Riding the Waves of Compliance

Navigating PCI DSS v4.0

What Organisations are expected to do before 2024

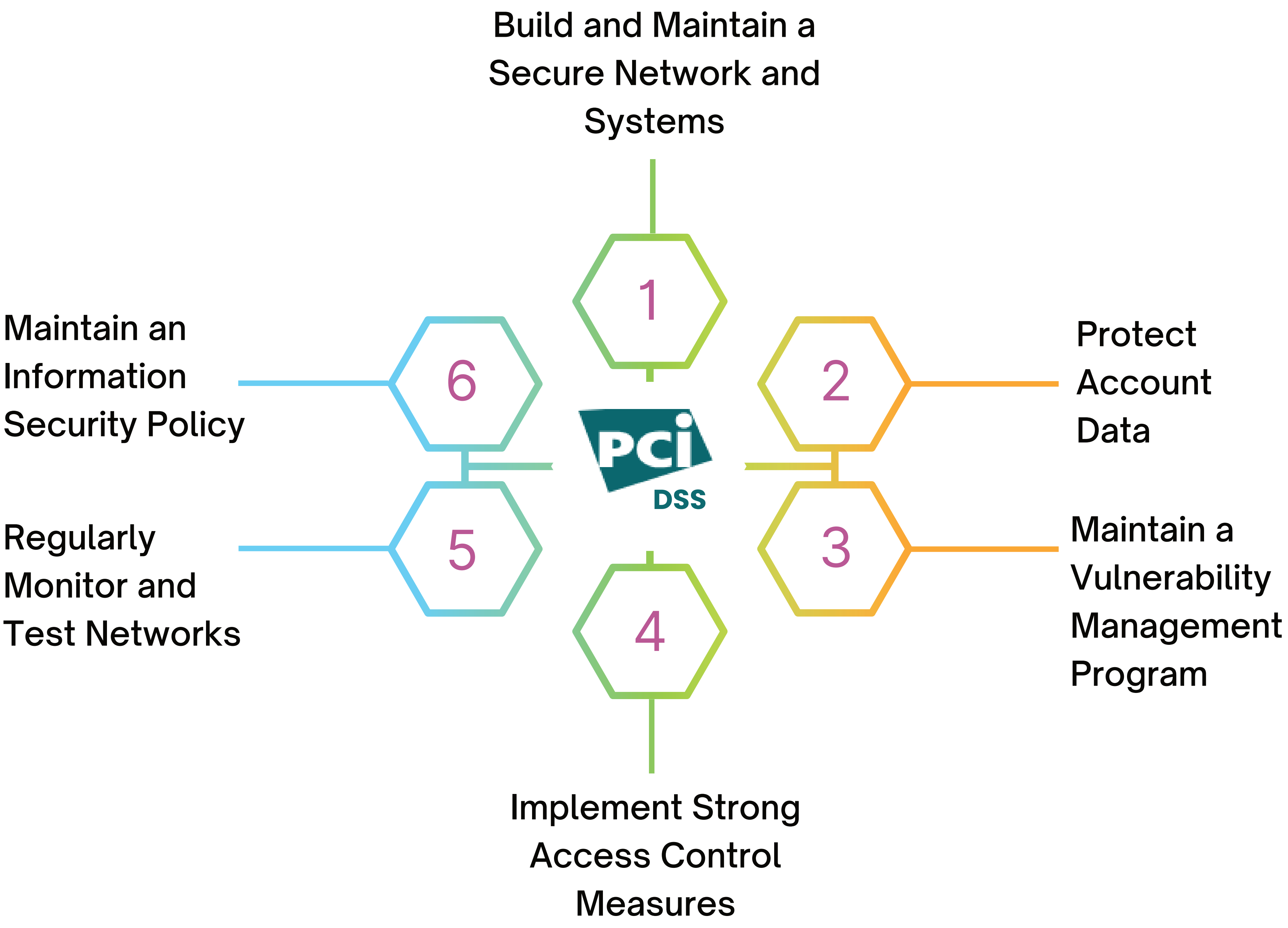
*Checklist of New Requirements Included

www.qrcsolutionz.com

In an increasingly digital world, the protection of sensitive payment card data has become more critical than ever.

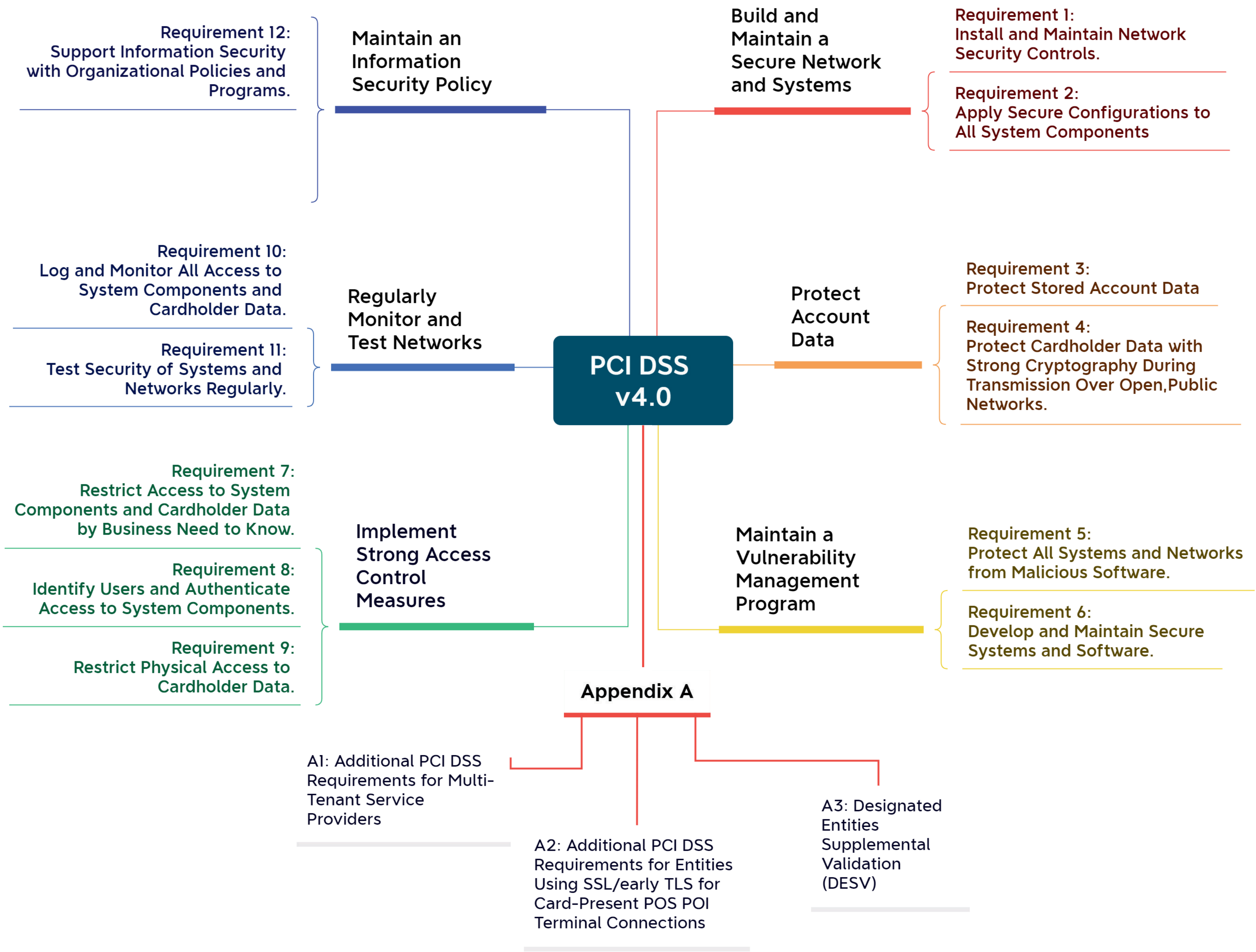
PCI DSS v4.0, the latest iteration of the Payment Card Industry Data Security Standard is designed to address the evolving challenges and emerging threats in the payment card industry.

PCI DSS v4.0 Security Objectives


Build and Maintain a Secure Network and Systems
1
Protect Account Data
2
Maintain a Vulnerability Management Program
3
Implement Strong Access Control Measures
4
Regularly Monitor and Test Networks
5
Maintain an Information Security Policy
6
PCI DSS

QRC®
Quality • Risk • Compliance
be assured . be secured

PCI Data Security Standard Requirements



PCI DSS v4.0

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls.

Requirement 2: Apply Secure Configurations to All System Components

Protect Account Data

Requirement 3: Protect Stored Account Data

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open,Public Networks.

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software.

Requirement 6: Develop and Maintain Secure Systems and Software.

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know.

Requirement 8: Identify Users and Authenticate Access to System Components.

Requirement 9: Restrict Physical Access to Cardholder Data.

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data.

Requirement 11: Test Security of Systems and Networks Regularly.

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs.

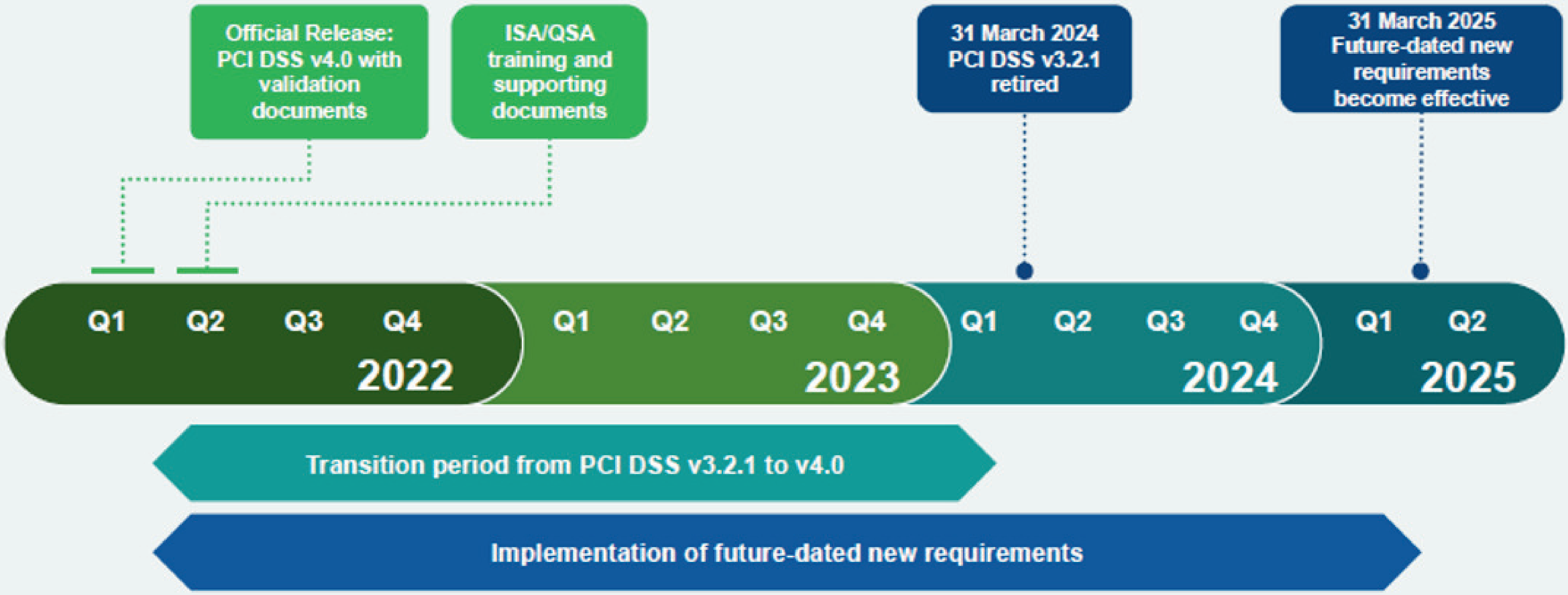
Appendix A

A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

A2: Additional PCI DSS Requirements for Entities Using SSL/early TLS for Card-Present POS POI Terminal Connections

A3: Designated Entities Supplemental Validation (DESV)

IMPLEMENTATION TIMELINE FOR v4.0


Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025 Future-dated new requirements become effective
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
Q3
Q4
2024
Q1
Q2
2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

Source : Reference Taken from PCI DSS 4.0 Standard published by PCI SSC.

Organizations are granted the period until March 31, 2024, for assessment under either PCI DSS v3.2.1 or v4.0. Post this date, on March 31, 2024, v3.2.1 will be phased out, mandating all organizations to undergo assessment following PCI DSS v4.0.

Additionally, there's an important milestone to consider for integrating new requirements introduced in v4.0. By March 31, 2025, organizations are required to have fully implemented the "best practice" requirements outlined in PCI DSS v4.0.

REVISIONS IN THE PCI DSS 4.0 REQUIREMENTS

PCI DSS 3.2.1		PCI DSS 4.0	
1.	Install and maintain a firewall configuration to protect cardholder data	1.	Install and maintain **network security controls**
2.	Do not use vendor-supplied defaults for system passwords and other security parameters	2.	**Apply secure configurations to all system components**
3.	Protect stored cardholder data	3.	Protect stored **account data**
4.	Encrypt transmission of cardholder data across open, public networks	4.	Protect cardholder data with **strong cryptography** during transmission over open. public networks
5.	Protect all systems against malware and regularly update anti-virus software or programs	5.	Protect all systems and **networks** from malicious software
6.	Develop and maintain secure systems and applications	6.	Develop and maintain secure systems and **softwares**
7.	Restrict access to cardholder data by business need to know	7.	Restrict access to **system components** and cardholder data by business need to know
8.	Identify and authenticate access to system components	8.	Identify **users** and authenticate access to system components
9.	Restrict physical access to card holder data	9.	Restrict physical access to cardholder data
10.	Track and monitor all access to network resources and cardholder data	10.	Log and monitor all access to **system components and** cardholder data
11.	Regularly test security systems and processes	11.	Test security of systems and **networks** regularly
12.	Maintain a policy that addresses information security for all personnel	12.	**Support information security with organizational policies and programs**

NEW REQUIREMENTS IN PCI DSS v4.0

The PCI DSS v4.0 comprises of a substantial number of new requirements — 64 in total. New requirements will taper in overtimewith only 13 of those 64 being effective immediately when using 4.0.

64

New Requirements

Applicable to	
All Entities	Service Providers Only
53	11

Effective Date	
Immediately for all v4.0 Assessments	31 March 2025
13	51

The additional 51 remain "best practices" until March 2025, when they too will be required to complete a PCI DSS assessment after v3.2.1 is retired.

If the SSC remains consistent in its versioning methodology, we should expect to see a minor update to version 4.1, or something of that nature, in March of 2025.

Key Compliance Processes You Need to Implement Before March 31, 2024

PCI DSS v4.0 will become effective on March 31, 2024.

In the short time, organizations need to ensure compliance with 11 fresh requirements to enure your successful 2024 PCI Report on Compliance. Below are few essential PCI DSS Compliance processes that you can put into effect before the year's end.

# Gain Control Over Your PCI Scope :

Without a well-defined scope, it becomes challenging to determine what areas require assessment. The effectiveness of your PCI DSS Compliance program hinges on your ability to efficiently manage all components within the scope of PCI DSS assessment.

New Requirements for Scope Management

- **PCI DSS v4.0 Requirement 12.5.2 (NEW!!!)**: Entities are required to document and confirm the PCI DSS scope at least once every 12 months and whenever there is a significant change to the in-scope environment.
- PCI DSS v4.0 introduces new documentation requirements for roles and responsibilities associated with activities in various requirement areas, including **Requirements 1.1.2; 2.1.2; 3.1.2; 4.1.2; 5.1.2; 6.1.2; 7.1.2; 8.1.2; 9.1.2; 10.1.2; 11.1.2 (NEW!!!)**. These roles and responsibilities must be documented, assigned, and clearly understood.

# Targeted Risk Assessments (TRAs) :

Practice of conducting Targeted Risk Assessments (TRAs) remains essential until March 2025. Nevertheless, the sooner you engage your Risk Assessment team in this process, the smoother the transition will be.

Targeted Risk Assessments are linked to requirements that allow organizations flexibility in determining the frequency of specific security and compliance tasks.

Requirements for Targeted Risk Assessments

- **PCI DSS v4.0 Requirement 5.2.3.1 :** Review the organization's deliberate risk analysis regarding how frequently it evaluates system components identified as having a low risk of malware exposure.

- Another example is **Requirement 11.3.1.1 :** Review the organization's deliberate risk analysis that defines the approach to addressing all other relevant vulnerabilities (those not classified as high-risk or critical based on the organization's vulnerability risk assessments in Requirement 6.3.1).

- Additionally, all Targeted Risk Assessments must conform to PCI DSS version 4.0 **Requirement 12.3.1**

# Customized Approach :

If you're considering employing customized approach to fulfill specific PCI DSS Requirements, I strongly advise exercising caution. The new tailored approach introduced in PCI DSS version 4.0 might not be the enthusiastic solution you've been anticipating.

Customized Approach won't **reduce compliance expenses,** and it **distinctly differs from a compensating control.**

# Items Noted For Improvement :

If you've been navigating your PCI DSS Compliance without a concrete plan, this newly introduced crucial step will help you organize and align your compliance efforts.

There's a positive and negative aspect to this recent addition.
On the upside, it's applicable solely to Level 1 merchants. Conversely, it's exclusively for Level 1 merchants.

PCI SSC brought forth the **Items Noted For Improvement (INFI)** worksheet requirement to be included alongside your annual Report on Compliance.

If your PCI Compliance initiative is already well-established, you've likely been incorporating a similar approach. Your initiative operates under a constant betterment strategy. A majority of organizations find it challenging to uphold PCI Compliance once their Report on Compliance is finalized.

With regard to INFI, it's preferable for you to pinpoint the security controls and processes that necessitate enhancement or rectification, and take appropriate action. This demonstrates to both your Qualified Security Assessor (QSA) and Acquirer that you treat your PCI Compliance duties with utmost seriousness.

CHECKLIST - CONTROLS TO BE IMPLEMENTED IMMEDIATELY TO COMPLY WITH PCI DSSv4.0

PCI v4.0 Requirements	Controls	In Place ?
2.1.2, 3.1.2, 4.1.2, 5.1.2, 6.1.2, 7.1.2, 8.1.2, 9.1.2, 10.1.2, and 11.1.2	Roles and responsibilities are to be documented, assigned, and understood. • Day-to-day responsibilities • Personnel understand and acknowledge responsibilities • RACI matrix (Responsible, Accountable, Consulted, and Informed)	No
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.	No
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months.	No
12.9.2	Third Party Service Providers (TPSPs) support customers' requests to provide PCI DSS compliance status and information about PCI DSS requirements that are the responsibility of the TPSP.	No

Reference Taken from PCI DSS 4.0 Summary of Changes, published by PCI SSC.

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
3.2.1	Any sensitive authentication data (SAD) stored prior to completion of authorization should implement data retention and disposal policies	No
3.3.2	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.	No
3.3.3	For Issuers and companies that support issuing process any storage of sensitive authentication data is : • Limited to business needs. • Encrypted using strong cryptography.	No
3.4.2	Controls to prevent copy and/or relocation of PAN when using remote access technologies.	No
3.5.1.1	Keyed cryptographic hashes when hashing is used to render PAN unreadable.	No
3.5.1.2	Disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
3.6.1.1	Additional requirement for service providers only : A documented description of the cryptographic architecture is maintained that includes : • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in **Requirement 12.3.4**.	No
4.2.1	Certificates used for PAN transmissions over open, public networks are valid and not expired or revoked.	No
4.2.1.1	Maintain an inventory of trusted keys and certificates	No
5.2.3.1	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1.**	No
5.3.2.1	If periodic malware scans are performed to meet **Requirement 5.3.2**, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1.**	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
5.3.3	For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioural analysis of systems or processes when the media is inserted, connected, or logically mounted.	No
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	No
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	No
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following : • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows : • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	No
7.2.4	All user accounts and related access privileges, including thirdparty/ vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	No
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	No
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows : • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1**). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
8.3.6	If passwords/passphrases are used as authentication factors to meet **Requirement 8.3.1,** they meet the following minimum level of complexity : • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).	No
8.3.10.1	If passwords/passphrases are the only authentication factor for customer user access, passwords/passphrases are changed at least every 90 days or the security posture of accounts is dynamically analyzed to determine real-time access to resources.	No
8.4.2	Multi-factor authentication for all access into the CDE.	No
8.5.1	MFA systems are implemented as follows : • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	No
8.6.2	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	No
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows : • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1**) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
9.5.1.2.1	The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1.**	No
10.4.1.1	Automated mechanisms are used to perform audit log reviews.	No
10.4.2.1	The frequency of periodic log reviews for all other system components (not defined in **Requirement 10.4.1)** is defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1**.	No
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems : • Network security controls, IDS/IPS • Change-detection mechanisms. • Anti-malware solutions, Physical access controls. • Logical access controls, Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to : • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	No
11.3.1.1	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at **Requirement 6.3.1**) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1**. • Rescans are conducted as needed.	No
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with **Req 8.2.2**.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
11.4.7	Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per **Requirement 11.4.3 and 11.4.4**.	No
11.5.1.1	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	No
11.6.1	A change- and tamper-detection mechanism is deployed as follows : • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows : – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1**).	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes : • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	No
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following : • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	No
12.5.2.1	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in **Requirement 12.5.2.**	No
12.5.3	Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	No
12.6.2	The security awareness program is : • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to : • Phishing and related attacks • Social engineering.	No
12.6.3.2	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with **Requirement 12.2.1.**	No
12.10.4.1	The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in **Requirement 12.3.1.**	No
12.10.5	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to : • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. • Detection of unauthorized wireless access points.	No

CHECKLIST - CONTROLS AS BEST PRACTICES UNTIL 31ST MARCH 2025

PCI v4.0 Requirements	Controls	In Place ?
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include : • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	No
A1.1.1	The multi-tenant service provider confirms access to and from customer environment is logically separated to prevent unauthorized access.	No
A1.1.4	The multi-tenant service provider confirms effectiveness of logical separation controls used to separate customer environments at leave once every six months via penetration testing.	No
A1.2.3	The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.	No
A3.3.1	Failures of the following are detected, alerted, and reported in a timely manner : • Automated log review mechanisms • Automated code review tools.	No

STAY TUNED . . .

Follow for more

✉ info@qrcsolutionz.com

🌐 www.qrcsolutionz.com