Copla

PCI DSS

Compliance Explainer

Table of content

What is PCI DSS

PCI DSS (v4.0.1) is the global baseline for protecting the cardholder data environment (CDE) across people, processes, and technology.

It applies to any organization that accepts, processes, stores, or transmits payment data, including PAN (Primary Account Number), Sensitive Authentication Data (SAD) such as full track data and CAV2/CVC2/CVV2/CID codes, and PIN/PIN blocks.
Systems that can impact the security of the CDE are in scope too, even if they only route data (e.g., proxies, load balancers, DNS, logging, time sync, jump hosts).
Version & timing: v4.0.1 is active now. Several requirements are future-dated until 31 March 2025, so teams should run a gap assessment and remediation plan now to hit the deadline comfortably.
Card brands (Visa, Mastercard, Amex, Discover, JCB) require compliance via their programs, and the PCI Security Standards Council maintains the standard.

Why it matters

- Reduces breach likelihood and chargeback/fraud exposure
- Required by acquirers and PSPs to open/maintain merchant accounts
- Avoids fines, higher interchange/fees, or termination of processing agreements
- Speeds enterprise security reviews and shortens sales cycles

Who must comply (merchants & service providers)

You must comply if you handle cardholder data (CHD), as it could impact the security of card processing. That includes e-commerce brands, SaaS platforms that take payments, retail/omni-channel sellers, call centers, and third-party service providers (e.g., hosting, managed services, contact centers, payment gateways) that can affect the CDE, even if they only route data.

Merchant validation levels *(brand-defined, based on annual transaction volume):*

- **Level 1** — typically > **6M** transactions/yr (or compromised/brand-mandated) → RoC by QSA/ISA
- **Level 2** — typically **1M–6M** transactions/yr → SAQ (acquirer may require RoC)
- **Level 3** — typically **20k–1M** e-commerce transactions/yr → SAQ
- **Level 4** — typically < **20k** e-commerce or up to ~1M total transactions/yr → SAQ

Validation routes *depend on your payment model and whether you store/process/forward CHD:*

- **SAQ (Self-Assessment Questionnaire):** variants A, A-EP, B, B-IP, C, C-VT, D matched to your payment flows and scope.
- **RoC (Report on Compliance):** independent assessment by a QSA (or ISA for internal) required for Level 1 merchants and most service providers, or whenever your acquirer/brand mandates it.

Service providers

Usually require an annual RoC regardless of volume and must provide a current AoC to customers (often referenced in card-brand or customer compliance packages).

The manual compliance burden *(without automation)*

Preparation effort depends heavily on scope (do you store/process CHD? Do you host payment pages? How segmented is your network?).

PCI DSS v4.0 also introduces targeted risk analyses (TRAs) and authentication changes that can add preparation time, especially if you're moving from SAQ A-EP to SAQ D or expanding your in-house CDE.

By scope: first-time readiness

Merchants (no CHD storage; hosted fields/tokenization — SAQ A/A-EP)

- Policies, risk, roles, training: **~80–140h**
- CDE scoping & data-flow mapping: **~40–70h**
- Secure configuration, patch/vuln mgmt, AV/EDR: **~60–100h**
- Logging/monitoring & access reviews: **~40–80h**
- Third-party due diligence (PSP, CDN, hosting): **~30–60h**
- Incident response & breach comms runbook: **~20–40h**

Subtotal: ~270–490h over 2–4 months

v4.0 uplift: budget +10–15% if TRAs and auth updates require process changes.

Ongoing run-state (typical)

- Quarterly: external ASV scans, internal scans, access reviews **(~12–20h/qtr)**
- Annual: pen test, IR test, policy refresh, SAQ/RoC package **(~60–120h/yr)**
- Evidence retention: maintain 12 months of logs and supporting artifacts to prove continuous compliance (not just an annual snapshot).

Service providers/merchants with in-house CDE (SAQ D or RoC)

- Network segmentation & hardening (FW, IDS/IPS): **~120–180h**
- Key management & crypto, PAN protection: **~70–120h**
- Secure SDLC & change control: **~80–130h**
- Logging/SIEM, FIM, time sync, retention: **~100–160h**
- Vulnerability mgmt (ASV scans, internal scans, pen test prep): **~120–180h**
- Physical & facility security: **~30–60h**
- Vendor management & AoCs: **~50–90h**
- Policies, risk, training, IR exercises: **~120–190h**

Subtotal: ~690–1,110h over 4–7 months

v4.0 uplift: plan +10–20% for TRAs, auth, and logging/control evidence expansion.

Indicative internal cost (blended €6–8k/month per FTE)

- SAQ A/A-EP merchants: **€25k–€55k**
- SAQ D / RoC environments: **€60k–€120k** (excludes external QSA fees, ASV scans, and pen tests)

By organization size — first-time readiness

Org size	< 50 people	50–150 people	150+ people
Typical path	SAQ A/A-EP (hosted payments)	SAQ D (partial in-house CDE)	RoC (full CDE/ service provider)
Timeline	2–4 mo	4–6 mo	5–7 mo
Internal effort	270–490h	500–850h	700–1,100h
Indicative internal cost*	€25k–€55k	€45k–€95k	€60k–€120k

* Costs assume blended €6–8k/month per FTE; excludes QSA fees, ASV scans, pen tests.

Note: If adopting new v4.0 future-dated requirements (e.g., TRAs, auth changes) in this cycle, expect the high end of the bands, or add ~10–20% buffer, particularly when moving A-EP → D.

PCI DSS v4.0 at a glance (key updates)

1. ***v3.2.1 retired on 31 Mar 2024; v4.0 is fully active.***

2. ***Future-dated v4.0 requirements effective 31 Mar 2025 (selected examples):***

   - 3.4.2 PAN masking enhancement: limit display (e.g., BIN + last 4) unless a documented business need justifies more.
   - 5.2.3 Anti-malware coverage: broadened expectations for commonly affected systems and periodic evaluations of effectiveness.
   - 8.x Authentication changes: stronger MFA coverage, updated password/auth policies, and use of Targeted Risk Analyses (TRAs) to set/justify certain intervals and parameters.
   - 10.x Logging & monitoring expansion: centralized logging, integrity protections, time sync, and review frequencies increasingly driven by TRAs; reinforce 12-month retention with sufficient online availability for recent logs.
   - Targeted Risk Analyses (TRAs): required for specific controls to tailor frequencies (e.g., password changes, monitoring/review cadence, scanning).

3. ***v4.0.1 is a clarification release — it does not add/remove requirements, but refines guidance and examples. Ensure your SAQ/RoC templates and evidence mappings are updated to the v4.0.1 formats and wording.***

The 12 PCI DSS requirement families

1. **Secure network & systems** — *configure firewalls/routers; harden services*
2. **Apply secure configurations** — *remove vendor defaults; enforce baselines*
3. **Protect stored account data** — *minimize storage; strong crypto & key mgmt*
4. **Protect transmissions of CHD** — *strong encryption in transit*
5. **Protect systems & networks from malware** — *AV/EDR; evaluate effectiveness*
6. **Develop & maintain secure systems/software** — *patching, vuln mgmt, SDLC*
7. **Restrict access by business need-to-know** — *RBAC, approvals, least privilege*
8. **Identify & authenticate users** — *MFA, strong auth, unique IDs*
9. **Restrict physical access** — *facilities, media, visitor controls*
10. **Log & monitor all access** — *centralized logs, time sync, integrity, reviews*
11. **Test security regularly** — *ASV/internal scans, pen testing, FIM*
12. **Support infosec with policies & governance** — *risk mgmt, training, supplier/vendor oversight, incident response, continuous improvement (v4.0 elevates vendor management and uses Targeted Risk Analyses to tune frequencies)*

PCI DSS v4.0 aligns more closely with ISO/IEC 27001, use your ISO ISMS as the backbone (policies, risk, controls, evidence) to streamline PCI work and avoid duplicate artifacts.

Where the burden spikes

Scope & data-flows

Shrinking the CDE via tokenization/ segmentation; keeping PAN out of logs, tickets, analytics

Logging & evidence

Proving the 13 domains with living records (access reviews, change logs, DR tests, correlating system/ app/cloud logs with access reviews; ensuring 12-month retention and recent online availability training).

