| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 1.1 | Processes and mechanisms for installing and maintaining network security controls are defined and understood. | | | | | | | |
| 1.1.1 | | x | | | | | x | x |
| 1.1.2 | | | | | | | x | x |
| 1.2 | Network security controls (NSCs) are configured and maintained. | | | | | | | |
| 1.2.1 | | x | | | | | x | x |
| 1.2.2 | | x | | | | | x | x |
| 1.2.3 | | x | | x | | | x | x |
| 1.2.4 | | x | | | | | x | x |
| 1.2.5 | | x | | x | | | x | x |
| 1.2.6 | | x | | x | | | x | x |
| 1.2.7 | | x | | | | | x | x |
| 1.2.8 | | x | | | | | x | x |
| 1.3 | Network access to and from the cardholder data environment is restricted. | | | | | | | |
| 1.3.1 | | x | | x | x | x | x | x |
| 1.3.2 | | x | | x | x | x | x | x |
| 1.3.3 | | x | | x | x | x | x | x |
| 1.4 | Network connections between trusted and untrusted networks are controlled. | | | | | | | |
| 1.4.1 | | x | | | | | x | x |
| 1.4.2 | | x | | | | | x | x |
| 1.4.3 | | x | | x | | | x | x |
| 1.4.4 | | x | | | | | x | x |
| 1.4.5 | | x | | | | | x | x |
| 1.5 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. | | | | | | | |
| 1.5.1 | | x | | | | x | x | x |
| 2.1 | Processes and mechanisms for applying secure configurations to all system components are defined and understood. | | | | | | | |
| 2.1.1 | | x | | | x | x | x | x |
| 2.1.2 | | | | | | | x | x |
| 2.2 | System components are configured and managed securely. | | | | | | | |
| 2.2.1 | | x | | | x | | x | x |
| 2.2.2 | x | x | | x | x | x | x | x |
| 2.2.3 | | x | | | x | | x | x |
| 2.2.4 | | x | | | x | x | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 2.2.5 | | x | | | x | x | x | x |
| 2.2.6 | | x | | | x | x | x | x |
| 2.2.7 | | x | | x | x | x | x | x |
| 2.3 | Wireless environments are configured and managed securely. | | | | | | | |
| 2.3.1 | | | | x | x | x | x | x |
| 2.3.2 | | | | x | x | x | x | x |
| 3.1 | Processes and mechanisms for protecting stored account data are defined and understood. | | | | | | | |
| 3.1.1 | x | x | x | x | x | x | x | x |
| 3.1.2 | | | | | | | x | x |
| 3.2 | Storage of account data is kept to a minimum. | | | | | | | |
| 3.2.1 | x | x | | | | | x | x |
| 3.3 | Sensitive authentication data (SAD) is not stored after authorization. | | | | | | | |
| 3.3.1 | | x | x | x | x | x | x | x |
| 3.3.1.1 | | | x | x | | | x | x |
| 3.3.1.2 | | x | x | x | x | x | x | x |
| 3.3.1.3 | | x | x | x | x | | x | x |
| 3.3.2 | | | | | | | x | x |
| 3.3.3 | | | | | | | | x |
| 3.4 | Access to displays of full PAN and ability to copy PAN is restricted. | | | | | | | |
| 3.4.1 | | | x | x | x | x | x | x |
| 3.4.2 | | | | | | | x | x |
| 3.5 | Primary account number (PAN) is secured wherever it is stored. | | | | | | | |
| 3.5.1 | | | | | | | x | x |
| 3.5.1.1 | | | | | | | x | x |
| 3.5.1.2 | | | | | | | x | x |
| 3.5.1.3 | | | | | | | x | x |
| 3.6 | Cryptographic keys used to protect stored account data are secured. | | | | | | | |
| 3.6.1 | | | | | | | x | x |
| 3.6.1.1 | | | | | | | | x |
| 3.6.1.2 | | | | | | | x | x |
| 3.6.1.3 | | | | | | | x | x |
| 3.6.1.4 | | | | | | | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| **3.7** | **Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.** | | | | | | | |
| **3.7.1** | | | | | | | x | x |
| **3.7.2** | | | | | | | x | x |
| **3.7.3** | | | | | | | x | x |
| **3.7.4** | | | | | | | x | x |
| **3.7.5** | | | | | | | x | x |
| **3.7.6** | | | | | | | x | x |
| **3.7.7** | | | | | | | x | x |
| **3.7.8** | | | | | | | x | x |
| **3.7.9** | | | | | | | | x |
| **4.1** | **Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.** | | | | | | | |
| **4.1.1** | | x | | | | | x | x |
| **4.1.2** | | | | | | | x | x |
| **4.2** | **PAN is protected with strong cryptography during transmission.** | | | | | | | |
| **4.2.1** | | x | | | x | | x | x |
| **4.2.1.1** | | | | | | | x | x |
| **4.2.1.2** | | | | | x | x | x | x |
| **4.2.2** | | x | | | x | | x | x |
| **5.1** | **Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.** | | | | | | | |
| **5.1.1** | | x | | | x | | x | x |
| **5.1.2** | | | | | | | x | x |
| **5.2** | **Malicious software (malware) is prevented, or detected and addressed.** | | | | | | | |
| **5.2.1** | | x | | | x | x | x | x |
| **5.2.2** | | x | | | x | x | x | x |
| **5.2.3** | | x | | | x | | x | x |
| **5.2.3.1** | | x | | | x | | x | x |
| **5.3** | **Anti-malware mechanisms and processes are active, maintained, and monitored.** | | | | | | | |
| **5.3.1** | | x | | | x | x | x | x |
| **5.3.2** | | x | | | x | x | x | x |
| **5.3.2.1** | | x | | | x | | x | x |
| **5.3.3** | | x | | | x | x | x | x |
| **5.3.4** | | x | | | x | x | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 5.3.5 | | x | | | x | x | x | x |
| 5.4 | Anti-phishing mechanisms protect users against phishing attacks. | | | | | | | |
| 5.4.1 | | x | | | x | x | x | x |
| 6.1 | Processes and mechanisms for developing and maintaining secure systems and software are defined and understood. | | | | | | | |
| 6.1.1 | | x | | | | | x | x |
| 6.1.2 | | | | | | | x | x |
| 6.2 | Bespoke and custom software are developed securely. | | | | | | | |
| 6.2.1 | | x | | | x | | x | x |
| 6.2.2 | | x | | | x | | x | x |
| 6.2.3 | | | | | | | x | x |
| 6.2.3.1 | | | | | x | | x | x |
| 6.2.4 | | x | | | x | | x | x |
| 6.3 | Security vulnerabilities are identified and addressed. | | | | | | | |
| 6.3.1 | x | x | | x | x | x | x | x |
| 6.3.2 | | x | | | | | x | x |
| 6.3.3 | x | x | | x | x | x | x | x |
| 6.4 | Public-facing web applications are protected against attacks. | | | | | | | |
| 6.4.1 | | x | | | | | x | x |
| 6.4.2 | | x | | | | | x | x |
| 6.4.3 | x | x | | | | | x | x |
| 6.5 | Changes to all system components are managed securely. | | | | | | | |
| 6.5.1 | | x | | | x | | x | x |
| 6.5.2 | | x | | | x | | x | x |
| 6.5.3 | | | | | | | x | x |
| 6.5.4 | | | | | | | x | x |
| 6.5.5 | | | | | | | x | x |
| 6.5.6 | | | | | | | x | x |
| 7.1 | Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. | | | | | | | |
| 7.1.1 | | | | | | | x | x |
| 7.1.2 | | | | | | | x | x |
| 7.2 | Access to system components and data is appropriately defined and assigned. | | | | | | | |
| 7.2.1 | | | | | | | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 7.2.2 | | x | x | x | x | x | x | x |
| 7.2.3 | | x | | | x | | x | x |
| 7.2.4 | | x | | | x | | x | x |
| 7.2.5 | | x | | | x | | x | x |
| 7.2.5.1 | | | | | | | x | x |
| 7.2.6 | | | | | | | x | x |
| 7.3 | Access to system components and data is managed via an access control system(s). | | | | | | | |
| 7.3.1 | | | | | | | x | x |
| 7.3.2 | | | | | | | x | x |
| 7.3.3 | | | | | | | x | x |
| 8.1 | Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. | | | | | | | |
| 8.1.1 | | x | | x | x | x | x | x |
| 8.1.2 | | | | | | | x | x |
| 8.2 | User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle. | | | | | | | |
| 8.2.1 | x | x | | | x | x | x | x |
| 8.2.2 | x | x | | x | x | x | x | x |
| 8.2.3 | | | | | | | | x |
| 8.2.4 | | x | | | x | x | x | x |
| 8.2.5 | x | x | | | x | x | x | x |
| 8.2.6 | | x | | | x | | x | x |
| 8.2.7 | | x | | x | x | | x | x |
| 8.2.8 | | x | | | x | | x | x |
| 8.3 | Strong authentication for users and administrators is established and managed. | | | | | | | |
| 8.3.1 | x | x | | | x | x | x | x |
| 8.3.2 | | x | | | x | | x | x |
| 8.3.3 | | x | | | x | | x | x |
| 8.3.4 | | x | | | x | | x | x |
| 8.3.5 | x | x | | | x | | x | x |
| 8.3.6 | x | x | | | x | x | x | x |
| 8.3.7 | x | x | | | x | | x | x |
| 8.3.8 | | x | | | x | | x | x |
| 8.3.9 | x | x | | | x | | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 8.3.10 | | | | | | | | x |
| 8.3.10.1 | | | | | | | | x |
| 8.3.11 | | x | | | | | x | x |
| 8.4 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. | | | | | | | |
| 8.4.1 | | x | | | x | x | x | x |
| 8.4.2 | | x | | | x | | x | x |
| 8.4.3 | | x | | x | x | | x | x |
| 8.5 | Multi-factor authentication (MFA) systems are configured to prevent misuse. | | | | | | | |
| 8.5.1 | | x | | | x | | x | x |
| 8.6 | Use of application and system accounts and associated authentication factors is strictly managed. | | | | | | | |
| 8.6.1 | | x | | | x | | x | x |
| 8.6.2 | | x | | | x | | x | x |
| 8.6.3 | | x | | | x | | x | x |
| 9.1 | Processes and mechanisms for restricting physical access to cardholder data are defined and understood. | | | | | | | |
| 9.1.1 | | | | x | x | x | x | x |
| 9.1.2 | | | | | | | x | x |
| 9.2 | Physical access controls manage entry into facilities and systems containing cardholder data. | | | | | | | |
| 9.2.1 | | x | | | x | x | x | x |
| 9.2.1.1 | | | | | x | | x | x |
| 9.2.2 | | | | x | x | | x | x |
| 9.2.3 | | | | | | | x | x |
| 9.2.4 | | | | | | | x | x |
| 9.3 | Physical access for personnel and visitors is authorized and managed. | | | | | | | |
| 9.3.1 | | | | | | | x | x |
| 9.3.1.1 | | | | | | | x | x |
| 9.3.2 | | | | | | | x | x |
| 9.3.3 | | | | | | | x | x |
| 9.3.4 | | | | | | | x | x |
| 9.4 | Media with cardholder data is securely stored, accessed, distributed, and destroyed. | | | | | | | |
| 9.4.1 | x | x | x | x | x | x | x | x |
| 9.4.1.1 | x | x | x | x | x | x | x | x |
| 9.4.1.2 | | | | | | | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 9.4.2 | x | x | x | x | x | x | x | x |
| 9.4.3 | x | x | x | x | x | x | x | x |
| 9.4.4 | x | x | x | x | x | x | x | x |
| 9.4.5 | | | | | | | x | x |
| 9.4.5.1 | | | | | | | x | x |
| 9.4.6 | x | x | x | x | x | x | x | x |
| 9.4.7 | | | | | | | x | x |
| 9.5 | Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. | | | | | | | |
| 9.5.1 | | | x | x | x | | x | x |
| 9.5.1.1 | | | x | x | x | | x | x |
| 9.5.1.2 | | | x | x | x | | x | x |
| 9.5.1.2.1 | | | | | | | x | x |
| 9.5.1.3 | | | x | x | x | | x | x |
| 10.1 | Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented. | | | | | | | |
| 10.1.1 | | | | | x | | x | x |
| 10.1.2 | | | | | | | x | x |
| 10.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. | | | | | | | |
| 10.2.1 | | x | | | | | x | x |
| 10.2.1.1 | | x | | | | | x | x |
| 10.2.1.2 | | x | | | x | | x | x |
| 10.2.1.3 | | x | | | | | x | x |
| 10.2.1.4 | | x | | | x | | x | x |
| 10.2.1.5 | | x | | | x | | x | x |
| 10.2.1.6 | | x | | | | | x | x |
| 10.2.1.7 | | x | | | | | x | x |
| 10.2.2 | | x | | | x | | x | x |
| 10.3 | Audit logs are protected from destruction and unauthorized modifications. | | | | | | | |
| 10.3.1 | | x | | | x | | x | x |
| 10.3.2 | | x | | | x | | x | x |
| 10.3.3 | | x | | | x | | x | x |
| 10.3.4 | | x | | | x | | x | x |
| 10.4 | Audit logs are reviewed to identify anomalies or suspicious activity. | | | | | | | |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 10.4.1 | | x | | | x | | x | x |
| 10.4.1.1 | | x | | | x | | x | x |
| 10.4.2 | | x | | | x | | x | x |
| 10.4.2.1 | | x | | | x | | x | x |
| 10.4.3 | | x | | | x | | x | x |
| 10.5 | Audit log history is retained and available for analysis. | | | | | | | |
| 10.5.1 | | x | | | x | | x | x |
| 10.6 | Time-synchronization mechanisms support consistent time settings across all systems. | | | | | | | |
| 10.6.1 | | x | | | x | | x | x |
| 10.6.2 | | x | | | x | | x | x |
| 10.6.3 | | x | | | x | | x | x |
| 10.7 | Failures of critical security control systems are detected, reported, and responded to promptly. | | | | | | | |
| 10.7.1 | | | | | | | | x |
| 10.7.2 | | | | | | | x | x |
| 10.7.3 | | | | | | | x | x |
| 11.1 | Processes and mechanisms for regularly testing security of systems and networks are defined and understood. | | | | | | | |
| 11.1.1 | | | | | | | x | x |
| 11.1.2 | | | | | | | x | x |
| 11.2 | Wireless access points are identified and monitored, and unauthorized wireless access points are addressed. | | | | | | | |
| 11.2.1 | | | | | x | | x | x |
| 11.2.2 | | | | | x | | x | x |
| 11.3 | External and internal vulnerabilities are regularly identified, prioritized, and addressed. | | | | | | | |
| 11.3.1 | | | | | x | | x | x |
| 11.3.1.1 | | | | | | | x | x |
| 11.3.1.2 | | | | | | | x | x |
| 11.3.1.3 | | | | | x | | x | x |
| 11.3.2 | x | x | | x | x | | x | x |
| 11.3.2.1 | x | x | | | x | | x | x |
| 11.4 | External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. | | | | | | | |
| 11.4.1 | | x | | | | | x | x |
| 11.4.2 | | | | | | | x | x |
| 11.4.3 | | x | | | | | x | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 11.4.4 | | x | | | | | x | x |
| 11.4.5 | | x | | x | x | | x | x |
| 11.4.6 | | | | | | | | x |
| 11.4.7 | | | | | | | | x |
| 11.5 | Network intrusions and unexpected file changes are detected and responded to. | | | | | | | |
| 11.5.1 | | x | | | | | x | x |
| 11.5.1.1 | | | | | | | | x |
| 11.5.2 | | x | | | x | | x | x |
| 11.6 | Unauthorized changes on payment pages are detected and responded to. | | | | | | | |
| 11.6.1 | x | x | | | | | x | x |
| 12.1 | A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current. | | | | | | | |
| 12.1.1 | | x | x | x | x | x | x | x |
| 12.1.2 | | x | x | x | x | x | x | x |
| 12.1.3 | | x | x | x | x | | x | x |
| 12.1.4 | | x | | | | | x | x |
| 12.2 | Acceptable use policies for end-user technologies are defined and implemented. | | | | | | | |
| 12.2.1 | | | | | x | | x | x |
| 12.3 | Risks to the cardholder data environment are formally identified, evaluated, and managed. | | | | | | | |
| 12.3.1 | | x | | | x | | x | x |
| 12.3.2 | | | | | | | x | |
| 12.3.3 | | | | | | | x | x |
| 12.3.4 | | | | | | | x | x |
| 12.4 | PCI DSS compliance is managed. | | | | | | | |
| 12.4.1 | | | | | | | | x |
| 12.4.2 | | | | | | | | x |
| 12.4.2.1 | | | | | | | | x |
| 12.5 | PCI DSS scope is documented and validated. | | | | | | | |
| 12.5.1 | | | | | | | x | x |
| 12.5.2 | | | | | | | x | x |
| 12.5.2.1 | | | | | | | | x |
| 12.5.3 | | | | | | | | x |
| 12.6 | Security awareness education is an ongoing activity. | | | | | | | |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| 12.6.1 | | x | x | x | x | x | x | x |
| 12.6.2 | | | | | | | x | x |
| 12.6.3 | | | | | | | x | x |
| 12.6.3.1 | | x | | | x | x | x | x |
| 12.6.3.2 | | | | | | | x | x |
| 12.7 | Personnel are screened to reduce risks from insider threats. | | | | | | | |
| 12.7.1 | | | | | | | x | x |
| 12.8 | Risk to information assets associated with third-party service provider (TPSP) relationships is managed. | | | | | | | |
| 12.8.1 | x | x | x | x | x | x | x | x |
| 12.8.2 | x | x | x | x | x | x | x | x |
| 12.8.3 | x | x | x | x | x | x | x | x |
| 12.8.4 | x | x | x | x | x | x | x | x |
| 12.8.5 | x | x | x | x | x | x | x | x |
| 12.9 | Third-party service providers (TPSPs) support their customers' PCI DSS compliance. | | | | | | | |
| 12.9.1 | | | | | | | | x |
| 12.9.2 | | | | | | | | x |
| 12.10 | 12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately. | | | | | | | |
| 12.10.1 | x | x | x | x | x | x | x | x |
| 12.10.2 | | | | | | | x | x |
| 12.10.3 | | x | | | x | | x | x |
| 12.10.4 | | | | | | | x | x |
| 12.10.4.1 | | | | | | | x | x |
| 12.10.5 | | | | | | | x | x |
| 12.10.6 | | | | | | | x | x |
| 12.10.7 | | | | | | | x | x |
| A1.1 | Multi-tenant service providers protect and separate all customer environments and data. | | | | | | | |
| A1.1.1 | | | | | | | | x |
| A1.1.2 | | | | | | | | x |
| A1.1.3 | | | | | | | | x |
| A1.1.4 | | | | | | | | x |
| A1.2 | Multi-tenant service providers facilitate logging and incident response for all customers. | | | | | | | |
| A1.2.1 | | | | | | | | x |

| PCI DSS v4 Control # | SAQ-A | SAQ-A-EP | SAQ-B | SAQ-B-IP | SAQ-C | SAQ-C-VT | SAQ-D Merchant | SAQ-D Service Provider |
|---|---|---|---|---|---|---|---|---|
| A1.2.2 | | | | | | | | x |
| A1.2.3 | | | | | | | | x |
| A2.1 | POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits. | | | | | | | |
| A2.1.1 | | | | x | x | | x | x |
| A2.1.2 | | | | | | | | x |
| A2.1.3 | | | | | | | | x |