we need an SAQ or a ROC?

This depends on payment-brand and acquirer requirements, your role and your environment. SAQs have specific eligibility criteria. We help clarify the appropriate route with the entity accepting your compliance submission.

Consulting and readiness support; formal QSA assessment and ASV scanning are scoped separately. Validation acceptance rests with the relevant acquirer or payment brand.

Reference: PCI SSC - PCI DSS and SAQ guidance (October 2026).

LET'S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

UK +44 20 3286 1927 | UAE +971 55 768 7199