Vulnerability management

Coordinating ASV + internal scans, remediation SLAs, and pen tests; proving closure evidence

Third-party attestations

Collecting AoCs; contracts that clearly allocate PCI responsibilities (shared-responsibility matrices)

Crypto & key management

HSMs/KEKs, rotation, dual-control, split-knowledge; documenting key lifecycle and custodians

Crypto & key management

HSMs/KEKs, rotation, dual-control, split-knowledge; documenting key lifecycle and custodians

Third-party attestations

Collecting AoCs; contracts that clearly allocate PCI responsibilities (shared-responsibility matrices)

90-day starter plan

Phase 1 — Mobilize (Weeks 1–3)

- Map payment flows and define scope & segmentation (shrink the CDE).
- Build the asset & data inventory.
- Identify all service providers early; collect current AoCs and set a PCI responsibility matrix.
- Select the SAQ/RoC route with your acquirer.
- Stand up the evidence workspace (policies, training, access-review cadence).
- Run a v4.0 future-dated gap assessment (TRAs, authentication changes, logging/12-month retention); create a remediation plan targeting 31 Mar 2025 items.

Phase 2 — Implement (Weeks 4–10)

- Close top gaps: enforce MFA for all CDE access (admin + user + remote).
- Harden configurations and apply secure baselines.
- Deploy/tune SIEM logging with time sync and 12-month retention (keep recent logs online).
- Schedule ASV & internal scans; track remediation SLAs.
- Finalize the incident-response plan and communications runbook.
- Draft cryptography & key-management procedures (custodians, rotation, dual-control).
- Progress vendor remediations identified in Phase 1 (AoCs, contract responsibilities).

Phase 3 — Prove & prepare (Weeks 11–13)

- Run scans & pen test; capture results.
- Remediate findings and retest to verify closure.
- Complete SAQ or prepare RoC package (evidence, mappings, narratives).
- Conduct an incident-response tabletop exercise now, and schedule it at least annually.
- Finalize executive attestation and issue the AoC.

How Copla reduces cost & time

Platform accelerators

- **Scope minimization toolkit:** tokenization & hosted-payment patterns, segmentation guide, and CDE boundary visuals
- **Pre-mapped v4.0 control set:** ready-to-tailor policies & procedures across all 12 requirements, with task owners and acceptance criteria
- **Evidence automation:** access reviews, training records, vendor AoCs, scan/pen-test tracking, and audit-ready exports (SAQ/RoC/AoC)
- **Risk & change workflows:** targeted risk analyses, change tickets, approvals, and demonstrable trails for QSAs

Typical outcomes

- **40–70%** faster readiness; **40–70%** lower internal compliance cost
- **2× better audit-readiness** (first-pass evidence completeness)
- **Fewer scope errors** via early data-flow mapping and tokenization patterns

Executive one-pager

Non-optional

PCI DSS is required to accept cards; non-compliance risks fines, fee hikes, and loss of processing

Scope drives effort

Smallest possible CDE = fastest path

Prove, not just claim

Logs, scans, key management, and vendor AoCs must be demonstrable

Action plan

Fund a 90-day starter; select SAQ/RoC path; automate evidence

Merchant Levels & validation paths *(at a glance)*

Level	1	2	3	4
Typical annual volume (brand-defined)	> 6M txns/yr (or brand-mandated)	~1M–6M txns/yr	~20k–1M e-commerce txns/yr	< 20k e-commerce or up to ~1M total txns/yr
Validation path	RoC	SAQ (acquirer may require RoC)	SAQ	SAQ
Assessor	QSA/ISA	Merchant (or QSA)	Merchant	Merchant
Output	RoC + AoC	SAQ + AoC (or RoC)	SAQ + AoC	SAQ + AoC

Service providers usually require an annual RoC regardless of volume and must provide a current AoC to customers.

Quick readiness checklist

- [ ] *Payment data-flows diagrammed; CDE boundary defined and minimized*
- [ ] *Correct SAQ/RoC path selected with acquirer agreement*
- [ ] *Policies approved; training launched; access governance set (RBAC + MFA)*
- [ ] *MFA enforced for all access to the CDE (not just admin)*
- [ ] *Secure configurations in place; patch/vuln cadence defined*
- [ ] *Logging/SIEM active; time sync & 12-month retention proven*
- [ ] *Quarterly ASV and internal scans scheduled; pen test plan defined*
- [ ] *Targeted Risk Analyses (TRAs) performed and documented for applicable controls*
- [ ] *Crypto & key mgmt documented; key custodians assigned*
- [ ] *Vendor AoCs collected; contracts reflect PCI responsibilities*
- [ ] *IR tabletop exercise conducted (and on an annual schedule)*
- [ ] *SAQ/RoC package prepared; AoC ready for customers*

Resources & next steps

Book a PCI DSS readiness review with our experts

Explore our PCI DSS blog for practical guides and expert insights.

Copla

PCI DSS COMPLIANT