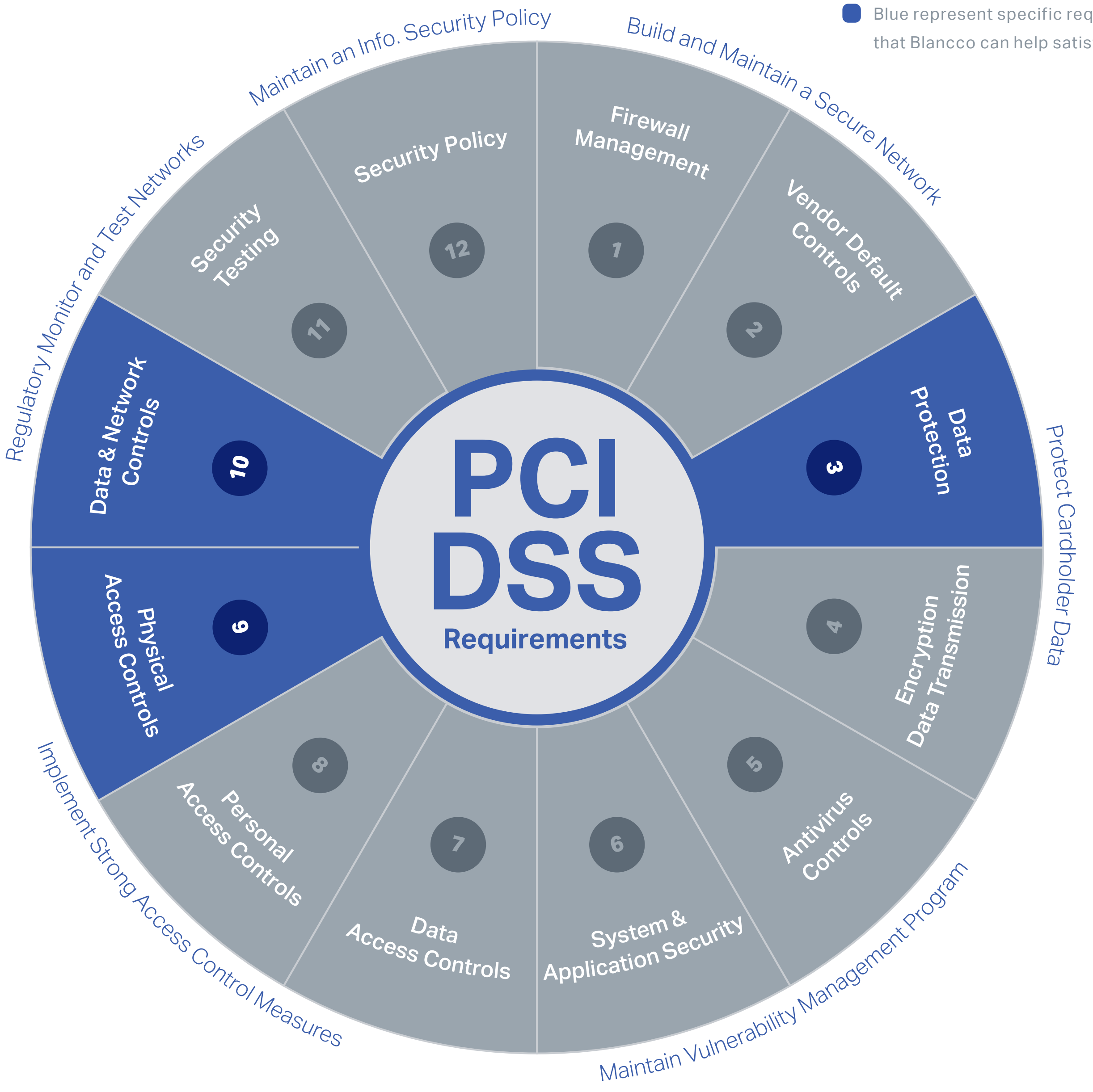
blancco

Which PCI DSS Requirements Do Blancco Solutions Satisfy?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintained in a secure environment. This includes all banks, finance service providers, retailers, restaurants, hotels and online service providers, among others.

