DataBee™ | COMCAST TECHNOLOGY SOLUTIONS

DataBee™ continuous PCI solution brief

Fast-track PCI DSS 4.0 readiness using ready-made dashboards for a unified compliance view

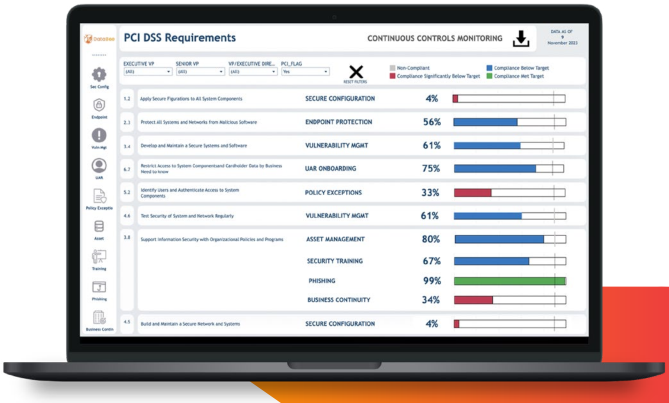
Digital wallets and payments are becoming a popular choice over traditional options. As a response to evolving enterprise payment tools and processing methods, the Payment Card Industry Data Security Standard (PCI DSS) has introduced compliance requirements to address new security and privacy challenges. PCI DSS 4.0, published in 2022, outlines specific time frames for consistent and repeatable security measures in response to technological advancements. Now organizations are facing a ticking clock — the first round of requirements for PCI DSS 4.0 goes into effect on March 31, 2024, with the full set of requirements following the next year on March 31, 2025.

Although most organizations have basic PCI controls in place, many find themselves struggling to develop cybersecurity protections for threats, coordinate and perform a targeted risk analysis, and update logical access controls. With PCI DSS 4.0, ten of the main requirements have added controls focused on documenting and assigning roles and responsibilities for compliance.

A consistent, accurate dataset providing reports based on management structures that identify process owners and business managers can save money and time as organizations seek to comply with PCI DSS 4.0's rigorous requirements.

Achieve continuous PCI preparedness with DataBee

DataBee™ provides continuous controls monitoring (CCM) capabilities with dashboards aligned to the PCI DSS 4.0 compliance framework. With DataBee, organizations have data-driven insights into audit risk through continuous monitoring and robust, easily accessible reporting. By weaving and enriching multiple data sources into security data fabric, DataBee enables operational managers, risk management, and internal audit functions to collaborate and report on the same contextualized insights derived from data they trust.



PCI DSS Requirements

CONTINUOUS CONTROLS MONITORING

DATA AS OF 9 November 2023

EXECUTIVE VP: (All) | SENIOR VP: (All) | VP/EXECUTIVE DIRE...: (All) | PCI_FLAG: Yes

1.2	Apply Secure Figurations to All System Components	SECURE CONFIGURATION	4%
2.3	Protect All Systems and Networks from Malicious Software	ENDPOINT PROTECTION	56%
3.4	Develop and Maintain a Secure Systems and Software	VULNERABILITY MGMT	61%
6.7	Restrict Access to System Componentsand Cardholder Data by Business Need to know	UAR ONBOARDING	75%
5.2	Identify Users and Authenticate Access to System Components	POLICY EXCEPTIONS	33%
4.6	Test Security of System and Network Regularly	VULNERABILITY MGMT	61%
3.8	Support Information Security with Organizational Policies and Programs	ASSET MANAGEMENT	80%
		SECURITY TRAINING	67%
		PHISHING	99%
		BUSINESS CONTINUITY	34%
4.5	Build and Maintain a Secure Network and Systems	SECURE CONFIGURATION	4%

For organizations seeking to achieve PCI DSS 4.0 compliance, DataBee's integration with management hierarchy data enables a consistent and accurate view of control compliance and ownership. By identifying process owners and business managers, you can create a culture of compliance accountability with robust and data-driven actionable reports based on management structure, reducing confusion about who in the organization is responsible for improving compliance. The predefined dashboard views and reports empower business managers by providing them data necessary to comply with the enterprise security policy with the ability to drill down into details about the people and assets they manage. DataBee applies organization hierarchy data to various other inputs identified with PCI tags, including vulnerability management scans, device inventories, phishing test results, and endpoint detection and response (EDR) tool data.

DataBee normalizes and maps security data to the Open Cybersecurity Schema Framework (OCSF) using patented entity correlation logic and asset owner discovery tools. The enriched dataset is sent to your data lake of choice where it can be easily tapped for insights and enabled for data sharing.

DataBee automatically identifies and connects data, empowering all three lines of defense with access to real-time, year-round, proven-at-scale CCM dashboards for visibility into compliance trends and actionable insights using industry-leading visualization tools — Tableau and Power BI.

DataBee's continuous PCI features

Single pane of glass with dashboards and reports for operational managers, risk management, and internal audit functions

Prebuilt and customizable PCI dashboards that automatically identify and connect data required to assess compliance and controls aligned to your business policies and standards

Layered dashboards and real-time reports based on management structure, enhancing communication and collaboration by identifying process owners and business managers

Year-round insights for real-time and historical controls and compliance trends

Robust and actionable reporting that eliminates point-in-time compliance and spreadsheets

Comcast governance, risk, and compliance (GRC) consulting services to accelerate your security data maturity journey

Enhanced communication throughout the compliance lifecycle — from defining controls objectives to evaluating controls implementation, ensuring accountability, and monitoring controls effectiveness

PCI DSS requirement	DataBee report
Apply secure configurations to all system components (#2)	Secure configuration
Protect all systems and networks from malicious software (#5)	Endpoint protection Vulnerability management
Develop and maintain secure systems and software (#6)	Vulnerability management
Restrict access to system components and cardholder data by business need to know (#7)	User access reviews
Identify users and authenticate access to system components (#8)	Policy exceptions
Log and monitor all access to system components and cardholder data (#10)	Security logging and monitoring, and log retention and normalization
Test security systems and networks regularly (#11)	Vulnerability management
Support information security with organizational policies and programs (#12)	Asset management Resiliency Training and phishing

Table 1: Sample of data and telemetry DataBee gathers and combines to show PCI DSS requirements

Get started with DataBee for PCI audit preparedness

The power of the DataBee security data fabric platform for CCM allows you to spend less time searching for the right data for controls and compliance reporting and more time on the quality and sustainability of controls and gaps remediation. With DataBee, you will quickly be able to:

- **Proactively understand and monitor compliance posture in accordance with internal policies, regulations, and industry standards.**
- **Continuously identify controls gaps and refine metrics.**
  Establish controls baselines and continuously test and measure against targets to prioritize critical remediations.
- **Create a culture of compliance accountability through data transparency and trust.**
  Automatically score and rescore your leaders and departments against controls standards and consistently track their performance trends over time.
- **Save time on audit preparedness.**
  Provide fast compliance answers with evidence of adherence to security controls, policies, and procedures.
- **Improve security operational efficiency and save money.**
  Eliminate the need for labor-intensive manual security data mapping and maintenance efforts.
- **Provide actionable remediation insights and prescriptive resolutions to address gaps and guard against threats.**
  Instruct leaders exactly where there are gaps and recommend how to close them.

Find out more

Are you ready to take advantage of an enterprise-scale security data fabric with continuous controls monitoring capabilities? Let's talk.
Request a custom DataBee demo | comca.st/databee

DataBee | COMCAST TECHNOLOGY SOLUTIONS

©2023 Comcast Technology Solutions