PCI DSS 4.0 Compliance for a Defensible, Audit-Ready Payment Security Program

A Strategic Briefing for CISOs, CTOs, Payment Ops Heads, Compliance Officers, and CFOs. PCI DSS 4.0 redefined what payment security means for every organization that stores, processes, or transmits cardholder data.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

PCI DSS 4.0 Compliance

The Gaps Most Organizations Do Not See Until It Is Too Late

Industry Benchmark 80% of organizations fail their initial PCI assessment. The most common reason is inaccurate Cardholder Data Environment scoping, driven not by lack of intent but by underestimated scope.

Current Environment Vulnerabilities & Gaps

Unvalidated CDE Scope

Systems touching the payment path included without formal data flow mapping or QSA review.

MFA Gaps on CDE Access

v4.0 extended MFA to ALL CDE access, not just remote. Many programs only cover remote sessions.

Uninventoried Payment Scripts

Req 6.4.3 mandates script inventory and integrity controls on payment pages. Most teams have not started.

Manual Log Review Processes

v4.0 requires automated log review. Manual processes no longer satisfy the requirement.

Outdated TLS Configurations

Updated TLS requirements under Req 4 are frequently missed during version transitions.

Incomplete Testing Coverage

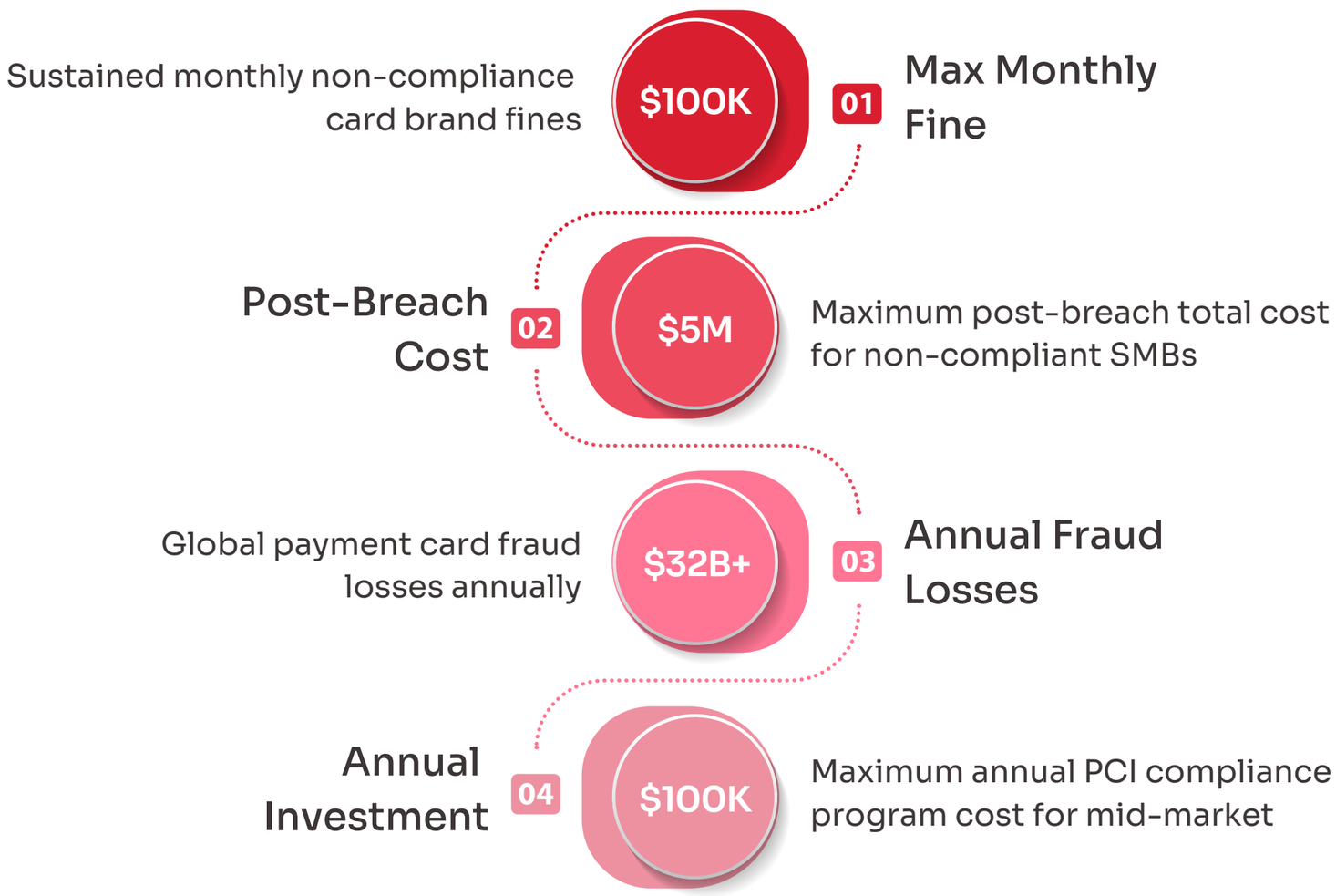
One annual penetration test does not satisfy Requirement 11. Quarterly ASV scans and internal vulnerability scans are also required.

What You Think vs. What We Find

Common Belief	Reality
We use a payment gateway, so PCI DSS does not apply to us	Web servers and redirect systems remain in scope. Malware injected into your payment path keeps liability with you regardless of gateway used.
Tokenization removes us from PCI DSS scope entirely	Tokenization reduces scope, not eliminates it. Tokenization systems remain in scope; QSA review required.
Completing the SAQ means we are fully compliant	The SAQ is a self-attestation. Card brands investigate SAQ accuracy post-breach and have applied maximum penalties for inaccuracies.
PCI DSS v3.2.1 compliance is still acceptable	v3.2.1 is formally retired. All assessments must be conducted against v4.0, including all 64 new requirements.
One annual penetration test satisfies all PCI DSS testing requirements	Req 11 mandates annual internal and external pen testing, quarterly external ASV scans, and internal vulnerability scans.

The Real Cost of Inaction

Why Prevention Is 30 to 60x Cheaper Than a Breach



Actual ROI

Your Actual ROI Calculation

With a Validated
PCI DSS 4.0 Compliance Program

- CDE scope documented with data flow diagrams, QSA reviewed, formally attested
- All 64 new v4.0 requirements assessed, remediated, validated before assessment
- SAQ or ROC completed with technical evidence, reducing post-breach liability
- MFA deployed for all CDE access; authentication hardening controls active
- Payment page script inventory and Req 6.4.3 integrity controls in place
- Cyber insurance underwriting improved with current SAQ and ASV scans
- Card processing rights protected; revenue stream intact through assessment

Compliance Fines Avoided by Regulatory Framework

Framework	Jurisdiction	Penalty Range	Trigger
PCI DSS	Global (Card Brands)	$5K–$100K/month	Non-compliance or breach while non-compliant
GDPR	European Union	Up to €20M or 4% of global turnover	Cardholder data breach involving EU residents
DPDPA	India	Up to ₹250 Crore	Personal data breach including payment data
RBI Guidelines	India	Regulatory action + license risk	Non-compliance for PG, PA, PPI, UPI entities

Common Resistance We Hear and the Facts Behind Each

What Clients Say	Why It Is Costing Them	The Fact
We have never had a breach	Breaches go undetected for an average of 243 days	Average post-breach cost for SMBs is $500K–$1M
We completed our SAQ last year	v3.2.1 is retired and last year's SAQ was conducted against a retired standard	All assessments must now be conducted against v4.0
Our gateway handles everything	Redirect systems and web servers remain in scope regardless	80% of initial PCI assessments fail due to scoping errors
We do not have budget this quarter	Monthly fine exposure starts at $5,000 and escalates to $100,000	Annual compliance investment of $25K–$100K prevents $500K–$5M exposure

Active Vulnerabilities in Your Payment Environment

PCI DSS v4.0 introduced 64 new requirements across all six security goal areas. Below is the technical landscape our assessors examine across every engagement, organized by domain, with specific technologies named.