Blancco addresses a number of requirements within PCI DSS with our data erasure solutions. Here are those requirements, the specific Blancco solutions that address them and how they are satisfied with Blancco.

🟦 Blue represent specific requirements that Blancco can help satisfy.



PCI DSS Requirements

Build and Maintain a Secure Network

1 Firewall Management

2 Vendor Default Controls

Protect Cardholder Data

3 Data Protection

4 Encryption Data Transmission

Maintain Vulnerability Management Program

5 Antivirus Controls

6 System & Application Security

Implement Strong Access Control Measures

7 Data Access Controls

8 Personal Access Controls

9 Physical Access Controls

Regulatory Monitor and Test Networks

10 Data & Network Controls

11 Security Testing

Maintain an Info. Security Policy

12 Security Policy

Requirement 3: Protect Stored Cardholder Data.

PCI DSS V3.2 REQUIREMENT	BLANCCO SOLUTION(S)	HOW SOLUTION SATISFIES REQUIREMENT:
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention	• Blancco File Eraser • Blancco Virtual Machine Eraser • Blancco LUN • Blancco Drive Eraser	Blancco Data Erasure solutions go a step beyond the deletion requirements listed here by securely and permanently erasing data from a variety of mediums, including laptops, drives, live environments and virtual machines. Blancco solutions enable programmatic processes by automating data erasure according to policy and requirement. **Specific Examples:** Blancco File erasure supports this PCI requirement with scripting and scheduling. Merchants can erase private credit card data on a regular, ongoing basis to ensure and prove compliance with erasure reports. Additionally, our erase-report-audit process keeps organizations' stored, unnecessary data to a minimum. Blancco File is supported by Blancco Virtual Machine Eraser and LUN Eraser in virtual machine, active storage and hypervisor environments. Blancco Drive Eraser supports full erasure of private data on HDDs and SSDs once those devices reach end-of-life.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely	• Blancco File Eraser • Blancco Virtual Machine Eraser • Blancco LUN Eraser • Blancco Drive Eraser	Blancco erasure products support cryptographic erasure techniques (when they exist) and can also apply additional erasure processes to increase the security when data is no longer needed or cannot be kept. **Specific Examples:** Blancco File Eraser can be used to erase files carrying credit card data in a Windows or a Unix environment, while Blancco Virtual Machine Eraser supports this process by erasing data on hypervisor layers within virtual machines without disruption to business operations. Blancco LUN Eraser allows organizations to erase data in active storage environments while allowing the operating system to remain intact, and Blancco Drive Eraser support erasure of data from HDDs and SDDs at end of life.

Requirement 9: Restrict Physical Access to Cardholder Data.

PCI DSS V3.2 REQUIREMENT	BLANCCO SOLUTION	HOW SOLUTION SATISFIES REQUIREMENT:
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	• Blancco File Eraser • Blancco Virtual Machine Eraser • Blancco LUN • Blancco Drive Eraser	Blancco erasure products meet the requirements for Clear and Purge as prescribed by the National Institute of Standards and Technology (NIST) 800-88. All data erasures are certified by 100% tamper proof reports.

Requirement 10: Track and Monitor Network Access.

PCI DSS V3.2 REQUIREMENT	BLANCCO SOLUTION	HOW SOLUTION SATISFIES REQUIREMENT:
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived or restorable from backup).	• Blancco Management Console	Blancco Management Console allows you to manage data erasure across all IT assets within a single program for consolidated reporting. Every time a data erasure is performed, a report is created and stored for compliance, audit, reporting, verification and retention purposes.

For over 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations like PCI DSS.

We support the need for heavily-regulated industries' to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Contact us today for additional information about how we can help you pass your next data security audit.

For more information about Blancco Technology Group, please visit our website at www.blancco.com.