GRC Interview & Study Guide

SOC 2 & PCI DSS

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

Service organisation assurance reports and the payment card industry security standard.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

SOC 2 & PCI DSS

Service organisation assurance reports and the payment card industry security standard.

Q: What is a SOC 2 report?

Basic

SOC 2 is an attestation report issued by an independent CPA firm under AICPA standards. It reports on a service organisation's controls relevant to the AICPA Trust Services Criteria:

- Security (the common criteria — always included).
- Availability.
- Processing Integrity.
- Confidentiality.
- Privacy.

The organisation chooses which criteria beyond Security are in scope. SOC 2 is not a certification — it is an auditor's opinion, and reports are generally restricted to customers and other parties with sufficient knowledge.

Practical example: A US hospital asks its cloud billing vendor for its SOC 2 Type II report instead of auditing the vendor itself, and reviews it annually as part of vendor monitoring.

Why this matters: SaaS and healthcare technology vendors are frequently asked for SOC 2 reports by customers; it is often a requirement to win deals.

Q: What is the difference between SOC 2 Type I and Type II?

Basic

- **Type I:** assesses whether controls are suitably designed and implemented as of a specific date.
- **Type II:** assesses design and operating effectiveness over a period of time (commonly 6 to 12 months; shorter for a first report).

Type II gives much stronger assurance because the auditor tests samples across the whole period. Many customers require a Type II.

Practical example: Type I (as of 30 June): the access review control is designed properly. Type II (1 Jan–30 June): the auditor tested samples across six months and found it operated every quarter.

Why this matters: A favourite interview question. It also maps directly to design vs operating effectiveness.

Q: What is PCI DSS and who must comply?

Basic

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements maintained by the PCI Security Standards Council. It applies to all entities that store, process or transmit cardholder data or sensitive authentication data, or that can affect the security of that environment — merchants, processors and service providers.

- Compliance is enforced contractually through card brands and acquiring banks, not by law (though some laws reference it).
- The current version is PCI DSS v4.0.1; v3.2.1 was retired in 2024, and requirements that were 'future-dated' in v4.0 became mandatory from 31 March 2025.
- Validation is via a Report on Compliance (ROC) by a Qualified Security Assessor or a Self-Assessment Questionnaire (SAQ), depending on volume and brand rules.

Practical example: A clinic that takes card payments for co-pays at the front desk is a merchant and must comply with PCI DSS. In practice it usually completes a Self-Assessment Questionnaire through its acquiring bank.

Why this matters: Any organisation that takes card payments has PCI obligations; scope mistakes are one of the most expensive errors in compliance.

Q: What are the five Trust Services Criteria categories in SOC 2?

Basic

- **Security (the Common Criteria, CC1–CC9):** mandatory in every SOC 2.
- **Availability:** the system is available for operation and use as committed.
- **Processing Integrity:** processing is complete, valid, accurate, timely and authorised.
- **Confidentiality:** information designated as confidential is protected.
- **Privacy:** personal information is collected, used, retained, disclosed and disposed of in line with commitments.

The criteria come from the AICPA's 2017 Trust Services Criteria, with revised points of focus published in 2022.

Practical example: A cloud EHR vendor includes Security, Availability and Confidentiality in its SOC 2 because hospital customers care most about uptime and protection of records. It leaves Processing Integrity out for now.

Why this matters: Choosing the right categories shapes the audit scope, cost and value to customers.

Q: What is the SOC 2 Common Criteria structure (CC1–CC9)?

Basic

- **CC1–CC5 follow the COSO internal control components:** Control Environment, Communication and Information, Risk Assessment, Monitoring Activities and Control Activities.
- CC6 Logical and Physical Access Controls.
- CC7 System Operations (including detection and incident response).
- CC8 Change Management.
- CC9 Risk Mitigation (including vendor and business partner risk).

Each criterion has points of focus that help, but they are not a checklist of mandatory requirements.

Practical example: The company maps its quarterly access review to CC6.2/CC6.3, its SIEM alerting to CC7.2, its CAB process to CC8.1, and its vendor reviews to CC9.2.

Why this matters: Knowing the structure helps you map controls efficiently and understand where an auditor will look for each topic.

Q: What is a QSA, an ISA, an ASV and an SAQ in PCI DSS?

Basic

- **QSA (Qualified Security Assessor):** an independent assessor approved by the PCI Security Standards Council who performs on-site assessments and signs Reports on Compliance (ROCs).
- **ISA (Internal Security Assessor):** a trained employee who can perform internal assessments.
- **ASV (Approved Scanning Vendor):** performs the quarterly external vulnerability scans required by PCI DSS.
- **SAQ (Self-Assessment Questionnaire):** a self-assessment for eligible merchants and service providers, with different types (A, A-EP, B, C, D and others) depending on how cards are accepted.

Which validation is required depends on the merchant level or service provider level set by card brands and acquirers.

Practical example: A mid-sized merchant validates with an SAQ D signed by an officer, uses an ASV for quarterly external scans, and its acquirer asks for a QSA-led ROC once transaction volume crosses the next level.

Why this matters: PCI terminology is used heavily in interviews and real projects. Mixing these up suggests a lack of hands-on experience.

Q: A small clinic asks which PCI DSS SAQ applies when it uses a standalone card terminal at the front desk. How do you guide them?

Basic · **Scenario**

- **Start by documenting how cards are accepted:** the type of terminal, how it connects (phone line, IP, mobile), and whether any card data is stored or written down.
- Standalone terminals often fit SAQ B (or SAQ B-IP for IP-connected devices), if all eligibility criteria are met.
- Confirm with the acquiring bank, which decides validation requirements.
- **Basic controls still apply:** inspect terminals for tampering, never keep card numbers on paper, train staff.
- If cards are also taken over the phone and keyed into a web portal, a different SAQ may apply.

Practical example: The clinic uses one IP-connected terminal approved for PCI and stores no card data. With the acquirer's confirmation it completes SAQ B-IP and adds a weekly terminal inspection checklist for front-desk staff.

Why this matters: Small merchants are often over-burdened by choosing the wrong SAQ, or under-protected by ignoring the eligibility criteria.

Q: What is the difference between SOC 1, SOC 2 and SOC 3?

Intermediate

- **SOC 1:** controls relevant to user entities' internal control over financial reporting (e.g. payroll or billing processors).
- **SOC 2:** controls relevant to security, availability, processing integrity, confidentiality and privacy. Detailed, restricted use.
- **SOC 3:** a general-use summary of a SOC 2 engagement without the detailed control testing — suitable for public distribution.

Practical example: A payroll processor gives its clients' financial auditors a SOC 1 (it affects financial statements), gives security teams a SOC 2 under NDA, and posts a SOC 3 seal on its website.

Why this matters: Asking for the right report from a vendor (or providing the right one to customers) saves time in third-party risk reviews.

Q: What are the 12 requirements of PCI DSS?

Intermediate

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 strong 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 organisational policies and programs.

Practical example: Requirement 3 (protect stored account data) means the e-commerce database must not keep CVV codes after authorisation and must render PANs unreadable, e.g., by tokenisation.

Why this matters: You do not always need them word for word, but you should know the themes and be able to place a control within them.

Q: How can an organisation reduce its PCI DSS scope?

Intermediate

- Network segmentation to isolate the cardholder data environment (CDE) from other systems (validated by testing).
- Do not store card data unless there is a business need; never store sensitive authentication data (e.g. full track data, card verification codes, PINs) after authorisation.
- Tokenisation, so internal systems handle tokens instead of primary account numbers (PANs).
- Point-to-point encryption (P2PE) solutions validated by the PCI SSC.
- Outsourcing payment pages to a compliant payment service provider (e.g. hosted payment page or redirect).

Outsourcing reduces scope but does not remove all responsibility — service provider compliance must be monitored.

