A Comprehensive Guide to PCI-DSS 4.0 for Data Security, Governance and Privacy Teams

by Sanjay Raja

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) applies to all businesses that accept, process, store, or transmit cardholder data, regardless of size or number of transactions.

Accepting payment cards, processing, storing, or transmitting cardholder data triggers the PCI DSS compliance requirement. In addition, every company that stores, processes, or transfers credit card data must meet the requirements of the PCI DSS and prove this once a year. Violations of PCI DSS could cause financial penalties and damage to your reputation.

PCI DSS 4.0 provides the latest guidance on what organizations need to do to ensure that they are taking the right security measures regarding their systems, networks, and processes to protect customers' sensitive data, such as credit card numbers and personal information, from unauthorized access or theft.

What's New in PCI DSS 4.0 Relevant to Cardholder Data

The most significant change from PCI DSS 3.2.1 to 4.0 is the introduction of the Customized Approach. This recognizes that the requirements don't fit every organization perfectly, and allows certain entities to select controls that they deem most suitable for their environment to manage associated risks. This also allows for customizations to be made based on emerging technologies. We remember when the adoption of cloud technology became complicated based on outdated standards in old versions. While there are other requirements, other data-related requirements include:

- Need to understand data ownership with new guidelines for the management of shared, group, and generic accounts.
- Authenticated Scanning of systems
- Encryption of sensitive authentication data (SAD)
- Prevention of copying and/or relocating of the primary account number (PAN) when using remote-access technologies
- Automated mechanisms to perform audit log reviews

The Self-Assessment Questionnaires and the Report on Compliance template have been greatly expanded in levels of detail and doubled in size. It is clear the amount of effort required to pass an audit has increased dramatically!

To map PCI-DSS 4.0 requirements to your data security and privacy program, you should approach this systematically by aligning the PCI-DSS controls with your existing security frameworks, policies, and technologies. Below is a step-by-step guide that:

- Reviews important considerations around streamlining PCI-DSS 4.0 and improving your security and privacy controls
- A detailed mapping of specific regulations and now to streamline the process of meeting these requirements
- How to build a practice that is always working towards continuous compliance

PCI-DSS 4.0 and Important Considerations

PCI-DSS 4.0 introduces updated requirements focusing on increased flexibility, security as a continuous process, and improved validation methods. While it covers areas such as network connectivity, storage requirements, and applications, in this paper we have focused on the best practices and requirements for securing the actual data. Please note that some sections that are described as best practices for now, will become enforceable requirements in October 2025.

Below we have mapped out the relevant sections for the Data Security, Governance, and Privacy teams, as they work together to both achieve PCI and also continuously improve their security posture by lowering risk. We not only highlight areas of importance but also provide recommendations on how to improve processes in meeting PCI-DSS 4.0 requirements. However, as a quick summary of considerations and best practices, at a high level, we recommend the following actions:

Identify Key Data and Systems

This is relevant to multiple requirements with PCI-DSS and is a necessary first step to making sure that no stone goes unturned when determining where sensitive data exists. However, what is also critical is not only identifying sensitive data but also understanding where it resides or can be moved, who owns this data, and who has access to it, including who can see it, copy it, or move it.

- **Data Identification:** Catalog your sensitive payment data (e.g., PAN, CVV, etc.), Personally Identifiable Information (PII), and any customer information subject to PCI-DSS controls. Leveraging AI to identify even unknown info types saves a

lot of manual effort as too many solutions dump data into an unknown category. This is increasingly more difficult as most solutions making misleading claims around finding account information within unstructured data or across data stream solutions do not go deep enough to be effective.

- **Data Flow Mapping:** Map how data moves through your systems, including where it is stored, processed, or transmitted. Ensure you know which systems handle cardholder data. Many data security solutions struggle to do this in real time or take snapshots that are quickly out of date based on modern, dynamic cloud architectures.

- **Digital Transformation and Identifying System:** Identify servers, databases, payment gateways, and other infrastructure involved in payment processing or storing sensitive data. This can be extraordinarily challenging to achieve across cloud, hybrid-cloud, and multi-cloud environments, newer info types, and combinations of structured and unstructured databases. A true AI-native data security solution can even predict areas where data may be stored or copied that are unexpected by data owners and stewards. Digital transformation efforts typically require planning for future scalability needs, this is also where many legacy solutions are not architected for rapid changes and scaling of data when using cloud computing.

Integrate Privacy Requirements

Many companies will also likely need to align with privacy regulations like GDPR or CCPA in addition to PCI-DSS. While PCI-DSS focuses on cardholder data security, integrating privacy controls helps protect the broader spectrum of customer information such as date of birth, contact info, and even social security card data.

PCI-DSS vs. GDPR: PCI focuses on payment data (e.g., PANs), whereas GDPR encompasses all PII. Make sure your data minimization, data subject rights, and breach notification policies satisfy both PCI and privacy laws.

Handling Risks is as Important as Finding Risks

Once you've identified risks associated with cardholder data, too many vendors provide minimal guidance or require a huge investment in professional services to develop response plans. This is because most data security solutions have poor guidance or remediation capabilities and are focused purely on offering visibility and risk assessments. However, without an automated set of comprehensive remediation actions and integrations with other solutions, responding to data risks can be manual, complicated, and require a lot of cross-functional effort.

Implement Monitoring and Assessments as a Step Towards Continuous Compliance

PCI-DSS 4.0 encourages a move toward continuous security rather than one-time compliance. Monitoring and assessments will not yield successful results or help the next audit, as modern IT operations are dynamic and data is in constant motion. This requires real-time solutions, ideally inline scanning, and performance capabilities that can scale regardless of current and future infrastructure that find issues as they appear versus at a point in time. We will discuss how to go further to achieve continuous compliance as effortlessly as possible in the last section.

