DATABANK

COMPLIANCE SOLUTIONS

PCI COMPLIANCE

MITIGATE RISK WITHOUT COMPROMISING PERFORMANCE

Payment Card Industry Data Security Standards sets the worldwide information security standards for credit card transactions to help control and minimize points of risk for fraud or compromise of sensitive information. In order to be compliant, retailers and other organizations must adhere to a rigorous set of standards for handling credit card data.

Achieving and maintaining compliance can be a challenge, requiring specialized knowledge, controls, infrastructure, and reporting that may not be attainable using internal resources for all organizations. As incidents of customer data theft continue to rise, it's especially critical to take additional precautions by investing in monitoring and management to keep customer information safe. Partnering with DataBank can simplify compliance through our comprehensive approach that allows your organization to manage risks and threats.

WHAT DOES PCI COMPLIANCE MEAN FOR MY ORGANIZATION?

IT APPLIES IF YOU ARE:

- A retailer operating your own on-premises or self-hosted Cloud ecommerce solution
- A single brick and mortar retailer, or operating multiple locations, and processing credit card transactions – no matter what volume

WHICH MEANS THAT:

- You must comply with 250+ sub-requirements across the 12 main categories for PCI-DSS 3.2
- Risk mitigation is easier to achieve by hosting your applications on a PCI compliant, QSA attested hosting platform within a PCI-DSS compliant data center.

Achieving and Maintaining Compliance With DataBank

Achieving compliance starts with your internal IT staff. The process should cover an assessment or gap analysis of your systems, remediation (should you find vulnerabilities), and submitting a report to the banks you do business with.

As a PCI-DSS compliant data center provider, DataBank can help you clear these obstacles efficiently and effectively. Our facilities and infrastructure are issued an annual Report on Compliance (RoC), indicating we have met or exceeded all audit controls. DataBank designs our platforms and operational processes to address as much as 80% of compliance control management, compared to 20% for many other service providers. This is why some of the largest publicly traded companies in the world turn to DataBank for PCI compliance.

The DataBank approach is consultative, proactive, and delivered by experts, which simplifies the process of staying up to date with PCI regulations, helping achieve and maintain compliance without adding staff or sacrificing IT system performance.

DATABANK

PCI COMPLIANCE CHECKLIST

LAYERED DEFENSE | CONTINUOUS MONITORING | PROACTIVE UPDATES | EXPERT GUIDANCE

Firewalls

- Only allow necessary traffic to enter your CDE
- Dynamic packet filtering
- Maintain a secure zone for any card data storage
- Document all firewall policies and procedures, including business justification for each port or protocol allowed through firewalls

Antivirus Software

- Maintain audit logs for review
- Document malware procedures and reviewing with necessary staff
- Examine system configurations and periodically evaluating malware threats to your system

Restricting Physical Access

- Keep physical media secure and maintain strict control over any media being moved within the building and outside of it
- Destroy media in a way that prevents reconstruction
- Maintain a list of all devices used for processing
- Train all employeesto inspect devices for tampering

Custom Passwords

- Enable only one primary function per server
- Use VPN technologies for web-based management
- Implement a system configuration and hardening guide

Sustain Secure Systems

- Maintain a change management process
- Maintain a process to keep up-to-date with the latest identified security vulnerabilities and their threat levels
- Install and maintain vendor-supplied security patches on all system components

Logging and Reporting

- Maintain a process to respond to anomalies or exceptions in logs
- Maintain processes and procedures to review logs and security events daily, as well as review system components defined by your risk management strategy
- Maintain audit logs that track every action taken by someone with administrative privileges

Safeguard Cardholder Data

- Document data retention policies
- Track all employee acknowledgement of training and understanding of policies
- Eliminate storage of sensitive authentication data after card authorization

Limit Cardholder Access

- Maintain a written policy that details access to cardholder data based on defined job roles and privilege levels
- Maintain access controls on any systems where cardholder data is stored and transmitted
- Maintain access controls to only allow authorized parties and denying all others without prior approval or access

Scans and Tests

- Maintain scheduled and consistent internal and external vulnerability scans
- Maintain change detection tools with alerts for unauthorized modification of critical content files, system files, or configuration files
- Perform critical file comparisons

Encryption of Cardholder Data

- Verify that encryption keys/ certificates are valid and trusted
- Perform ongoing review and implementation of best practices, policies, and procedures for sending and receiving payment card data
- Continually check the latest encryption vulnerabilities and update as needed

Unique identifiers

- Disable all remote access accounts when not in use
- Monitor all remote access accounts used by vendors, business partners, and IT support personnel
- Maintain a multi-factor authentication solution for all remote access sessions

Maintaining Policy

- Maintain incident response plan in the event data is compromised
- Document a policy for engaging with third-party providers, obtaining a written agreement acknowledging responsibility for the cardholder data they possess, and having a process for engaging new providers

HIPAA HITECH Compliant

FedRAMP

PCI

AICPA SOC

www.databank.com | 800.840.7533

Data Centers | Colocation | Connectivity | Cloud & Hybrid Solutions | Managed Services