NETWORK INTELLIGENCE
The Digital Security Company

GUIDANCE DOCUMENT

PCI DSS v4.0.1:
Requirements effective from April 2025

- ***Shashvat Kumar***

- *Requirement Details*
- *The Crux*
- *References*

Requirement Details

The following are the control descriptions, activity details, and the applicability notes for the requirements which the entities must implement and adhere to by the end of March 2025 to maintain their ongoing PCI DSS compliance:

S. No.	Control Description	Req. No.	Applicability	Action Needed
1	Expanded scope of Data Retention & Disposal policy, procedure, and processes	3.2.1	Applicable to both service providers and merchants.	• Amend the existing Data Retention & Disposal policy and procedure documents to incorporate within them the coverage of any Sensitive Authentication Data (SAD) such as CVV, track 2 data, and PIN which is stored prior to completion of authorization. • Implement controls for secure deletion of SAD immediately after the authorization is completed.
2	Cryptographic protection to SAD storage	3.3.2	Applicable to both service providers and merchants.	Encrypt the SAD which is stored electronically prior to completion of authorization using strong cryptography.
		3.3.3	Applicable only to issuers and companies that support issuing services and store SAD.	Encrypt all storage of SAD using strong cryptography.
3	Protection of PAN while using remote-access technologies	3.4.2	Applicable to both service providers and merchants.	• Implement controls to prevent copy functionality and/ or relocation of PAN when using remote-access technologies such as virtual desktop. • Document all exceptions to this process which should be explicitly approved and must be

S. No.	Control Description	Req. No.	Applicability	Action Needed
				supported by a justifiable and defined business need.
4	Enhanced hashing requirement for PAN protection	3.5.1.1	Applicable to both service providers and merchants.	• Ensure that the hashing function which is used to protect PAN is based on strong cryptography and uses keyed cryptographic hashes of the entire PAN. • The key which is used for this hashing function should be protected using the existing PCI DSS key management requirements (R3.6 and R3.7).
5	Enhanced disk-level/ partition-level encryption	3.5.1.2	Applicable to both service providers and merchants who rely only on disk-level or partition-level encryption for securing PAN.	• Ensure that the disk-level or partition-level encryption is implemented only for such PAN which is stored on removable media. • In case disk-level or partition-level encryption is implemented for securing PAN storage on non-removable media, ensure that additional control from R3.5 (encryption, hashing, truncation, or tokenization) is also used to secure PAN separately on the stored data.
6	Use of separate & unique cryptographic keys in production & test environments	3.6.1.1	Applicable only to service providers.	• Amend the Cryptographic Architecture document to include clauses preventing the use of the same

S. No.	Control Description	Req. No.	Applicability	Action Needed
				cryptographic key for protection of stored PAN in test and production environments. • Ensure the usage of separate and unique cryptographic keys for protection of stored PAN in test and production environments.
7	Validity checks for certificates used to safeguard PAN during transmission	4.2.1	Applicable to both service providers and merchants.	• Implement controls to ensure that the certificates which are used to protect PAN during transmission are valid and are not expired or revoked. • Document the methods used in the procedure document.
8	Inventory management for security purposes	4.2.1.1	Applicable to both service providers and merchants.	• Amend the existing policy and procedure documents to define the processes in place to draft and maintain an inventory of all the trusted keys & certificates which are used to safeguard PAN during transmission. • Draft and maintain an inventory of all the trusted keys & certificates which are used to safeguard PAN during transmission. Ensure that the inventory is kept up-to-date at all times.

S. No.	Control Description	Req. No.	Applicability	Action Needed
		6.3.2	Applicable to both service providers and merchants who have custom and bespoke software.	• Draft and maintain an inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software. Ensure that the inventory is kept up-to-date at all times. • Utilize this inventory for vulnerability and patch management processes.
		12.3.3	Applicable to both service providers and merchants.	• Draft and maintain an inventory of all cryptographic cipher suites and protocols in use. Ensure that the inventory is kept up-to-date at all times. The inventory should be reviewed at least once every 12 months. • The inventory should include ‘purpose’ and ‘where used’ details for the cryptographic cipher suites and protocols. • Utilize this inventory for active monitoring of industry trends regarding continued viability and security of all cryptographic cipher suites and protocols in use.

