Cyber **security**

PCI DSS MADE SIMPLE: FROM COMPLIANCE TO CONFIDENCE

THREAT **READY**

LRQA.COM

LRQA

Your Risk Management Advantage

Previous Next

PCI DSS OVERVIEW

What is PCI DSS?

A global standard for securing credit card data and reducing fraud.

Who needs it?

Any organisation storing, processing or transmitting cardholder data : retailers, service providers, call centres and beyond.

Why it matters

- Protects customers and brand reputation
- Reduces fraud risk
- Demonstrates commitment to security

THE PCI DSS JOURNEY – WHERE ARE YOU?

Understand your position, next steps, and how LRQA can help at every stage.

STAGE 1
UNAWARE OR UNCERTAIN

"Do we even need PCI DSS?"

AUDIENCE

Start-ups, e-commerce companies, new merchants or service providers

PAIN POINTS

Confusion, lack of clarity, risk of fines or scope creep

ACTION

Use a simple self-checklist to determine if PCI applies

STAGE 2
INITIAL ASSESSMENT & DISCOVERY

"We know we need it, but we're not sure where to start."

ACTIVITIES

Gap analysis, define scope, cardholder data flow mapping

WHAT LRQA DOES

Tailored discovery sessions, PCI awareness training, Gap Analysis, scoping

RISK IF SKIPPED

Wasted effort, over-scoping, incomplete compliance

THE PCI DSS JOURNEY – WHERE ARE YOU?

STAGE 3
PREPARATION & PLANNING

"We want to get compliant but need help building the right processes."

ACTIVITIES

Remediation plans, technical advice, policy development, supplier due diligence

WHAT LRQA DOES

Workshops, architectural consulting, risk assessments, team security training and awareness

RISK IF SKIPPED

Non-compliance, wasted investment, audit delays

STAGE 4
ASSESSMENT AND VALIDATION

"We're ready for the audit-what does success look like?"

ACTIVITIES

QSA-led assessment, SAQ review, documentation and evidence collection

WHAT LRQA DOES

On-site assessments*, pre-flight checks,SAQ Assistance, RoC and AoC production

RISK IF RUSHED

Incomplete evidence, failed requirements, brand damage.

*If LRQA conducts a PCI Assessment, we may only provide a Gap Analysis or Pre-assessment. Other services would create a conflict of interest. **Contact us to find out more.**

THE PCI DSS JOURNEY – WHERE ARE YOU?

STAGE 6 BUSINESS-AS-USUAL MAINTENANCE

"We passed - now how do we stay compliant all year?"

ACTIVITIES

Recurring tasks (scans, reviews), continuous compliance, version updates (e.g. PCI DSS v4.0.1)

WHAT LRQA DOES

Scheduled support, reviews, guidance on evolving PCI requirements and maintaining compliance, guidance on managing third-party service providers

RISK IF IGNORED

Annual audit failure, hidden non-compliance, reactive fixes

STAGE 7 UNSURE WHERE YOU FIT?

Not sure where you are on the journey?

That's okay. Many vendors fall between stages or have partial coverage. We can help you clarify your position and next steps.

Find out more →

PCI DSS REQUIREMENTS

The PCI DSS covers 12 broad requirements comprising the following:

1. Install and maintain network security controls

2. Apply secure configurations to all system components

3. Protect stored account data

4. Protect cardholder data with dtrong cryptography during transmission over open, public networks

5. Protect all systems and networks from malicious software

6. Develop and maintain secure systems and software

7. Restrict access to system components and cardholder data by business need to know

8. Identify users and authenticate access to system components

9. Restrict physical access to cardholder data

10. Log and monitor all access to system components and cardholder data

11. Test security of systems and networks regularly

12. Support information security with organizational policies and programs

Merchants can potentially reduce their compliance scope and align to specific self-assessment questionnaires (SAQs) if they meet all eligibility criteria of that SAQ, depending on the payment channels they use.

Specific SAQs automatically exclude PCI DSS requirements that are not relevant to the scope of that SAQ, which can simplify achieving and maintaining compliance for the merchant.

TOP TIPS FOR SMOOTH COMPLIANCE

Start early

Don't leave PCI DSS to audit time.

Reduce scope

Limit where cardholder data is stored or transmitted.

Document everything

Policies, procedures, evidence.

Engage the right partner

QSA expertise avoids rework.

Make it BAU

Treat security as an ongoing process, not a project.

WHY LRQA?

Expertise

Our qualified security assessors and experienced testers combine compliance expertise with hands-on technical insight, helping you achieve PCI DSS compliance while improving resilience against real-world threats.

End-to-end support

From gap analysis and remediation through to assessment and health checks, we support you at every stage of the PCI DSS journey.

Tailored approach

We provide practical, risk-based guidance shaped around your organisation’s goals, ensuring compliance strategies that work in practice, not just on paper.

Previous

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **cybersolutions@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage