FIRST UNDERWRITERS INSURANCE BROKERS
Independent Insurance Brokers & Risk Managers

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

PCI COMPLIANCE CHECKLIST

Small Business Essentials

Retail • Restaurants • E-Commerce • Professional Services • Healthcare

A Cyber Risk Management Tool from Your Independent Insurance Broker

If your business accepts credit cards, debit cards, or any form of electronic payment, you are required to comply with the Payment Card Industry Data Security Standard (PCI DSS). This applies to every business— from a single-register retail shop to a large e-commerce operation.

PCI DSS compliance is not optional. Non-compliance can result in fines of$5,000 to $100,000 per month from your acquiring bank, increased transaction fees, loss of the ability to accept card payments, and personal liability for any resulting data breach. Most small businesses
fall under SAQ (Self-Assessment Questionnaire) levels A, A-EP, or D, depending on how they process payments.

This checklist simplifies the 12 PCI DSS requirements into actionable items for small businesses. It is not a substitute for the formal SAQ, but
it will help you identify gaps and prepare for your annual compliance validation.

BUSINESS INFORMATION

Complete before beginning the compliance review.

Business Name: _____

Business Type (Retail / Restaurant / E-Commerce / Services): _____

Assessment Date: _____

Assessor Name & Title: _____

Payment Processor / Acquiring Bank: _____

POS System or Payment Platform: _____

SAQ Type (A / A-EP / B / C / D): _____

Approximate Annual Card Transactions: _____

NOTE: Not sure which SAQ applies to your business? Most small businesses using a hosted payment page (Stripe, Square, Shopify) qualify for SAQ A — the simplest level. If you process cards on your own systems, you likely need SAQ C or D. Your payment processor or acquiring bank can confirm your SAQ type.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

BUILD AND MAINTAIN A SECURE NETWORK (Req 1-2)

1 Install and Maintain Network Security Controls

Firewalls and routers are your first line of defense. They control what traffic enters and leaves your network.

☐ YES	☐ NO	☐ N/A	Business firewall (hardware or software) is installed and actively protecting the network
☐ YES	☐ NO	☐ N/A	Firewall configuration has been reviewed within the past 12 months
☐ YES	☐ NO	☐ N/A	Inbound traffic is restricted to only what is necessary for business operations
☐ YES	☐ NO	☐ N/A	Outbound traffic from the cardholder data environment is restricted and monitored
☐ YES	☐ NO	☐ N/A	Wi-Fi network used for payment processing is separate from guest and employee Wi-Fi
☐ YES	☐ NO	☐ N/A	Remote access to the network requires VPN with multi-factor authentication (MFA)
☐ YES	☐ NO	☐ N/A	Personal firewalls are enabled on all laptops and mobile devices that access card data

TIP: If you use a consumer-grade router from your internet provider, you likely do not have an adequate firewall. A business-grade firewall with intrusion detection is strongly recommended for any business processing card payments.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

2 Apply Secure Configurations to All System Components

Vendor-supplied defaults (passwords, settings, unnecessary services) are well-known to attackers and must be changed before any system is deployed.

YES	NO	N/A	
☐	☐	☐	Default passwords on ALL systems have been changed (routers, POS, printers, cameras)
☐	☐	☐	Default or unnecessary user accounts have been removed or disabled
☐	☐	☐	Unnecessary services, protocols, and features have been disabled on all systems
☐	☐	☐	System configuration standards are documented and applied consistently
☐	☐	☐	Wi-Fi access points use WPA2 or WPA3 encryption (never WEP) with a strong password
☐	☐	☐	Router admin interface is not accessible from the internet

PROTECT ACCOUNT DATA (Req 3-4)

3 Protect Stored Account Data

The best way to protect cardholder data is to not store it at all. If you must store it, strict controls are required.

YES	NO	N/A	
☐	☐	☐	Business does NOT store full credit card numbers after transaction authorization
☐	☐	☐	Business does NOT store CVV/CVC codes, PIN data, or full magnetic stripe data
☐	☐	☐	If card data must be stored, it is encrypted using strong cryptography (AES-256)
☐	☐	☐	A data retention policy defines what cardholder data is kept and for how long
☐	☐	☐	Stored cardholder data is purged when it exceeds the defined retention period

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

☐ YES	☐ NO	☐ N/A	Card numbers are masked when displayed (show only last four digits)
☐ YES	☐ NO	☐ N/A	Paper receipts, reports, or logs containing full card numbers are securely destroyed
☐ YES	☐ NO	☐ N/A	POS system does not store prohibited data (verify with your POS vendor in writing)

BROKER INSIGHT: Most small businesses should NOT store any cardholder data. If your POS system or e-commerce platform handles card processing through a third-party gateway (Square, Stripe, Clover, Toast), the card data never touches your systems — and your compliance burden is dramatically reduced.

4 Protect Cardholder Data During Transmission

Card data must be encrypted whenever it travels across any network — especially the internet.

☐ YES	☐ NO	☐ N/A	All payment transactions are transmitted using TLS 1.2 or higher (HTTPS only)
☐ YES	☐ NO	☐ N/A	E-commerce website uses a valid, current SSL/TLS certificate from a trusted CA
☐ YES	☐ NO	☐ N/A	Card data is never sent via email, text message, chat, or fax
☐ YES	☐ NO	☐ N/A	Wireless networks transmitting card data use strong encryption (WPA2/WPA3)
☐ YES	☐ NO	☐ N/A	Payment terminal connections to the processor are encrypted end-to-end

IMPORTANT: If your e-commerce site collects card numbers directly on your web page (rather than redirecting to a hosted payment page), you are subject to the most rigorous SAQ D requirements. Switching to a hosted payment page (Stripe Checkout, PayPal) can dramatically simplify your PCI compliance.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM (Req 5-6)

5 Protect All Systems Against Malware

Anti-malware software must be deployed on all systems commonly affected by malware, including workstations, POS terminals, and servers.

YES	NO	N/A	
☐	☐	☐	Antivirus or endpoint protection (EDR) is installed on ALL computers and POS systems
☐	☐	☐	Anti-malware software is actively running and cannot be disabled by users
☐	☐	☐	Virus definitions are updated automatically (daily at minimum)
☐	☐	☐	Full system scans are performed on a regular schedule (weekly recommended)
☐	☐	☐	Anti-malware logs are retained and reviewed periodically

6 Develop and Maintain Secure Systems and Software

All systems must be kept up to date with security patches to protect against known vulnerabilities.

YES	NO	N/A	
☐	☐	☐	Operating systems on all computers receive automatic security updates
☐	☐	☐	Critical security patches are installed within 30 days of release
☐	☐	☐	POS software and firmware are updated to the latest version provided by the vendor
☐	☐	☐	Web applications (e-commerce) are protected by a web application firewall (WAF)
☐	☐	☐	Third-party software (browsers, plugins, Java) is kept current or removed
☐	☐	☐	End-of-life software (no longer receiving security updates) has been replaced

Notes / Corrective Actions Needed:

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

> **RISK FACTOR:** Many small business POS breaches exploit outdated software. If your POS vendor is no longer providing security updates, that system is a critical vulnerability. Replace end-of-life POS systems before your next compliance validation.

IMPLEMENT STRONG ACCESS CONTROL (Req 7-9)

7 Restrict Access to Cardholder Data by Business Need

Access to cardholder data and payment systems should be limited to only those employees whose job requires it.

YES	NO	N/A	
☐	☐	☐	Access to payment systems is restricted to only employees who need it for their role
☐	☐	☐	Employee access levels are documented and reviewed at least annually
☐	☐	☐	Access is revoked immediately when an employee leaves or changes roles
☐	☐	☐	POS system login credentials are unique to each employee (no shared logins)
☐	☐	☐	Administrative access to payment systems is limited to designated managers or IT

8 Identify Users and Authenticate Access

Every person with access to payment systems must have a unique ID. Shared accounts make it impossible to trace actions to a specific individual.

YES	NO	N/A	
☐	☐	☐	Each employee has a unique user ID for all payment and business systems
☐	☐	☐	No shared, group, or generic accounts are used to access payment systems
☐	☐	☐	Passwords are at least 12 characters with a mix of letters, numbers, and symbols
☐	☐	☐	Multi-factor authentication (MFA) is used for all remote access to payment systems
☐	☐	☐	User sessions time out and require re-authentication after 15 minutes of inactivity

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

9 Restrict Physical Access to Cardholder Data

Physical security protects payment terminals, servers, and paper records from tampering, theft, or unauthorized access.

YES	NO	N/A	
☐	☐	☐	Payment terminals (POS devices, card readers) are in view of employees at all times
☐	☐	☐	Payment terminals are inspected regularly for signs of tampering or skimming devices
☐	☐	☐	Employees are trained to recognize and report signs of terminal tampering
☐	☐	☐	Server rooms or network closets containing payment infrastructure are locked
☐	☐	☐	Visitor access to areas with payment systems is logged and escorted
☐	☐	☐	Paper records containing cardholder data are stored in locked locations
☐	☐	☐	Paper records containing cardholder data are cross-cut shredded when no longer needed
☐	☐	☐	Media (hard drives, USB drives) containing card data are physically destroyed when retired

RISK FACTOR: Terminal tampering and skimming are among the most common PCI breaches for brick-and-mortar businesses. Train employees to inspect terminals daily: check for loose components, extra wiring, overlay devices on the card slot or PIN pad, and anything that looks different from normal.

Notes / Corrective Actions Needed:

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

REGULARLY MONITOR AND TEST NETWORKS (Req 10-11)

10 Log and Monitor All Access to System Components

Logging creates a trail of who did what, when, and where. Without logs, you cannot detect a breach or prove what happened during an incident.

☐ YES	☐ NO	☐ N/A	Logging is enabled on all systems that store, process, or transmit cardholder data
☐ YES	☐ NO	☐ N/A	Logs capture user access, login attempts (successful and failed), and admin actions
☐ YES	☐ NO	☐ N/A	System clocks are synchronized using NTP to ensure accurate timestamps
☐ YES	☐ NO	☐ N/A	Logs are retained for at least 12 months (with 3 months immediately accessible)
☐ YES	☐ NO	☐ N/A	Logs are reviewed regularly for suspicious activity (daily review recommended)
☐ YES	☐ NO	☐ N/A	Log data is protected from unauthorized modification or deletion
☐ YES	☐ NO	☐ N/A	Automated alerts are configured for critical security events

TIP: For small businesses, log review does not require a dedicated SIEM. Many managed IT providers offer log monitoring as part of their service. At minimum, enable logging on your firewall, POS system, and any server handling payment data, and review weekly for failed logins or unusual access patterns.

Notes / Corrective Actions Needed:

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

11 Test Security of Systems and Networks Regularly

Regular testing verifies that your security controls are working as intended and identifies new vulnerabilities before attackers find them.

YES	NO	N/A	
☐	☐	☐	Quarterly external vulnerability scans are performed by an Approved Scanning Vendor (ASV)
☐	☐	☐	Internal vulnerability scans are performed at least quarterly
☐	☐	☐	Vulnerability scans are repeated after any significant network or system change
☐	☐	☐	Wireless access points are scanned quarterly to detect unauthorized devices
☐	☐	☐	Penetration testing is performed at least annually (if required by your SAQ level)
☐	☐	☐	Intrusion detection or intrusion prevention systems (IDS/IPS) are in place and monitored
☐	☐	☐	File integrity monitoring (FIM) alerts on unauthorized changes to critical system files

PCI REQUIREMENT: ASV scans are required quarterly for all businesses that process, store, or transmit cardholder data. Your payment processor can provide a list of approved scanning vendors. Many offer affordable small-business plans starting at $100-$300 per quarter.

BROKER INSIGHT: Penetration testing and ASV scan results are increasingly requested by cyber insurance carriers as part of the underwriting process. Passing results can positively impact your premium, while gaps may trigger exclusions.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

MAINTAIN AN INFORMATION SECURITY POLICY (Req 12)

12 Support Information Security with Policies and Programs

A written security policy establishes the rules, responsibilities, and procedures for protecting cardholder data across your entire organization.

YES	NO	N/A	
☐	☐	☐	Written information security policy exists and has been reviewed in the past 12 months
☐	☐	☐	Security policy addresses all 12 PCI DSS requirements
☐	☐	☐	Acceptable use policies exist for employee-facing technologies (internet, email, devices)
☐	☐	☐	All employees receive security awareness training upon hire and at least annually
☐	☐	☐	Employees acknowledge the security policy in writing (signature or electronic)
☐	☐	☐	An incident response plan exists for responding to a suspected card data breach
☐	☐	☐	Incident response plan includes notification procedures for your payment processor
☐	☐	☐	Third-party service providers with access to card data are identified and monitored
☐	☐	☐	Service provider contracts include acknowledgment of PCI DSS responsibilities
☐	☐	☐	Risk assessment is performed at least annually to identify threats and vulnerabilities

IMPORTANT: Your incident response plan should include your cyber insurance carrier's 24/7 breach hotline, your broker's contact information, and the steps to preserve evidence. A PCI breach triggers notification obligations to your acquiring bank and potentially to affected cardholders.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

ANNUAL COMPLIANCE CALENDAR

PCI compliance is not a one-time event. Use this calendar to track your recurring obligations throughout the year.

Frequency	Task
Quarterly	External vulnerability scan by ASV
Quarterly	Internal vulnerability scan
Quarterly	Wireless access point scan for rogue devices
Quarterly	Review firewall and router rule sets
Annually	Complete and submit Self-Assessment Questionnaire (SAQ)
Annually	Penetration test (if required by SAQ level)
Annually	Review and update information security policy
Annually	Conduct employee security awareness training
Annually	Review user access privileges and remove unnecessary access
Annually	Perform formal risk assessment
Annually	Verify PCI compliance of all third-party service providers
Daily	Review security logs for suspicious activity
Daily	Inspect payment terminals for tampering (retail)
Ongoing	Apply critical security patches within 30 days of release
Ongoing	Revoke access immediately for terminated employees

PCI REQUIREMENT: Set calendar reminders for quarterly ASV scans and your annual SAQ submission deadline. Missed scans can result in non-compliance fines from your acquiring bank — even if your security controls are otherwise in place.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

IMPORTANT: PCI compliance and cyber insurance work together. A PCI breach without cyber insurance can be catastrophic for a small business — forensic investigation alone can cost $20,000-$100,000, plus notification costs, card brand fines, and potential lawsuits. Your cyber policy can cover these costs, but only if you have documented compliance efforts in place.

Notes / Corrective Actions Needed:

ASSESSMENT SIGN-OFF

By signing below, the assessor and business owner confirm that this checklist was completed in good faith and the results accurately reflect the current PCI compliance posture of the business.

Assessor Signature: _____ **Date:** _____

Business Owner Signature: _____ **Date:** _____

Does Your Cyber Policy Cover a PCI Breach?

As independent brokers, we review your PCI compliance posture, ensure your cyber policy includes PCI fine and penalty coverage, and help you build a defense-in-depth strategy for card data security.

Call (425) 242-5357 | Visit www.firstunderwriters.com

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This checklist is for educational purposes only. It does not constitute legal advice or guarantee PCI compliance. Consult a Qualified Security Assessor (QSA).