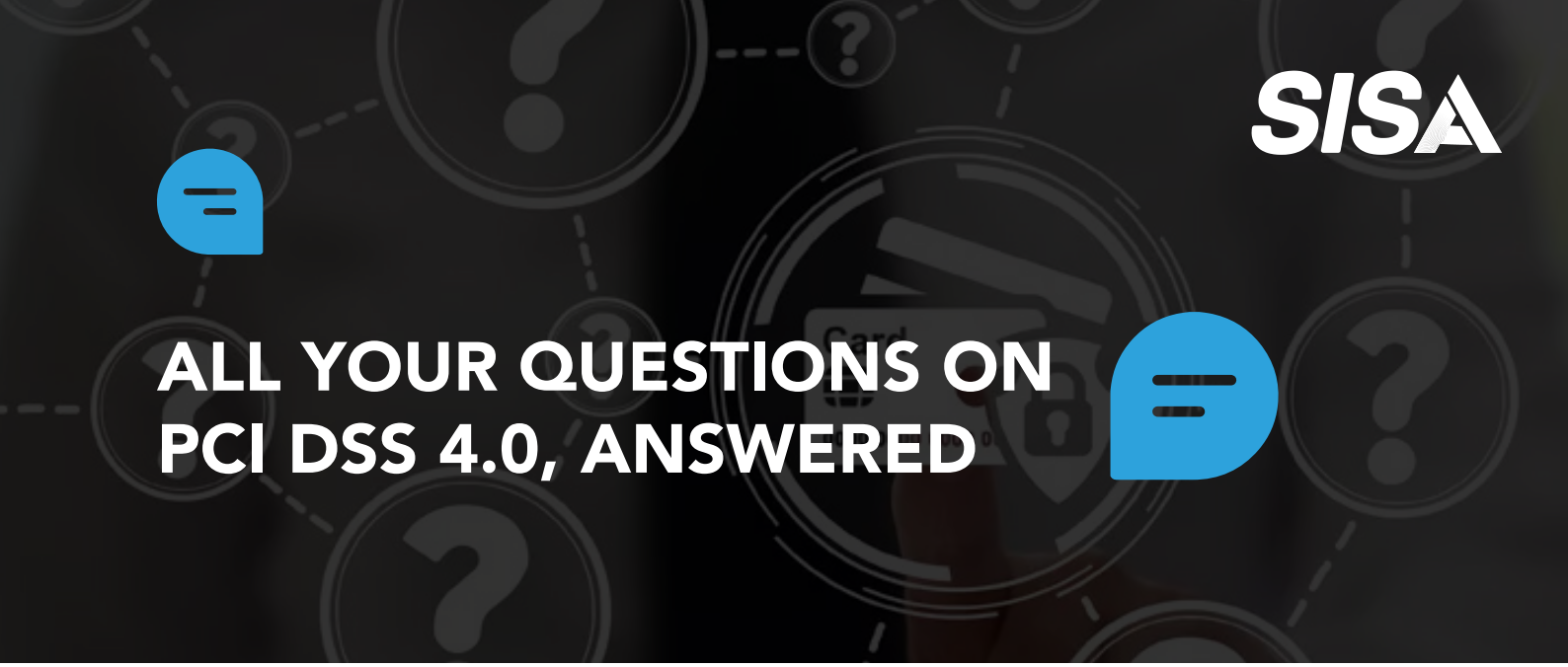


ALL YOUR QUESTIONS ON PCI DSS 4.0, ANSWERED

The newly released PCI DSS 4.0 continues to be hotly debated and discussed, since its launch on 31st March 2022. The new standards are aimed at enhancing the security of systems involved in processing, storage and transmission of cardholder data while also addressing new payment environments, technologies and evolving risks.

This post helps answer some of the frequently asked questions on the new standard including implementation queries, to help create awareness and guide organizations in their transition.

1 If an organization gets re-certified on January 2024 and the following certification is done in January 2025, can they still be certified on v.3.2.1 because v4.0 will be cut-off from March 2025?

- PCI DSS version 3.2.1 will get retired on 31st March 2024. Hence any assessment being performed post that will have to be on v4.0.

2 What are the major changes in version 4.0?

- Kindly refer to PCI DSS summary of changes (v3.2.1 to v4.0) document at PCI SSC document library page for information on changes introduced in v4.0.
- Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards

3 Do we have any changes on Data Encryption?

- Yes, PCI DSS v4.0 allows Disk level encryption for only removable media as per requirement 3.5.1.2 (“New requirement that disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media or, if used on non-removable electronic media, the PAN is also rendered unreadable via a mechanism that meets Requirement 3.5.1.”).
- Kindly refer to PCI DSS summary of changes (v3.2.1 to v4.0) document at PCI SSC document library page for information on changes introduced in v4.0.
- Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards

4 When will Prioritized Approach document for PCI DSS v4.0 be released? Can we continue to follow the prioritized v3.2.1 in the meantime?

- PCI SSC has not highlighted the release date for Prioritized Approach document. SISA expects that PCI SSC will be releasing the supporting document within next 2-3 months.
- Prioritized approach v3.2.1 is applicable only for PCI DSS v3.2.1. Considering that PCI DSS v3.2.1 is valid until 31st March 2024, organizations can continue using the document until then.

5 What is the difference b/w customized approach controls and compensating controls?

- Compensating Controls are applicable for entities which are not able to meet the requirement as stated in the defined approach due to the documented technical or business constraints, but the entity has implemented alternative controls to mitigate the risk associated with that control.
- Customized approach is defined for entities which have mature risk management practices and choose to implement different controls that meet the customized approach objectives but do not meet the requirement as stated.

6 How about third-party contractors and their approach to customized environment? Is that workable?

- Customized approach is defined for entities which have mature risk management practices and choose to implement different controls that meet the customized approach objectives but do not meet the requirement as stated.
- Hence the entity must ensure that the 3rd party contractors have very good knowledge, high security maturity level and/or risk management practice to make it eligible for customized approach. A proper due diligence must be carried out.

7 Does PCI DSS v4.0 address data leakage threats and associated controls, if any?

- PCI DSS v4.0 has not covered the threats and associated controls related with data leakage.
- A part of requirement 11.5.1.1 (additional requirement for service provider) standard highlights that having a DLP solution is a good practice.
- A part of requirement A3.2.6 Appendix 3 (DESV) standard highlights that, mechanisms should be in place to detect and prevent cleartext PAN from leaving the CDE via unauthorized channel, method or processes.

8 Currently Biometric is used as physical security control for CDE environment so do we need MFA for physical security control. For example: Biometric + PIN?

- The requirement of MFA is basically for all remote access and administrators with non-console access to CDE. MFA is not required for any physical access per se.

9 **Is there any summary comparison chart for v3.2.1 vs v4.0?**

- Kindly refer to PCI DSS summary of changes (v3.2.1 to v4.0) document at PCI SSC document library page for information on changes introduced in v4.0.
- Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards

10 **For organizations that are currently implementing v3.2.1 when will v4.0 be applicable?**

- PCI DSS v3.2.1 will be valid until 31st March 2024.
- Entities can start implementing controls as highlighted in v4.0 to ensure the compliance before opting for the assessment as per v4.0.
- Post 31st March 2024 v3.2.1. will retire and all entities must be certified on v4.0. All evolving requirements under v4.0 should be addressed, and an organization must be compliant against these requirements before 2025.

11 **Risk assessment in Vulnerability assessment appears more stringent in v4.0, which now requires Medium and Low rating, and this will yield a lot of vulnerabilities to be mitigated. Is the Risk Assessment required going to be a manual approach or can we use automated tools like Tenable which has integrated Threat intelligence and Data Science wherein, it has VPR or Vulnerability Priority Rating which prioritizes those real threats that are publicly exploitable?**

- PCI never mandates b/w an automated solution or a manual approach being followed. The flexibility is with the end customer. The only important parameter here is the risk associated with a particular control must be identified and actioned upon accordingly. Please note though, that PCI mandates an authenticated scan to be performed to identify the vulnerabilities.

12 **Can you share Website/Link to refer/learn about new standard, changes etc.?**

- Kindly refer the document library page of PCI SSC website.
- Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards

13 **Previously we had customized actions covered under CCW… How will that change now?**

- Customized approach is defined for entities which have mature risk management practices and choose to implement different controls that meet the customized approach objectives but do not meet the requirement as stated.
- Hence the entity must ensure that the 3rd party contractor has very good knowledge, high security maturity level and/or risk management practice to make it eligible for customized approach.

14 Whether the customized approach would include the term called compensatory controls?

Compensating controls and customized controls are two different things.

