PENTESTERRA

PCI DSS V4.0.1 GAP ASSESSMENT

Would Your Payment Data Pass a SAQ Today?

Gap assessment across 63 PCI DSS v4.0.1 sub-requirements - the level of detail of a SAQ-D-style self-assessment - for anyone handling payment card data.

IN SHORT

Covers the 12 PCI DSS requirements expanded to their numbered sub-requirements (~63) - the level a merchant or service provider answers at in a SAQ-D-style self-assessment. Requirements 1, 2, 4, 6 and 11 have a strong externally-observable component.

63
PCI DSS v4.0.1 sub-requirements covered

12
Core requirements expanded to SAQ-D level

Global
Anyone who stores, processes or transmits card data

THE SITUATION TODAY

WHO YOU ARE
You're the security or IT lead of a merchant or service provider that handles payment card data and needs to prepare the self-assessment or the QSA audit.

WHAT HAPPENED
The annual PCI DSS deadline is approaching, and the last self-assessment was filled in out of habit rather than real verification.

WHY IT HURTS
A card-data breach with non-compliant PCI DSS controls brings direct fines from the payment networks, on top of losing the ability to process payments at all.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's PCI DSS v4.0.1 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of PCI DSS v4.0.1, grouped the way you'll see them in the platform.

Requirements 1-3: Network and cardholder data protection

The most directly verifiable technical perimeter.

- Network security controls
- Secure configurations for systems and networks
- Protection of stored cardholder data

Requirements 4-6: Cryptography and secure development

How data travels and how the software handling it is written.

- Strong cryptography during transmission
- Protection from malicious software
- Secure development and maintenance of software

Requirements 7-9: Access control

Who can access what, physically and logically.

- Access restricted by business need to know
- User identification and authentication
- Restricted physical access

Requirements 10-12: Logging, testing and governance

The continuous evidence a QSA will verify.

- Logging and monitoring of all access
- Regular security testing of systems and networks
- Information security policies and programme

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for PCI DSS v4.0.1

A complete report, ready to present to clients, auditors, or your board.

Request your PCI DSS v4.0.1 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance