BUZZ

PCI-DSS COMPLIANCE CHECKLIST

A complete guide by BUZZ to meet PCI Security Standards

Table of Contents

Introduction

Welcome to our PCI DSS Compliance Checklist, a streamlined resource designed to guide you through the essentials of Payment Card Industry Data Security Standard compliance. This checklist will help you determine if PCI DSS applies to your business, understand your compliance level based on transaction volume, and navigate through the various Self-Assessment Questionnaires (SAQs).

Expect clear, actionable questions with brief descriptions and examples of acceptable evidence, making it easier for you to assess and enhance your organization's data security posture. Whether you're new to PCI DSS or looking to refine your existing compliance strategies, this checklist is your starting point towards a secure and compliant payment environment.

Developed by major credit card companies, including Visa, MasterCard, American Express, and Discover, PCI DSS aims to safeguard cardholder data and maintain the integrity of payment systems. Organizations that handle, process, or store credit card information are required to comply with these standards to mitigate the risk of data breaches and unauthorized access. PCI DSS outlines specific security measures, such as encryption, access controls, and regular system monitoring, to create a secure environment for handling payment card data. Achieving and maintaining PCI DSS Compliance is crucial for businesses to not only protect customer information but also to maintain trust and credibility within the payment card industry. Non-compliance can result in financial penalties, loss of customer trust, and potential legal consequences.

BUZZ PCI DSS Compliance Services

Explore our PCI Compliance Consulting Services - expertly crafted to secure your cardholder data and ensure regulatory adherence. Our specialized team excels in delivering comprehensive, PCI-focused solutions accessible through our dedicated compliance service platform making us your trusted PCI DSS service provider.

BUZZ PCI DSS services can help your organization in meeting up PCI compliance security standards as follows:

PCI DSS Compliance Gap Analysis: A Payment Card Industry Data Security Standard (PCI DSS) Compliance Gap Analysis is an assessment that helps your organization to identify areas where they fall short to meet the requirements of the PCI DSS. BUZZ PCI DSS identifies these gaps by analyzing the Cardholder Data Environment, reviewing of PCI-DSS Control Objectives, doing assessment of Data Encryption & Protection, providing PCI-DSS Compliance reports.

PCI-DSS Security Architecture Review: PCI DSS Security Architecture Review is a comprehensive assessment of the security measures and controls in place within an organization to protect credit card data. PCI DSS services by BUZZ helps your organization strengthen your architecture to align with PCI-DSS standards by, continuous evaluation of Network Security, reviewing your Access Control Measures as per the set PCI Secure Software standards, reviewing the Data Flow and Storage, ensuring the security policies are in alignment with PCI-DSS.

PCI-DSS Encryption and Data Protection Services: PCI-DSS (Payment Card Industry Data Security Standard) Encryption and Data Protection Services play a crucial role in safeguarding sensitive information associated with credit and debit card transactions. BUZZ helps organization enhance its data protection as per PCI-DSS requirements by implementing PCI-DSS Compliant Encryption, Data Masking and Tokenization Solutions, provide strategies for Secure Data Transmission, follow key Management Best Practices to get PCI DSS Compliance

PCI-DSS Intrusion Detection and Response Planning: The PCI-DSS framework mandates stringent security measures to protect payment card data, and intrusion detection plays a pivotal role in identifying and mitigating potential threats. BUZZ experts help your organization by developing PCI-DSS compliant security incident responses, Intrusion Detection, Incident Response Planning for PCI Compliance, reviewing PCI-DSS Security Logging regularly and PCI-DSS Threat Intelligence Integration.

PCI-DSS Certification Assistance: Is a vital service provided by BUZZ that supports organizations in achieving and maintaining compliance with the rigorous security standards set by the payment card industry. Experts at BUZZ guide you through the PCI-DSS certification process which includes activities like - Audit Preparation, Assistance with PCI-DSS Documentation, Post-Audit Compliance Support, and regular PCI-DSS Compliance Health Checks.

Regular PCI-DSS Compliance Audits and Penetration Testing: Regular PCI-DSS compliance audits and penetration testing contribute to a robust security posture, safeguarding against data breaches and maintaining the trust of customers and stakeholders in the handling of payment card information. BUZZ helps you maintain continuous PCI-DSS compliance by scheduling audits, conducting PCI Penetration Test, PCI Compliance Test, vulnerability assessments for ongoing PCI-DSS, and provide improved strategies for PCI DSS compliance.

Applicability Evaluation

Does PCI DSS Apply to Your Organization?

If your organization processes, stores, or transmits cardholder data, PCI DSS compliance is mandatory. This includes any handling of credit card information, whether in digital or physical format.

Understanding Your Business's PCI DSS Level

Identify your business's PCI DSS level based on transaction volume and data handling methods.

Level 1: Over 6 million transactions annually.

Level 2: 1 to 6 million transactions annually.

Level 3: 20,000 to 1 million e-commerce transactions annually.

Level 4: Fewer than 20,000 e-commerce transactions, or up to 1 million annually.

Determining the Right Self-Assessment Questionnaires (SAQs)

PCI DSS compliance can also be assessed through various Self-Assessment Questionnaires (SAQs), depending on your business and how you handle cardholder data.

SAQ A: For merchants who outsource all cardholder data functions and do not electronically store, process, or transmit any cardholder data.

SAQ B: For merchants using only standalone, dial-out terminals and do not electronically store cardholder data.

SAQ C: For merchants with payment application systems connected to the Internet, without electronic cardholder data storage.

SAQ D: For all other merchants and service providers not covered by the above, and those who store, process, or transmit cardholder data.

PCI DSS Readiness Checklist

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

	Questions	Brief Description
☐	How are connections to cardholder data environments managed?	Identification, justification, and documentation of all network connections to cardholder data environments.
☐	Are firewall and router configurations secure and regularly reviewed?	Secure configuration and routine review of firewalls and routers to prevent unauthorized access.
☐	Is there a process for managing changes to network and firewall/router configurations?	Formal procedure for testing, approving, & documenting changes in network and firewall/router configurations.
☐	How are network and personal devices secured against unauthorized external access?	Protection measures for network and personal devices against unauthorized external access, including personal firewalls.
☐	Are controls in place for traffic management and network monitoring?	Strict control of network traffic to allow only necessary access, with active monitoring for security.

Acceptable Evidence

- Network diagrams, firewall and router configuration settings, compliance reports, change management records, access control lists.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

	Questions	Brief Description
☐	Are vendor defaults and unnecessary default accounts changed or removed?	Changing vendor-supplied defaults and disabling/removing unnecessary default accounts for security.
☐	Is strong cryptography used for data transmission, especially over public networks?	Utilizing robust encryption and secure protocols for cardholder data during transmission.
☐	Are shared or generic accounts and passwords prohibited?	Enforcing individualized credentials to maintain security and accountability.
☐	Are access controls to cardholder data based on a need-to-know basis?	Implementing need-to-know access control measures aligned with job roles.
☐	Is there a process for malware protection & regular system updates?	Maintaining systems against malware and ensuring regular updates with security patches

Acceptable Evidence

- Configuration checklists, encryption policy documents, security policy documents, access control policies, antivirus policies.

Requirement 3: Protect Stored Cardholder Data

	Questions	Brief Description
☐	Is cardholder data storage minimized and managed securely?	Limiting cardholder data storage to business needs & managing it with documented handling & disposal procedures.
☐	Are PANs unreadable in storage and masked when displayed?	Rendering PANs unreadable in storage and masking them to show only the last four digits when displayed.
☐	Is access to stored cardholder data restricted and authenticated?	Restricting access to stored cardholder data to authorized personnel with business need, and implementing robust authentication processes.
☐	Are cryptographic keys for encrypting cardholder data securely managed?	Securely managing cryptographic keys for cardholder data encryption, including their storage, access, and lifecycle.
☐	Is there a tested incident response plan for cardholder data breaches?	Maintaining a tested incident response plan for cardholder data breaches and regularly testing security systems and processes

Acceptable Evidence

- Data retention policies, encryption standards, access control lists, key management procedures, incident response plans.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

	Questions	Brief Description
☐	Is strong cryptography used for data transmission over public networks?	Utilizing strong encryption and secure protocols like SSL/TLS, SSH, or IPSEC for transmitting cardholder data over open networks.
☐	Are trusted keys/certificates used with appropriate encryption strength?	Ensuring the use of trusted encryption keys and certificates with adequate encryption strength.
☐	Are security protocols in place to minimize data exposure during transmission?	Implementing protocols to reduce the risk of cardholder data exposure during transmission, especially over public networks.
☐	Is cardholder data transmission via end-user messaging technologies prohibited?	Banning the transmission of cardholder data through end-user messaging like email, instant messaging, or SMS.
☐	Do wireless networks follow best practices for encryption and authentication?	Adhering to industry best practices for encryption and authentication in wireless networks transmitting cardholder data.

Acceptable Evidence

- Network configuration documents, encryption protocol settings, certificate authority documentation, communication policies, wireless network configuration settings.

Requirement 5: Protect All Systems Against Malware and Regularly Update Antivirus Software or Programs

	Questions	Brief Description
☐	Is antivirus software deployed and active on all relevant systems?	Ensuring deployment and active running of antivirus software on systems, especially those handling cardholder data.
☐	Are antivirus updates and scans performed regularly?	Keeping antivirus software up-to-date with the latest malware signatures and performing regular system scans.
☐	Is there a process for managing antivirus software and audit logs?	Verifying that antivirus software is current and active, with a process for generating and retaining audit logs as per PCI-DSS.
☐	Are there procedures for responding to antivirus alerts and assessing effectiveness?	Implementing response procedures for antivirus alerts & regularly assessing the effectiveness of antivirus mechanisms.
☐	Is there user training on antivirus software maintenance and malware risks?	Providing training to users on the importance of antivirus maintenance and awareness of malware risks.

Acceptable Evidence

- Antivirus deployment records, update logs, compliance reports, incident response procedures, training materials.

Requirement 6: Develop and Maintain Secure Systems and Applications

	Questions	Brief Description
☐	Are systems and software updated with security patches promptly?	Timely updates of all system components and software with the latest security patches, and a process for identifying and ranking new vulnerabilities.
☐	Are secure coding practices established and followed?	Adherence to secure coding guidelines for both internal development & third-party applications, integrating security throughout the development lifecycle.
☐	Are change control procedures and web application security measures in place?	Management of system and software changes through change control procedures, and securing web applications against known attacks.
☐	Is there a comprehensive vulnerability management program?	Implementation of an effective vulnerability management program for all critical systems and applications, with ongoing security testing.
☐	Are custom code reviews & developer security training conducted?	Reviewing custom code for vulnerabilities before release & providing security training & awareness programs to developers.

Acceptable Evidence

- Patch management policies, secure coding policies, development lifecycle documentation, vulnerability management policies, code review policies.

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

	Questions	Brief Description
☐	Is access to data and systems job-based and are privileged rights minimized?	Access to system components and cardholder data is based on job roles, with minimal necessary privileges for users with special access.
☐	Are access control systems robust and unique IDs assigned for data access?	Strong access control systems in place to limit cardholder data access, with unique IDs for each user accessing this data.
☐	Is access granted based on job function and promptly revoked if needed?	Access rights are aligned with job functions, and there's a swift process to revoke access for terminated users.
☐	Are access controls and user rights regularly reviewed and well-understood?	Ongoing review of access controls & user rights for appropriateness, & comprehensive user training on access policies.

Acceptable Evidence

- Access control policies, user access lists, privileged account audit reports, job descriptions, review records.

Requirement 8: Identify and Authenticate Access to System Components

	Questions	Brief Description
☐	Are unique IDs assigned for system/data access and user ID management robust?	Assigning unique IDs before system or data access and managing user IDs and credentials comprehensively.
☐	Are strong password policies and multifactor authentication in place?	Implementing robust password policies with regular updates & using multifactor authentication for remote access.
☐	Are passwords encrypted and initial/reset passwords secure?	Encrypting passwords during transmission and storage, and ensuring secure, unique initial and reset passwords.
☐	Is access promptly disabled for terminated or inactive users?	Swiftly disabling access for terminated users, deactivating inactive IDs, and locking out IDs after multiple failed
☐	Are remote access sessions securely monitored and controlled?	Ensuring secure and authorized access for all remote sessions to the network and cardholder data environment.

Acceptable Evidence

- User ID assignment policies, password policies, encryption policies, termination procedures, remote access monitoring logs.

Requirement 9: Restrict Physical Access to Cardholder Data

	Questions	Brief Description
☐	Are facility entry controls and access restrictions for cardholder data in place?	Implementing measures to control and monitor physical access to systems with cardholder data for personnel and visitors.
☐	Is media containing cardholder data physically secured and managed?	Securing all media with cardholder data and managing its distribution, storage, retrieval, and destruction.
☐	Are access control systems & visitor authentication effectively used?	Using access control systems for systems with cardholder data and authenticating visitors accessing these areas.
☐	Is there a process for incident response & monitoring in sensitive areas?	Managing security incidents in areas with cardholder data access & monitoring these areas, e.g., with video cameras.
☐	Are there secure disposal processes for cardholder data and physical media?	Implementing secure disposal methods for cardholder data & physical media to prevent unauthorized access or recovery.

Acceptable Evidence

- Entry control mechanisms, media storage logs, access control system records, incident response procedures, data destruction policies.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

	Questions	Brief Description
☐	Are accesses to cardholder data and privileged actions logged?	Logging all individual accesses to cardholder data and actions by users with root/admin privileges, linking access to specific users.
☐	Are audit logs retained and reviewed for anomalies?	Keeping audit logs for at least one year, with three months readily available, and regularly reviewing them for unusual activities.
☐	Are audit trails secured and automated for monitoring access?	Securing audit trails against unauthorized changes and implementing automated systems for tracking access to network resources and data.
☐	Is there a process for detecting security system failures and unauthorized modifications?	Promptly detecting & reporting security control failures, using file integrity monitoring, and responding to incidents identified by monitoring systems.

Acceptable Evidence

- Access logs, logging policies, log retention policies, audit trail protection mechanisms, incident detection procedures.

Requirement 11: Regularly Test Security Systems and Processes

	Questions	Brief Description
☐	Are regular vulnerability scans and annual penetration tests conducted?	Performing internal & external network vulnerability scans quarterly and after significant changes, plus annual and post-change penetration testing.
☐	Are intrusion detection/prevention systems monitoring network traffic?	Using intrusion detection or prevention systems at the cardholder data environment perimeter and for overall network traffic monitoring.
☐	Is there a process for updating security systems and using file integrity monitoring?	Regularly updating security systems with the latest patches and using file integrity monitoring tools for unauthorized modifications.
☐	Are wireless access points tested and security controls regularly assessed?	Regularly testing wireless access points for unauthorized access and assessing the effectiveness of security controls and systems.

Acceptable Evidence

- Scan schedules, intrusion detection system configurations, patch management policies, wireless network scans, security testing schedules.

Requirement 12: Maintain a Policy that Addresses Information Security for All Personnel

	Questions	Brief Description
☐	Is a comprehensive security policy established and disseminated?	Developing, maintaining, and sharing a formal security policy, including specific information security guidelines for all personnel.
☐	Are employees and contractors trained in data security awareness?	Providing regular security awareness training to employees and contractors about protecting cardholder data and their security responsibilities.
☐	Is there an annual risk assessment and tested incident response plan?	Conducting annual risk assessments for the cardholder data environment and maintaining tested incident response procedures for breaches.
☐	Are security policies regularly reviewed and background checks conducted?	Ensuring annual reviews and updates of security policies and procedures, and performing background checks on personnel with data access.

Acceptable Evidence

- Security policy documents, training materials, risk assessment reports, policy review records, HR records.

Conclusion and Next Steps

This guide, along with the PCI DSS Readiness Checklist, provides a comprehensive framework to evaluate your organization's compliance posture. The checklist covers a wide range of questions that cut across all aspects of PCI DSS requirements, ensuring a thorough assessment.

After determining your applicability, PCI DSS level, and the appropriate SAQ category, use the checklist to gauge your current compliance status. Regular reviews and updates to your security measures are crucial for maintaining compliance.

If gaps in compliance are identified, address them promptly. For detailed assessments and tailored advice, consider consulting with a PCI DSS compliance expert.

About BUZZ

At BUZZ, we focus on making cybersecurity manageable and effective for Small and Medium-sized Businesses (SMBs). Our **'Assess-Comply-Secure'** strategy equips businesses to face cybersecurity challenges confidently.

We recognize that every business has unique cybersecurity needs. Our team specialises in providing **personalised solutions,** from risk assessments to security implementations, ensuring that your specific concerns are addressed. Our goal is to not just deliver services but to build a secure digital environment for your business.

BUZZ stands out for offering **high-quality** cybersecurity services at a **competitive price.** We believe in making excellent cybersecurity accessible to all businesses, regardless of size. Our commitment is to provide comprehensive, cost-effective solutions that prioritise your digital protection.

Choose BUZZ for dedicated cybersecurity support that puts your business first.
To learn more about BUZZ and avail our services, visit our website:
www.buzzhq.io