SSB DEFENCE

PCI DSS READINESS GUIDE

Protecting Payment Data and Building Practical Compliance

Hospitality • Retail • E-commerce • Professional Services
POS • Online Payments • Virtual Terminals • Third-Party Providers

PRACTICAL GUIDANCE FOR BUSINESS LEADERS
Version 1.0 | August 2026

Important notice

This guide provides general PCI DSS, cybersecurity and business-readiness information. It is not a PCI DSS assessment, Attestation of Compliance, legal opinion or substitute for instructions from your acquirer or payment brand. Confirm your required validation method with the organization that accepts your PCI DSS compliance documentation.

Executive Summary

PCI DSS is the global payment-card security standard for organizations that store, process or transmit cardholder data, and for systems that can affect the security of the cardholder data environment. The current active standard is PCI DSS v4.0.1.

A central distinction for business owners is the difference between compliance and validation. PCI DSS requirements can apply regardless of merchant size. Merchant level generally determines how compliance is demonstrated - for example through a Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC).

Transaction count - not sales revenue

Merchant validation levels are generally based on the number and type of card transactions over a 12-month period, not on a dollar-sales threshold. Payment brands and acquirers manage their own compliance programs, so the exact validation requirement must be confirmed with the merchant's acquirer or compliance-accepting entity.

What this guide will help you do

- Understand PCI DSS v4.0.1 in practical business language.
- Recognize the difference between self-assessment and externally assessed validation.
- Understand common merchant-level thresholds and why they are not dollar-revenue thresholds.
- Identify the payment systems and vendors that create PCI DSS scope.
- Reduce scope by simplifying how payment data moves through the business.
- Address e-commerce, hospitality, retail and legacy-system risks.
- Build a management-level PCI DSS readiness checklist and roadmap.

1. PCI DSS in Plain Language

PCI DSS is maintained by the PCI Security Standards Council. The payment brands and acquiring institutions operate the programs that require merchants and service providers to validate compliance.

PCI DSS v4.0.1 was published in June 2024 as a limited revision to v4.0. It did not add or remove requirements. Requirements that were previously future-dated became effective on 31 March 2025 and should now be treated as current requirements.

The 12 requirements

- 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 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 systems and processes regularly.
- 12. Support information security with organizational policies and programs.

PCI DSS is not a product

No firewall, endpoint product, payment terminal or cloud service can make an organization PCI compliant by itself. Compliance depends on the design and operation of the entire applicable environment.

2. Understand the Payment Environment

Before selecting an SAQ or buying security tools, map how payment information enters, moves through and leaves the business. Scope often becomes larger because payment systems are unnecessarily connected to general business networks.

Common payment channels

- Standalone payment terminals and integrated POS systems.
- Hotel PMS and restaurant/bar POS integrations.
- E-commerce websites, shopping carts and booking engines.
- Hosted payment pages, redirects and embedded payment forms.
- Virtual terminals used by authorized staff.
- Mail-order / telephone-order processes.
- Recurring billing and stored-payment-token arrangements.
- Third-party payment gateways, processors and managed service providers.

Scope reduction

The simplest system to secure is often the system that never needed access to payment data in the first place. Segmentation, validated P2PE solutions, tokenization and properly outsourced payment functions can reduce exposure when implemented correctly.

3. Merchant Levels: Self-Assessed vs. Externally Assessed

Merchant levels are payment-brand program classifications used to determine validation requirements. They are not PCI DSS requirements themselves, and they are not based on annual sales revenue. The examples below illustrate current Visa and Mastercard structures; the merchant must confirm its actual classification and required evidence with its acquirer/payment brand.

Example level	Typical annual transaction volume	Typical validation	Practical meaning
Level 1	Over 6 million transactions (all channels)	ROC / AOC; external QSA commonly required by program	Formal assessment and evidence review.
Level 2	1 million to 6 million transactions	Generally SAQ / AOC	Merchant commonly self-assesses, subject to brand/acquirer rules.
Level 3	E-commerce volume below Level 2 threshold; brand definitions vary	Generally SAQ / AOC	E-commerce-focused validation category.
Level 4	Other smaller merchants below higher-level thresholds	SAQ or acquirer-defined validation	PCI DSS still applies; validation may be managed primarily by the acquirer.

Visa example - August 2026

Visa currently classifies Level 1 as over 6 million Visa transactions annually, Level 2 as 1-6 million, and Level 3 as less than 1 million Visa e-commerce transactions. Visa's public program materials state that merchant level is determined by total Visa transaction volume over 12 months.

Mastercard example - 2026

Mastercard's 2026 rules use Level 1 above 6 million Mastercard/Maestro transactions, Level 2 above 1 million through 6 million, Level 3 for certain e-commerce merchants, and Level 4 for merchants not classified in Levels 1-3. Mastercard also permits or requires different validation treatment in specified circumstances.

A merchant can be moved to a higher level

Payment brands or acquirers may impose enhanced validation based on risk, including after a compromise. A low transaction count should never be treated as a guarantee that self-assessment will always be accepted.

4. Which SAQ Applies?

An SAQ is not chosen simply by merchant size. Eligibility depends on how payments are accepted and whether the environment meets every eligibility criterion for that SAQ. PCI SSC advises merchants to confirm validation and reporting requirements with the compliance-accepting entity.

SAQ A Card-not-present merchants that fully outsource account-data functions and meet all SAQ A eligibility criteria.

SAQ A-EP E-commerce merchants that outsource payment processing but whose website can affect the security of the payment transaction.

SAQ B / B-IP Certain merchants using imprint machines or qualifying standalone dial-out/IP-connected terminals, subject to the SAQ's exact eligibility criteria.

SAQ C / C-VT Certain payment-application or virtual-terminal environments that meet the specific eligibility conditions.

SAQ P2PE Merchants using a PCI-listed validated point-to-point encryption solution and meeting the SAQ's eligibility criteria.

SAQ D Merchants that do not qualify for a shorter SAQ or have a broader applicable environment.

Do not pick the easiest questionnaire

Using the wrong SAQ can create a false sense of compliance. The payment design determines SAQ eligibility; the acquirer/payment brand determines what validation evidence it will accept.

5. E-commerce & Website Security

Outsourcing payment processing does not make the merchant website irrelevant. A compromised merchant page can redirect a customer, alter payment flow or introduce malicious scripts even where the card data is ultimately entered into a third-party payment service.

Current PCI SSC guidance for SAQ A distinguishes between redirects/fully outsourced payment functions and embedded payment forms. SAQ A merchants with e-commerce webpages also have applicable external vulnerability scanning obligations in the current SAQ A framework.

Management questions

- Does the customer leave our site for payment, or is the provider's payment form embedded in our page?
- Which scripts run on pages involved in checkout or booking?
- Who can change website code, plugins, tags or content-management components?
- Are external vulnerability scans required for our validation method?
- How quickly would we detect unauthorized changes to the payment experience?
- Is the website patched and maintained even when payment processing itself is outsourced?

6. Hospitality & Retail Payment Environments

Hospitality

- Front-desk terminals, PMS integrations and reservation/booking systems.
- Restaurant, bar, spa, golf and other property POS systems.
- Telephone reservations and virtual-terminal use.
- Remote support by PMS, POS and payment vendors.
- Multiple properties connected through shared networks or management systems.
- Legacy interfaces that pass payment data between otherwise separate systems.

Retail

- Integrated POS and back-office systems.
- Standalone terminals sharing networks with business devices.
- Inventory, accounting and e-commerce integrations.
- Remote vendor access and unattended support tools.
- Store-to-head-office connectivity and centralized administration.
- Temporary devices, seasonal locations and mobile payment acceptance.

Segmentation must be real

Putting a payment terminal on a different Wi-Fi name is not automatically effective segmentation. The controls must actually restrict communication and be tested where segmentation is relied upon to reduce PCI DSS scope.

7. Legacy Systems & Practical Risk Reduction

Businesses often depend on older POS, PMS, accounting or operational systems that cannot be replaced immediately. PCI DSS does not create a blanket permission to ignore unsupported technology, but neither should modernization be approached without considering business continuity.

A practical sequence

- Identify exactly why the legacy system is in PCI DSS scope.
- Determine whether payment data can be removed from the system or replaced with tokens.
- Restrict connectivity and administrative paths.
- Segment the system from unrelated business networks.
- Control and monitor remote vendor access.
- Document patching limitations and available mitigations.
- Maintain tested recovery options and spare/restore capability where appropriate.
- Develop a realistic migration plan with business ownership and dates.

Compensating controls are not shortcuts

PCI SSC provides formal guidance for compensating controls and the customized approach. These mechanisms require documented justification and evidence; they should not be used simply because a normal requirement is inconvenient.

8. Third-Party Service Providers

Payment processors, gateways, managed IT providers, hosting companies, cloud providers and software vendors can all affect payment security. Outsourcing a function changes the control model; it does not automatically eliminate the merchant's responsibility to understand the service.

- Maintain an inventory of service providers that store, process, transmit or can affect account-data security.
- Confirm the provider's PCI DSS status using recognized evidence, not an unofficial 'PCI certificate.'
- Understand which PCI DSS responsibilities belong to the provider and which remain with the merchant.
- Document incident-notification and escalation obligations.
- Review remote access, privileged access and subcontractors.
- Reassess the relationship when services or integrations change.

Recognized evidence

PCI SSC states that official PCI SSC reporting forms - such as ROC, AOC and SAQ documentation - are the recognized forms for validating PCI DSS compliance. A generic certificate is not a substitute.

9. Incident Response & Evidence

A payment-data incident is a poor time to discover that no one knows which systems process cards, who the processor contact is or where logs are retained. Incident readiness should be designed before compromise occurs.

- Define who has authority to declare and manage a payment-security incident.
- Maintain processor, acquirer, insurer, legal and technical escalation contacts.
- Preserve logs and evidence; do not casually wipe or rebuild affected systems before appropriate investigation.
- Know how payment processing can continue safely if a system must be isolated.
- Document third-party notification obligations.
- Conduct periodic incident-response exercises appropriate to the business.

10. PCI DSS Management Readiness Checklist

☐ We know our acquiring bank / payment processor and who accepts our PCI DSS validation.
☐ We know our merchant level for each relevant payment brand/program.
☐ We have confirmed whether our validation is an SAQ, ROC or other acquirer-defined process.
☐ We have selected the SAQ based on eligibility criteria, not convenience.
☐ We have mapped every payment channel and system that can affect the cardholder data environment.
☐ We know whether any full PAN or sensitive authentication data is stored and why.
☐ We have reduced unnecessary storage and access to account data.
☐ We have documented network segmentation where it is used to reduce scope.
☐ We control administrative and vendor remote access.
☐ We use MFA where required and appropriate.
☐ We maintain secure configurations and patch applicable systems.
☐ We understand how unsupported or legacy systems are protected and when they will be replaced.
☐ We inventory third-party service providers and review their PCI DSS evidence.
☐ We know whether external ASV scans apply to our environment.
☐ We maintain security logging and monitoring appropriate to the environment.
☐ We test security controls rather than relying only on policy documents.
☐ We have an incident-response plan and current escalation contacts.
☐ We train personnel who handle payments or administer payment systems.
☐ We review the payment environment when websites, vendors, POS/PMS systems or integrations change.
☐ Management reviews PCI DSS readiness and unresolved risks at least annually.

11. Building a Practical PCI DSS Roadmap

DISCOVER Map payment channels, business processes, systems, people, vendors and current validation obligations.

ASSESS Determine scope, SAQ/ROC requirements, security gaps, legacy dependencies and evidence quality.

PLAN Prioritize scope reduction, control improvements and remediation according to risk and operational impact.

PROTECT Implement and document proportionate technical, operational and organizational controls.

EVOLVE Reassess after changes to payment technology, websites, vendors, locations, transaction volumes or PCI requirements.

Business First. Technology Second.

PCI DSS readiness should make the payment environment simpler, more understandable and more resilient. Good design can reduce both security risk and the amount of technology that must remain in PCI DSS scope.

How SSB Defence Can Help

SSB Defence helps organizations understand the technology and operational environment around payment processing, reduce unnecessary exposure and prepare practical remediation roadmaps.

- PCI DSS readiness and payment-environment discovery.
- Cardholder data flow and scope review.
- SAQ readiness support and evidence-gap review.
- Network segmentation and legacy-system risk assessment.
- Hospitality PMS/POS and retail payment-environment review.
- E-commerce and third-party dependency review.
- Business continuity and incident-response planning.
- Prioritized remediation roadmap.

Start with a conversation

Before buying another security product, understand the payment flow, the required validation method and which systems genuinely need to be in scope.

Sources & Further Reading

- PCI Security Standards Council - PCI DSS v4.0.1 and official Document Library (current standard and reporting templates).
- PCI Security Standards Council - FAQs on SAQ eligibility, compliance-accepting entities, ASV scanning and recognized validation evidence.
- Visa - Account Information Security / PCI compliance validation program (current merchant-level criteria).
- Mastercard - Security Rules and Procedures, Merchant Edition, 3 February 2026 (merchant levels and validation requirements).
- PCI Security Standards Council - Guidance for Compensating Controls and the Customized Approach, June 2026.

SSB DEFENCE

Business First. Technology Second.