- Customized approach is defined for entities which have mature risk management practices and choose to implement different controls that meet the customized approach objectives but do not meet the requirement as stated. Hence the entity must ensure that the 3rd party contractor has very good knowledge, high security maturity level and/or risk management practice to make it eligible for customized approach.
- Compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as stated, due to legitimate and documented technical or business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

15 Any specific requirements change for Service Providers?

- Kindly refer to "6. Summary of New Requirements" on page 29 of PCI DSS summary of change (v3.2.1 to v4.0) document at PCI SSC document library page.
- Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards

16 Can an organization migrate or switch over or toggle between the defined & customized approach during the re-certification?

- Yes, but this again depends on the scope of work covered during the certification process and the applicability of controls defined.

17 How about continuation of compliance in case of any mergers or acquisitions?

- Same process as usual. A delta assessment must be performed, and all the relevant documents must be updated. Else this can be covered during the re-certification process.

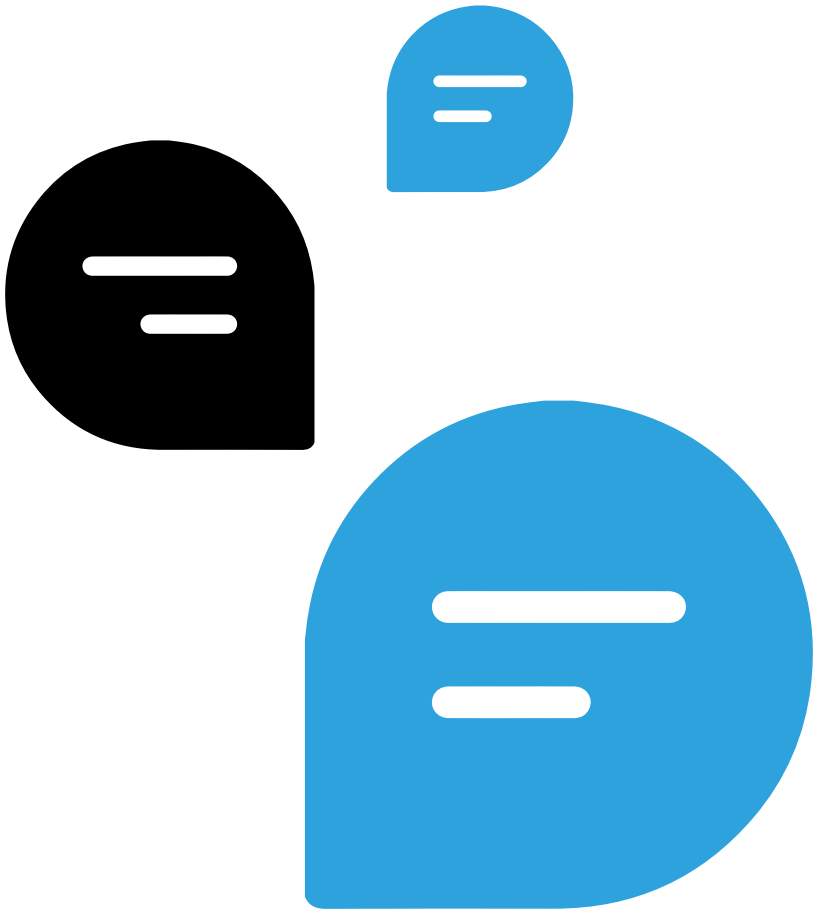
18 How and when will the new PCI DSS standards be aligned / integrated with the Regulatory asks/ guidelines (in our case RBI) on PCI DSS?

- Different RBI guidelines released for entities in payment eco-system mandate entities to be PCI DSS compliant. Considering that PCI DSS v3.2.1 will be valid until 31st March 2024, entities can continue following the same until RBI releases specific guidelines mandating compliance as per PCI DSS v4.0.

19 **Does the new standard recommend or enforce the use of strong cryptographic standards like FIPS 140-2?**

- Please refer to https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1649361221495 (Cryptography)

To know more about the key strategies and best practices to seamlessly transition to **PCI DSS v4.0, check out our Webinar on PCI DSS 4.0: A Step Towards a Better Cybersecurity Posture'** or read our earlier **Blog** post.



About SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

We are one of the Global PCI Forensic Investigators

1,000+	2,000+	40+
Active engagements	Global customers served	Countries

Global Presence

US | UK | Bahrain | Saudi Arabia | UAE | India | Singapore | Australia