Identity and Access

- MFA gaps on all CDE access (not just remote)
- Shared credentials and service accounts
- 12-character password minimum enforcement
- Privileged access review cadence

Network Security

- Firewall rule review and segmentation documentation
- Default credential elimination on all network devices
- Unrestricted inbound/ outbound rules
- CDE segmentation validation testing

Data Protection

- PAN storage and truncation rule compliance
- Disk encryption for stored cardholder data
- Updated TLS configuration validation
- Key management lifecycle controls

E-Commerce and Scripts

- Payment page script inventory (Req 6.4.3)
- Script integrity controls and CSP implementation
- Third-party script authorization and monitoring
- Skimming and Magecart-style injection vectors

Logging and Monitoring

- Automated log review implementation
- Log integrity and tamper protection
- Audit trail completeness for CDE events
- Alert thresholds and response procedures

Vulnerability Management

- Quarterly ASV external scan compliance
- Internal vulnerability scan cadence
- Secure SDLC controls for payment applications
- Anti-malware coverage across all CDE systems

Did You Know?

Requirement 6.4.3 is one of the most commonly missed new v4.0 controls. It requires organizations to maintain an inventory of all scripts loaded and executed on payment pages, with a written justification for each. Most e-commerce teams have never performed this inventory.

PCI DSS Requirement 11 mandates four distinct testing activities, annual internal pen testing, annual external pen testing, quarterly external ASV scans, and internal vulnerability scans after significant changes. A single annual pen test satisfies only one of these four obligations.

Did You Know?

Every Layer, Every Component and Every Requirement

Our Commitment is to assess every system, every network path, every access control, and every logging mechanism within your Cardholder Data Environment. Partial coverage is not coverage. It is a gap waiting to be found by a QSA or an attacker.

Identity and Access Management

- MFA deployment across all CDE access vectors
- Password policy enforcement (12-character minimum)
- Privileged account inventory and review
- Service account and shared credential audit
- Access provisioning and de-provisioning controls

Network Security

- Firewall ruleset review and documentation
- CDE segmentation architecture validation
- Default credential elimination verification
- Network diagram accuracy assessment
- Segmentation penetration testing

Data Protection

- PAN storage location discovery and mapping
- Truncation and masking rule validation
- TLS version and cipher suite review
- Encryption key management lifecycle
- Disk encryption for all CDE storage

Application and E-Commerce

- Payment page script inventory (Req 6.4.3)
- Content Security Policy implementation
- Secure SDLC process review
- Web application penetration testing
- Third-party component authorization

Logging and Monitoring

- Automated log review implementation check
- Audit trail completeness for all CDE events
- Log integrity and tamper-evidence controls
- Alert configuration and response procedures
- SIEM coverage mapping to PCI requirements

Compliance Mapping

- All 64 new v4.0 requirements gap assessment
- SAQ type determination and accuracy review
- RBI and CERT-In alignment for India entities
- DORA and GDPR parallel control mapping
- Targeted risk analysis documentation review

Covering Multiple Obligations Through a Single Program

RBI

- India payment security for aggregators, gateways, PPI, UPI

DORA

- EU ICT risk management for financial entities

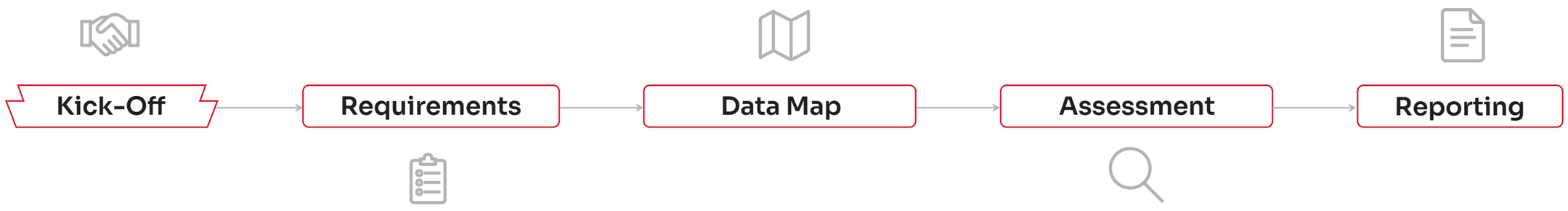
GDPR

- Parallel data protection obligations on cardholder data

PCI P2PE

- Point-to-point encryption for physical environments

What Happens at Every Phase



Each phase is structured to produce QSA-ready documentation. From initial kick-off through security certificate issuance, every activity maps directly to a PCI DSS v4.0 requirement or evidence artifact.

Engagement Timeline by Scope

Scope	Duration	Description
Single Merchant Account / Basic CDE	1–2 Weeks	SAQ eligible merchants with limited CDE systems and straightforward payment flows
Multi System / Moderate Complexity	2–4 Weeks	Mid-market merchants with multiple CDE systems, ecommerce components, and internal networks
Enterprise / Complex Environment	4–6 Weeks	Level 1 merchants or service providers requiring full ROC, multiple business units, and segmentation testing
Multi Cloud or Multi Region	6–8 Weeks	Organizations with cloud hosted CDE components across AWS, Azure, or GCP with cross region data flows

Timeline Drivers

The Four Factors That Affect Duration

1 CDE System Count

The number of in scope systems directly determines assessment depth and evidence collection time.

2 Data Flow Complexity

Undocumented or complex payment flows require additional mapping before testing can begin.

3 Remediation Backlog

Organizations with known gaps may require remediation cycles before reassessment can proceed.

4 Assessment Path

SAQ engagements move faster than full ROC engagements, which require QSA on site validation activities.

What They Actually Deliver

Your Decision on Who Tests You

Not all PCI DSS assessors bring the same credentials, methodology, or post-assessment support. The table below reflects the specific capabilities your program requires under v4.0.

Capability	Typical Consultancy	BriskInfoSec Approach
Accreditation	Self-certified or limited regional recognition	CREST Approved (India's only firm, all regions) + CERT In Empanelled + ISO 27001 2022
Penetration Testing	General pen test report without QSA alignment	CREST approved testers; results meet PCI DSS Req 11.3 QSA documentation standards
CDE Scoping	Template questionnaire without data flow validation	Data flow mapping with QSA-aligned scope documentation and formal gap analysis
v4.0 Gap Coverage	Partial review of selected new requirements	Full gap assessment against all 64 new v4.0 requirements with prioritized remediation plan
E Commerce Controls	General web application testing	Payment page script inventory, Req 6.4.3 integrity controls, CSP implementation
RBI and India Compliance	Limited regional knowledge and no empanelment	CERT-In empanelled for PA, PG, PPI, UPI audits; RBI payment standards fully aligned
Post Assessment Support	Report delivered and engagement closed	CREST approved testers; results meet PCI DSS Req 11.3 QSA documentation standards

Service Provider Levels and Their Assessment Obligations

1 — Level 1 Merchant

6M+ transactions per year. Annual QSA ROC required. Highest obligation tier.

2 — Level 2-3 Merchant

20K to 6M transactions. Annual SAQ plus quarterly ASV scans required.

3 — Level 4 Merchant

Under 20K e-commerce or 1M other transactions. SAQ recommended with scans.

4 — Service Provider L1

300K+ transactions processed. Annual QSA ROC required. Strictest obligations.

Key Insight : The consistent pattern across PCI enforcement cases is that organizations that fail assessments had the right intent but underestimated scope. v4.0 expanded requirements around MFA, e-commerce script integrity, authentication hardening, and automated log review. Most boards are now asking whether all 64 are covered.

Your Path From This Page to Compliance Across Four Engagement Tiers

1 — PCI DSS Gap Assessment

Benchmark all 64 new v4.0 requirements against your current program. Receive a prioritized remediation roadmap with clear ownership and timelines.

2 — CDE Scoping & Remediation

Data flow mapping, scope documentation, penetration testing, and control remediation support. Produces QSA-ready scope artifacts.

3 — Full PCI DSS 4.0 Program

End-to-end implementation through SAQ or ROC completion. Timeline based on merchant level and scope. All 64 requirements covered and validated.

2 — Ongoing Compliance

Quarterly ASV scans, annual pen test cycles, LURA portal evidence management, and annual re-assessment support to maintain continuous compliance.

How We Engage in Three Steps Toward Your Roadmap

Book a Conversation

45-minute confidential discussion to understand your current PCI posture, merchant level, and compliance timeline. No obligation, no sales pressure.

Receive Your Roadmap

Tailored gap assessment scope, v4.0 requirement coverage, and implementation plan delivered within 5 business days of initial discussion.

Partner on Execution

Phased program from CDE scoping through QSA assessment with LURA portal tracking and quarterly compliance maintenance throughout the year.

An Expedited Scoping Proposal

1	Organization Name	Your company or entity name
2	Industry Vertical	E-commerce, Retail, Fintech, Payment Service Provider, or Other
3	Annual Card Transaction Volume	Estimated transactions per year to determine merchant level
4	Current PCI DSS Version in Use	v3.2.1, v4.0, or Not Yet Assessed
5	Merchant or Service Provider Level	Level 1, 2, 3, 4 or Service Provider Level 1 or 2
6	Known CDE Systems in Scope	Approximate count of in-scope systems
7	Previous QSA Assessment or SAQ History	Most recent assessment date and type
8	Preferred Engagement Timeline	When you need to be assessment-ready

Payment security is not something you achieve once. It is something you maintain every day to keep cardholder trust. The organizations that navigate PCI assessments with confidence all maintain a validated, fully-scoped compliance program as an ongoing practice.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique cloud security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

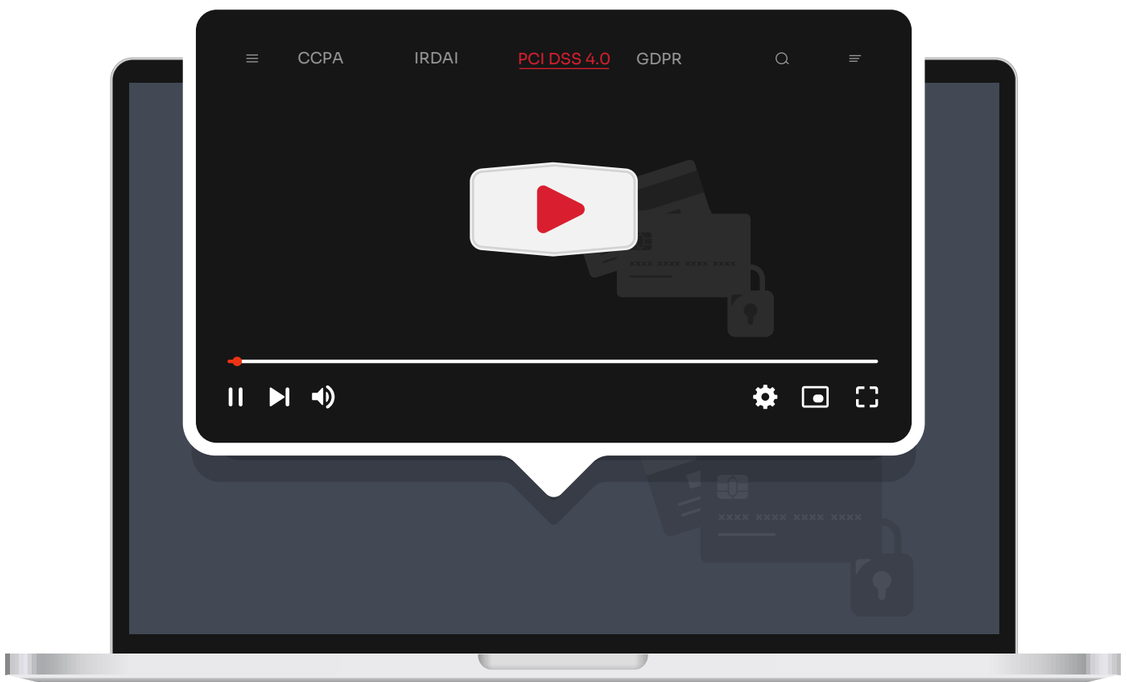
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence
India
UAE