Practical example: An online shop moves to a hosted payment page (iframe/redirect) from its PSP, so card data never touches its servers. That can reduce it from SAQ D to a much shorter SAQ A, if the eligibility criteria are met.

Why this matters: Less scope means fewer systems to secure and audit — lower cost and lower risk.

Q: What are the key changes in PCI DSS v4.0/v4.0.1, and what became mandatory on 31 March 2025?

Intermediate

PCI DSS v4.0 was published in 2022 and v4.0.1 (a limited revision with clarifications) in 2024. v4.0 was retired at the end of 2024. Key themes:

- **Two ways to validate:** the defined approach and the customized approach.
- Targeted risk analyses (12.3.1) to justify the frequency of some activities.

Many requirements were 'future-dated' (best practice until 31 March 2025, then mandatory), including:

- MFA for all access into the cardholder data environment (8.4.2).
- Management of payment page scripts (6.4.3) and change and tamper detection on payment pages (11.6.1).
- Automated technical controls against phishing (5.4.1) and authenticated internal vulnerability scans (11.3.1.2).

Always check the current Council documents and FAQs for exact wording.

Practical example: An e-commerce site implements a script inventory with business justification and integrity checks for every script on its checkout page (6.4.3), and a tamper-detection tool that alerts on unauthorised page changes (11.6.1), to counter web-skimming attacks.

Why this matters: Many organisations are still embedding the future-dated requirements. Interviewers expect you to know what changed and why.

Q: What is the customized approach in PCI DSS v4.x?

Intermediate

- The defined approach follows each requirement and its testing procedures as written.
- The customized approach lets an entity meet a requirement's stated objective with its own control design, when it has a mature risk management process.
- The entity must document a controls matrix and a targeted risk analysis for each customized requirement, and the assessor designs testing procedures.
- Some requirements cannot use the customized approach, and it is not available through self-assessment questionnaires.

It is not a shortcut. It usually requires more documentation and evidence, not less.

Practical example: A large bank uses a modern continuous authentication and device-trust model instead of a specific password rule. It documents the control's objective coverage, a targeted risk analysis and testing evidence, which the QSA validates.

Why this matters: The customized approach is a big conceptual change in PCI DSS and a favourite interview topic for advanced roles.

Q: What is a bridge letter (gap letter) in SOC reporting?

Intermediate

A bridge letter is a statement from the service organisation's management covering the period between the end of the last SOC report and the current date (or the next report).

- It states whether there have been material changes to the system or controls, and whether management is aware of any control failures.
- It is a management assertion, not audited, so it gives limited assurance.
- Customers typically accept bridge letters for a short gap (often up to about 3 months). Beyond that they should ask for a newer report or other evidence.

Practical example: A vendor's SOC 2 period ended 31 March, and you are reviewing in August. You request a bridge letter covering April–July and check it against news of incidents and changes in the vendor's service.

Why this matters: Vendor reviews often happen months after the SOC report period. Knowing what a bridge letter does and does not provide avoids false assurance.

Q: What are complementary user entity controls (CUECs) and subservice organisations in a SOC report?

Intermediate

- CUECs are controls the customer (user entity) must operate for the service organisation's controls to achieve their objectives. Example: the customer must remove its own users from the vendor's platform.
- Subservice organisations are vendors the service organisation relies on, such as a cloud hosting provider.

- **Carve-out method:** the subservice organisation's controls are excluded from the report, so you need its own SOC report.
- **Inclusive method:** the subservice organisation's controls are included and tested in the report.
- Complementary subservice organisation controls (CSOCs) are controls the subservice organisation is expected to operate.

Practical example: A SOC 2 for a billing platform lists the CUEC 'customers are responsible for reviewing their user access quarterly'. The hospital adds this to its own access-review control and audit evidence.

Why this matters: Many customers skip these sections, then assume protection they do not have. CUECs become your own control obligations.

Q: A vendor sends you a SOC 2 Type I when you asked for Type II. What do you do?

Intermediate · **Scenario**

- **Understand why:** they may be new to SOC 2 and have a Type II in progress.
- A Type I only shows control design at a point in time. It does not show the controls operated over a period.
- Ask for the Type II timeline, the planned period and any interim evidence (penetration test, ISO certificate, internal audit results).
- **For a high-risk vendor, consider contract conditions:** provide the Type II within a set time, with the right to further assessment if it is qualified.
- Record the residual risk and get acceptance if onboarding proceeds.

Practical example: The vendor's Type II period ends in four months. You approve onboarding with no PHI in the pilot, a contract clause requiring the Type II report within 30 days of issue, and a VP risk acceptance for the interim period.

Why this matters: Accepting a Type I as if it were a Type II is a common TPRM mistake that leaves operating risk untested.

Q: Your company wants to stop storing card numbers but needs to issue refunds. What options reduce PCI DSS scope?

Intermediate · **Scenario**

- **Tokenisation:** replace the PAN with a token from the payment service provider, which can be used for refunds and recurring payments without holding the card number.
- Use the PSP's hosted payment pages or iframes so card data never touches your systems.
- Delete historical PAN data after confirming retention needs (requirement 3.2.1) and that no business process depends on it.
- Segment any remaining systems that still touch card data, and validate segmentation by testing.
- Update the data flow diagram and confirm scope with your QSA or acquirer.

Practical example: A clinic chain replaces stored card numbers with PSP tokens, deletes 5 years of old card data, and moves from SAQ D to a much smaller assessment because card data no longer enters its environment.

Why this matters: The cheapest PCI control is not holding card data. Scope reduction lowers cost and breach risk together.

Q: An e-commerce site discovers an unknown script on its checkout page. What do you do?

Intermediate · **Scenario**

1. Treat it as a possible web-skimming (Magecart-style) incident. Activate incident response.
2. Remove or block the script, preserve evidence (page source, logs, timeline) and find how it got there.
3. Determine the exposure window and whether card data could have been captured.
4. **Follow PCI incident procedures:** inform your acquirer and card brands as required, and consider whether a PCI Forensic Investigator (PFI) is needed.
5. **Strengthen controls:** script inventory and authorisation (6.4.3), change and tamper detection (11.6.1), Content Security Policy and subresource integrity.

Practical example: The tamper-detection tool alerts on a new script loading from a look-alike domain. It is removed within an hour, logs show a 3-day exposure window, the acquirer is notified, and the team traces the injection to a compromised third-party marketing plugin.

Why this matters: This is exactly the threat the PCI DSS v4 script requirements were written for, and it is a realistic interview scenario.

Q: When reviewing a vendor's SOC 2 report, what do you look for?

Advanced

- Report type (Type II preferred), period covered and how recent it is; ask for a bridge letter if there is a gap to today.
- **Scope:** are the services and systems you use actually included? Which Trust Services Criteria are covered?
- **Auditor's opinion:** unqualified vs qualified (qualified means significant issues).
- Exceptions/deviations in testing and management's responses.
- Subservice organisations (e.g. cloud hosting) and whether they are carved out or included — you may need their reports too.
- **Complementary User Entity Controls (CUECs):** controls your organisation must operate for the vendor's controls to be effective.

Practical example: While reviewing a vendor's SOC 2, you notice the period ended 11 months ago, the data centre is carved out, and there is an exception on change management. You ask for a bridge letter, the hosting provider's report, and the remediation status.

Why this matters: Simply collecting a SOC 2 PDF is not due diligence. Reading it properly is what protects the organisation.

Q: How should you read the auditor's opinion and exceptions in a SOC 2 report?

Advanced

- **Opinion types:** unqualified (clean), qualified (one or more criteria not met), adverse or disclaimer (rare and serious).
- Section 4 lists tests and results. Exceptions do not automatically mean a qualified opinion. Consider how many, how severe and whether other controls compensate.
- Read management's responses to exceptions and check whether fixes are dated and credible.
- **Check the scope and period:** are the services you use in scope? Is the period recent?
- Record your conclusions and any follow-up questions in the vendor risk file.

Practical example: The report has an unqualified opinion but 3 exceptions in change management (deployments without approval). You ask the vendor for its remediation status and add a contract commitment to notify you of significant changes.

Why this matters: A SOC 2 report is only useful if you read it critically. A clean opinion with narrow scope can still leave your risk untreated.

Q: What is the difference between a PCI DSS service provider and a merchant, and why does it matter for vendors?

Advanced

- A merchant accepts payment cards for goods or services.
- A service provider is a business that stores, processes or transmits account data on behalf of another entity, or could affect the security of that data (for example managed security or hosting providers).
- Merchants must manage their service providers under requirement 12.8, including written agreements and monitoring their PCI DSS compliance status annually.
- Service providers have extra requirements, and requirement 12.9 requires them to acknowledge their responsibility to customers in writing.
- A responsibility matrix (who does which requirement) is essential.

Practical example: A merchant uses a payment gateway and a managed firewall provider. It obtains each provider's PCI DSS Attestation of Compliance, a responsibility matrix, and reviews them yearly as part of its own assessment evidence.

Why this matters: Most card breaches involve third parties. Clear responsibility splits prevent gaps that both sides assume the other is covering.

Q: Your QSA says your network segmentation is not adequate, so the whole corporate network is in PCI scope. What do you do?

Advanced · **Scenario**

- **Understand the gap precisely:** which connections are allowed between the CDE and other networks, and which segmentation tests failed.
- **Redesign segmentation:** strict firewall rules allowing only necessary traffic, separate admin paths (jump hosts with MFA), and no shared services that bypass controls.
- Run segmentation penetration testing to prove isolation. Service providers must test every six months; merchants at least annually and after changes.
- Consider reducing the CDE further (tokenisation, outsourcing payment processing).
- Agree the timeline with the QSA and acquirer. Until fixed, the larger scope applies.

Practical example: The test showed the corporate Wi-Fi could reach a CDE database port. The rule is removed, admin access moves to an MFA jump host, a retest confirms isolation, and the QSA accepts the reduced scope for the assessment.

Why this matters: Segmentation is the main tool for PCI scope control. When it fails, compliance cost and risk both grow sharply.

Q: A customer finds out your SOC 2 report excludes the product they are buying. How do you handle it?

Advanced · **Scenario**

- Be transparent about the current scope and why the product was excluded (for example, it was launched after the period started).

- **Offer alternative assurance:** how the product inherits shared controls (identity, change management, hosting) that are in scope, plus a penetration test summary or ISO certificate.
- Commit to a timeline for adding the product to the next SOC 2 period, and offer a bridge letter.
- Review your SOC 2 scope process so new products are added in time and sales teams describe the scope accurately.

Practical example: The new analytics module launched mid-period. The customer receives a letter explaining which shared controls cover it, a recent pentest summary, and a commitment to include it in next year's SOC 2. Sales materials are corrected.

Why this matters: Scope mismatches damage trust and can affect contracts. Honesty plus a credible plan is the best response.

Q: You are moving from SOC 2 Type II annual audits to continuous assurance. How would you design it?

Advanced · **Scenario**

- Automate evidence collection for key controls from source systems (cloud configuration, identity, ticketing, endpoint management).
- Define control health checks with thresholds and alerts, so failures are seen and fixed within days rather than found by the auditor months later.
- Keep a log of exceptions and remediation, which becomes evidence of monitoring (CC4).
- Agree with the audit firm how they will use the automated evidence, and whether shorter or rolling report periods would help customers.
- Share a customer-facing trust centre with current status and documents.

Practical example: Daily checks flag any production storage bucket without encryption. Each alert opens a ticket closed within 48 hours, and the auditor tests the monitoring control plus a sample of tickets instead of manual screenshots.

Why this matters: Customers want current assurance, not a report that is a year old. Continuous controls monitoring reduces audit effort and surprises.