S. No.	Control Description	Req. No.	Applicability	Action Needed
				• Define and document a plan to respond to anticipated changes in cryptographic vulnerabilities.
		12.3.4	Applicable to both service providers and merchants.	• Draft and maintain an inventory of all hardware and software technologies in use. Ensure that the inventory is kept up-to-date at all times. The inventory should be reviewed at least once every 12 months. • The inventory should include details of 'end-of-life' and 'end-of-support' industry announcements for the technologies in use. • Utilize this inventory for ensuring that the technologies continue to receive security fixes from vendors promptly and continue to support PCI DSS compliance. • Define and document a plan to remediate the outdated technologies including those for which the vendor has announced the 'end-of-life'. Get this plan approved by the senior management.

S. No.	Control Description	Req. No.	Applicability	Action Needed
9	Targeted Risk Analysis Methodology	12.3.1	Applicable to both service providers and merchants.	• Define and document a Targeted Risk Analysis methodology which is based on all the criteria as defined in R12.3. • Perform Targeted Risk Analysis and document the results on an annual basis for all the PCI DSS requirements where the entity utilizes customized approach and where the standard provides the flexibility to an entity to determine the periodicity of a control requirement.
10	Perform Targeted Risk Analysis	5.2.3.1	Applicable to those service providers and merchants who have system components which have been identified as not at risk for malware.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of periodic evaluations of system components identified as not at risk for malware. • Document the results of the TRA and the determined frequency.
		5.3.2.1	Applicable to those service providers and merchants who conduct periodic malware scans to meet R5.3.2.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of periodic scans on the system components. • Document the results of the TRA and the determined frequency.

S. No.	Control Description	Req. No.	Applicability	Action Needed
		7.2.5.1	Applicable to both service providers and merchants.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of access review activity for the system and application accounts of the entity. • Document the results of the TRA and the determined frequency.
		8.6.3	Applicable to both service providers and merchants.	• Perform targeted risk analysis based on R12.3 methodology to determine the password complexity and frequency of password change activity for the application and system accounts. • Document the results of the TRA and the determined frequency.
		9.5.1.2.1	Applicable to those service providers and merchants who use POI devices.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency and type of periodic POI device inspections to be performed. • Document the results of the TRA and the determined frequency.
		10.4.2.1	Applicable to both service providers and merchants.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of periodic log reviews for all those system

S. No.	Control Description	Req. No.	Applicability	Action Needed
				components which are not already covered by R10.4.1. • Document the results of the TRA and the determined frequency.
		11.3.1.1	Applicable to both service providers and merchants.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of closure timelines for vulnerability types other than high or critical (for example medium, low, and informational). • Document the results of the TRA and the determined frequency.
		11.6.1	Applicable to those service providers and merchants who have payment pages and scripts and whose change-and-tamper-detection mechanism for such page and scripts does not function at least once a week.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency at which the change-and-tamper-detection mechanism for the payment page and scripts should function. • Document the results of the TRA and the determined frequency.

S. No.	Control Description	Req. No.	Applicability	Action Needed
		12.10.4.1	Applicable to both service providers and merchants.	• Perform targeted risk analysis based on R12.3 methodology to determine the frequency of periodic training activity for incident response personnel. • Document the results of the TRA and the determined frequency.
11	Enhanced anti-malware solution capabilities	5.3.3	Applicable to both service providers and merchants.	Enable controls on anti-malware solution to perform automatic scans or continuous behavioral analysis of systems or processes whenever a removable media is inserted, connected, or logically mounted.
12	Implement anti-phishing mechanisms	5.4.1	Applicable to both service providers and merchants.	Define processes and implement appropriate controls to detect and protect personnel against phishing attacks.
13	Deployment of Web Application Firewall (WAF)	6.4.2	Applicable to both service providers and merchants.	Deploy WAF in front of public-facing web applications and configure it as per the criteria of R6.4.1 to detect and prevent web-based attacks.
14	Protection of payment pages and scripts	6.4.3	Applicable to those service providers and merchants who have payment page scripts or	• Define processes and implement controls to assure the integrity of all such scripts.