Detailed Mapping of PCI-DSS 4.0 for Data, Security and Teams

PCI-DSS 4.0 Section	Requirement	How to Address
3.2.1	Account data storage is kept to a minimum through the implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. • Limiting data storage amount and retention time to that which is required for legal regulatory, and/or business requirements. • Specific retention requirements for stored account data that define the length of the retention period and include a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	**Borneo automates the workflows and steps to delete unnecessary data collected, but data anonymization by redacting the entities as defined by PCI-DSS is also an action that can be taken.**
3.3	Sensitive Authorization Data (SAD) is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process	**Borneo can identify inadvertently kept SAD and take the necessary steps to automatically determine the retention period and then automatically take steps to delete this data as necessary**

3.4	Access to displays of full Personal Account Numbers (PAN) and the ability to copy PAN is restricted. This includes both display but also copying or relocation of PAN data.	**Borneo can not only detect PAN across any data type, including any unstructured data, and identify when it is stored on potentially unauthorized systems, but also builds and automatically executes remediation workflows to:** 1. Mask data as defined by 3.4.1 2. Make changes to access controls for copy of data, especially when remote, as defined by 3.4.2
3.5	The primary account number (PAN) is secured wherever it is stored.	**Borneo can determine when data is exposed and identify these risks, but also based on policy build can automatically execute remediation workflows to make the data secure and unreadable as necessary, including:** 1. Tokenization of the Data 2. Encryption of Data
6	Develop and Maintain Secure Systems and Software	**While this is primarily focused on software and development, as developers copy data sets or move them across different (cloud) storage repositories for developing and testing individual components, the potential for exposed data becomes higher. Borneo can identify sensitive data and data ownership to improve data stewardship of any data used in the development and testing of these software systems as defined by section 6.**
7	Restrict Access to System Components and Cardholder Data based on Access Rules	**Borneo leverages integrations with identity systems and automatically combines that with effective data masking to obfuscate PCI data from individuals who need access to some, but not all data contained in an institution's system based on job function.** **Other solutions make copies of manually specified data to assess risk. Borneo is the only solution that can perform in-memory scanning of data in real time and does not introduce unnecessary data exposure and costs by making copies.**

A3.2.5.1	Discovery scans identify account data, including data flows. This primarily is focused on clear text but applies to other data types as well.	**Borneo can identify the primary account number as well as other sensitive data on all its supported file formats. This includes unstructured data of any kind. More importantly, it is unnecessary to do periodic scanning as a Borneo is a real-time**
A3.2.5.2	Once account information has been discovered (in clear text) or unexpectedly, remediation steps must be taken and verified.	**Borneo's Data Risk Remediation platform is the only solution to provide remediation workflows and playbooks that can be executed automatically by the appropriate team. Verification becomes instantaneous rather than through a later snapshot of the current state (i.e. determination of removed data).**
8.6.2	Passwords/passphrases are not hard coded in scripts, configuration/property files, or bespoke and custom source code	**Borneo can automate the Defined Approach Testing Procedure 8.6.2.b by monitoring all data sources in real time and identifying any passwords or passphrases.**
12.5.2	PCI DSS scoping validation, including identifying all locations where account data is stored, processed, and transmitted:	**Borneo's PCI data identification solution can detect Primary Account Numbers in unexpected places, such as an error log or memory dump file.**
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident:	**Borneo's models can be used to measure exposure through accurate data classification. Identify impacted PCI, data subjects, and compromised data in the event of a security incident for reporting under the GDPR.**
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data:	**Borneo identifies all PCI data entities and can generate a report specifying which entity type has been located in the data.**

Achieving Continuous Compliance

Remediating data risks quickly is essential for achieving continuous compliance because it minimizes the window of vulnerability that can lead to non-compliance with standards like PCI-DSS 4.0. When risks are identified and addressed swiftly, you reduce the likelihood of data breaches or other security incidents that could trigger audits, fines, or reputational damage. This proactive approach also ensures that your security controls remain aligned with regulatory requirements, preventing gaps that might otherwise lead to non-compliance over time.

Furthermore, quick remediation demonstrates a commitment to a strong security posture, which can streamline the compliance process during audits. It allows your organization to maintain up-to-date documentation and evidence of corrective actions, showing auditors that risk management processes are effectively enforced. By continuously monitoring, identifying, and remediating risks, you create a feedback loop that supports not only compliance but also long-term data security resilience. The bottom line is investing in a data security solution with a focus on remediation is critical to improving current compliance requirements, but also improve your overall security posture to not only prevent a successful breach but also achieve continuous compliance.

Borneo Data Risk Remediation Platform Built to Achieve Continuous Compliance for Today's Organizations

Built by practitioners for practitioners, Borneo's Data Risk Remediation Platform provides a unified data security solution focused on delivering continuous remediation for organizations seeking to comply with regional regulations focused on protecting PII, ensuring privacy and robust security, such as the PCI-DSS 4.0. By enabling organizations to simplify and automate the tasks for meeting the requirements of regulatory agencies with a high degree of accuracy, Borneo enables organizations to automatically take the necessary steps to protect sensitive data in hours or days versus weeks or months. Through Borneo's ability to remediate data risks in real time, organizations can achieve continuous compliance.

Having built from the ground up to support multi-cloud architectures, leverage AI to automate manual tasks, and provide accurate remediation steps based on integrations across cloud, data warehouses, and SaaS applications,

To learn more about how Borneo can eliminate your data risks and help you streamline compliance with PCI-DSS 4.0, please contact us at info@borneo.io, visit our website at https://borneo.io, or visit us on LinkedIn and X.