S. No.	Control Description	Req. No.	Applicability	Action Needed
			scripts that include a TPSP’s/ payment processor’s embedded payment page/ form.	• Define processes and implement controls to ensure that only authorized scripts can be loaded and executed. • Draft and maintain an inventory of all scripts on payment pages and scripts with a written business/ technical justification against each as to why it is required. Ensure that the inventory is kept up-to-date at all times. • Define the methods and processes used to meet these controls in a procedure document.
		11.6.1	Applicable to those service providers and merchants who have payment pages and scripts.	• Implement a change-and-tamper-detection mechanism for payment page which can detect unauthorized modifications to the security-impacting HTTP headers and the script contents when the payment page is received by the consumer browser. • Configure this mechanism to generate alerts for any unauthorized modification attempt. • Configure the mechanism to function at least once a week to compare and evaluate the received HTTP

S. No.	Control Description	Req. No.	Applicability	Action Needed
				headers and payment pages against the baseline and expected values. • Define the methods and processes used to meet these controls in a procedure document.
15	Enhancement in logical Access Management processes	7.2.4	Applicable to both service providers and merchants.	• Perform access review activity for all user accounts and related access privileges at least once every 6 months. • The management should acknowledge that access privileges remain appropriate. • Document the results of the review activity. • Define the access review process of the entity in a procedure document.
		7.2.5	Applicable to both service providers and merchants.	• Perform access review activity for all system and application accounts and related access privileges at a frequency defined in targeted risk analysis. • The management should acknowledge that access privileges remain appropriate. • Document the results of the review activity. • Define the access review process of the entity in a procedure document.

S. No.	Control Description	Req. No.	Applicability	Action Needed
16	Enhancement in password policy requirements	8.3.6	Applicable to both service providers and merchants.	• Password length parameter for user accounts should be set to a minimum of 12 characters. • If the system does not support setting password length as 12 characters, it should be set to a minimum of 8 characters.
		8.3.10.1	Applicable only to those service providers who use single-factor of authentication implementation for customer user access.	Password expiry parameter for these accounts should be set to a maximum of 90 days or implement a control to dynamically analyze the security posture of such accounts which determines real-time access to resources automatically.
		8.6.3	Applicable to both service providers and merchants.	• Passwords/ passphrases for system and application accounts should be changed at the frequency defined in the targeted risk analysis and upon suspicion or confirmation of compromise. • Passwords/ passphrases for system and application accounts should be constructed with appropriate complexity as determined in the targeted risk analysis. • Amend the existing policy and procedure documents to incorporate these processes.

S. No.	Control Description	Req. No.	Applicability	Action Needed
17	Managing interactive use of system and application accounts	8.6.1	Applicable to those service providers and merchants where any application or system account can be used for interactive login.	• Implement controls and define processes to prevent interactive use of application and system accounts unless needed for an exceptional circumstance. • Ensure that the exceptions are time-bound. • Ensure that business justification for interactive use is documented and the management explicitly approves the interactive use. • Ensure that individual identity is confirmed before granting access to account and that the actions taken are attributable to an individual user. • Define these processes in a procedure document.
		8.6.2	Applicable to those service providers and merchants where any application or system account can be used for interactive login.	• Remove presence of hardcoded passwords/ passphrases for any application and system account that can be used interactively from scripts, configuration files, property files, or source code. • Amend the system development procedure document to include the clause preventing the hardcoding of passwords/ passphrases for these accounts and processes in place to ensure its implementation.

S. No.	Control Description	Req. No.	Applicability	Action Needed
18	Enhancement in Multifactor Authentication (MFA) requirements	8.4.2	Applicable to both service providers and merchants.	Implement MFA for all non-console access into the CDE.
		8.5.1	Applicable to both service providers and merchants.	• Maintain vendor documentation of the MFA solution in use. • Ensure that MFA solution is configured in accordance with the best security practices as outlined in the vendor documentation. • Ensure that the MFA solution is not susceptible to replay attack. • Ensure that the MFA solution requires at least two different types of authentication factors at all times and that success of all authentication factors is required before access is granted. • Ensure that MFA solution cannot be bypassed by users, including administrators, and that any exception to this is authorized by management based on the documented need and is temporary in nature.
19	Deployment of automated log review mechanism (such as SIEM)	10.4.1.1	Applicable to both service providers and merchants.	• Deploy an automated log review mechanism such as a SIEM solution.

S. No.	Control Description	Req. No.	Applicability	Action Needed
				• Configure the SIEM solution appropriately to facilitate the audit log review process.
20	Expanded scope of failure management requirements for critical security control systems	10.7.2	Applicable to both service providers and merchants. Earlier, this requirement was applicable only to service providers.	• Service providers should extend the existing failure detection and alerting mechanism and processes to ‘audit log review mechanisms’ and ‘automated security testing tool (if used)’ solutions as well. • Service providers should amend the existing procedure document to incorporate the detection, alerting, addressing, and responding processes for failure of ‘audit log review mechanisms’ and ‘automated security testing tool (if used)’ solutions. • Merchants should implement controls and define detection, alerting, addressing, and responding processes for failure of any critical security control systems (including but not limited to NSCs, IDS/ IPS, change-detection mechanisms, anti-malware solutions, physical access controls, logical access controls, audit logging mechanisms, segmentation controls, audit log review mechanisms, automated security testing tools).

S. No.	Control Description	Req. No.	Applicability	Action Needed
				- Merchants should define detection, alerting, addressing, and responding processes for failure of all the above-mentioned critical security control systems in a procedure document.
		10.7.3	Applicable to both service providers and merchants. Earlier, this requirement was applicable only to service providers.	- Merchants should implement controls and define responding processes for failure of any critical security control systems. - Merchants should define responding processes for failure of all the above-mentioned critical security control systems in a procedure document. - Merchants should document the cause of failure, duration of failure, required remediation details in a report for all such failure incidents.
		A3.3.1	Applicable only to Designated Entities (DE). These entities are designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements.	- Designated Entities should extend the existing failure detection and alerting mechanism and processes to ‘automated audit log review mechanisms’ and ‘automated code review tools (if used)’ solutions as well. - Designated Entities should amend the existing procedure document to incorporate the detection,

S. No.	Control Description	Req. No.	Applicability	Action Needed
				alerting, addressing, and responding processes for failure of ‘automated audit log review mechanisms’ and ‘automated code review tools (if used)’ solutions.
21	Enhanced Vulnerability Management requirements	11.3.1.1	Applicable to both service providers and merchants.	• Address vulnerability types other than critical or high (such as medium, low, and informational) within the timeframe as defined in the targeted risk analysis. • Conduct internal vulnerability rescans also for vulnerability types other than critical or high as needed after the closure of such vulnerabilities.
		11.3.1.2	Applicable to both service providers and merchants.	• Ensure that the internal vulnerability scans are performed via authenticated scanning via accounts with sufficient privileges. • Ensure that all the system components which do not support authenticated scanning are defined and documented.
		11.4.7	Applicable to only multi-tenant service providers.	Multi-tenant service providers must support their customer by providing evidence that external penetration testing has been performed by them or

S. No.	Control Description	Req. No.	Applicability	Action Needed
				allow their customers to perform such testing on its environment by providing appropriate access and permissions.
22	Enhanced intrusion protection requirement	11.5.1.1	Applicable only to service providers.	• Deploy an intrusion-detection and/ or intrusion-prevention technique (such as IDS/ IPS) that is capable of detecting, alerting, preventing, and addressing covert malware communication channels. • Maintain documentation of the methods used for meeting this requirement.
23	PCI DSS scope review requirements	12.5.2.1	Applicable only to service providers.	• Identifying and documenting the PCI DSS scope in accordance with all the criteria of R12.5.2. • Reviewing the PCI DSS scope at least once every 6 months and after any significant change and making the necessary updates to the documents and diagrams. • Capture the results of the review activity in the PCI DSS scope document to confirm that the documented scope is accurate.

S. No.	Control Description	Req. No.	Applicability	Action Needed
		12.5.3	Applicable only to service providers.	• Conduct a review of PCI DSS scope document after significant changes to organizational structure to assess its impact on the PCI DSS scope and applicability of controls. • Capture the results of the review activity in the PCI DSS scope document. • Communicate the results of the review activity to the executive management.
24	Enhancement in Security Awareness program for employees	12.6.2	Applicable to both service providers and merchants.	• Review the contents of the Security Awareness program at least once every 12 months. • Update the document as needed to address and incorporate any new threats and vulnerabilities that may impact the security of cardholder data or when information regarding the role of employees pertaining to information security and protection of cardholder data is updated or modified.
		12.6.3.1	Applicable to both service providers and merchants.	• Ensure that the training material also includes awareness about Phishing and related attacks.

S. No.	Control Description	Req. No.	Applicability	Action Needed
				- Ensure that the training material also includes awareness about Social Engineering and the associated attacks.
		12.6.3.2	Applicable to both service providers and merchants.	Ensure that the training material also includes awareness about the acceptable use of end-user technologies and the Acceptable Usage policy.
25	Expanded scope of Incident Response plan and procedures	12.10.5	Applicable to both service providers and merchants.	- Define processes and controls to monitor and respond to alerts from 'change-and-tamper-detection' mechanism in addition to other security monitoring systems (including but not limited to IDS/ IPS, NSC, FIM, rogue WAP detector). - Amend the existing Incident Response plan to incorporate and document these processes.
		12.10.7	Applicable to both service providers and merchants.	- Define and document incident response procedures for responding to the detection of stored PAN anywhere it is not expected to exist. - The procedures should include processes for PAN's retrieval, secure deletion, and/or migration into the defined CDE boundary.

S. No.	Control Description	Req. No.	Applicability	Action Needed
				• The procedures should include processes for checking SAD presence along with PAN should also be defined. • The procedures should include processes for determining where the CHD and SAD came from and how these ended at the unexpected storage location. • The procedures should include processes for remediating the data leaks or process gaps which caused the incident. • Incident Response plan to be initiated at the discovery of such data and the above-defined procedures should be referred to. • Draft an Incident Report documenting all the required fields as per the Incident Response procedures.
26	Logical separation of customer environments for multi-tenant service providers	A1.1.1	Applicable only to multi-tenant service providers.	• Define processes and implement technical controls to enforce logical separation between environments of one customer from another and between

S. No.	Control Description	Req. No.	Applicability	Action Needed
				environments of multi-tenant service provider and customers. • Enforce authorization controls where the customer must access the environment of multi-tenant service provider. • Define the processes and controls in place to enforce such logical separation in a procedure document.
		A1.1.4	Applicable only to multi-tenant service providers.	Test the effectiveness of logical separation controls used to separate customer environments via penetration testing which is supported by a documented report at least once every 6 months.
27	Introduction of incident and vulnerability reporting mechanism for customers of multi-tenant service providers	A1.2.3	Applicable only to multi-tenant service providers.	• Define processes and implement an incident and vulnerability reporting mechanism for the customers. • Define processes for addressing such reported incidents and vulnerabilities and taking the required remediation action as per R6.3.1 and R12.10.

The Crux

If your entity has not already defined processes and implemented controls for these requirements, it is now or never! You must start the work immediately without further delay as with every single day passing it shall increase the risk of your entity becoming non-compliant to PCI DSS v4.0.1 standard. Ensure to meet these requirements before March 31, 2025, to maintain your ongoing PCI DSS compliance.

We have a team of Security Experts and QSAs who can assist and guide you throughout your PCI DSS Compliance Programmes. You can reach out to us contact@networkintelligence.ai for any consultation & implementation support that you may require.

References

- *PCI DSS v4.0.1*