



Payment Card Industry Compliance Services

A CTI Security Advisory Service

PCI SERVICES

The key to consumer confidence, economic stability, business security, and growth.

The PCI Security Standards Council (PCI SSC) is an open global forum launched in 2004 to develop, maintain, and manage standards for credit card merchants and payment applications.

Their Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all organizations that process, store, or transmit credit card information maintain a secure environment.

WHO MUST MEET PCI COMPLIANCE

PCI standards apply to all organizations or merchants that store, process, or transmit cardholder data, regardless of size or number of transactions.

SERVICE OVERVIEW

Requirements for PCI Compliance

There are four levels of PCI compliance requirements, based on the volume of transactions.

All merchants are required to be compliant with the PCI DSS, which includes regular monitoring and testing of their networks. Level 1 merchants processing greater than \$6 million are subject to annual audits by a Qualified Security Assessor (QSA) and require an annual Report on Compliance (ROC). Other exceptions may apply if deemed necessary by the acquiring bank. In addition, any merchant with e-commerce must also complete a vulnerability scan by an Approved Scanning Vendor (ASV).

PCI DATA SECURITY STANDARD

| HIGH LEVEL OVERVIEW | |
|--|---|
| Build and maintain a secure network | 1. Install and maintain firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks |
| Maintain vulnerability management program | 5. Use and regularly update anti-virus software programs 6. Develop and maintain secure systems and applications |
| Implement strong access control measures | 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and process |
| Maintain information security policy | 12. Maintain policy that addresses information security for all personnel |

MEETING PCI STANDARDS

Level of compliance and the applicable PCI standards are often confusing to organizations and can certainly leave them guessing. Do their processes and controls meet the standards? And, more importantly, what falls under the scope of PCI? For example, if an organization has only one or two credit card terminals, but its network includes multiple locations with virtual servers, is the whole network within scope?

CTI can provide the answers. Our process begins with a gap assessment to determine proper network segmentation for effectively and efficiently managing what is in scope for your PCI audit. We then review your network architecture and controls and provide feedback on problem areas to prepare you for a successful audit.

MEETING PCI STANDARDS (cont.,)

For organizations that require an audit, we are able to perform audits using the current PCI DSS protocol, and provide you with a Report on Compliance (ROC) and Attestation of Compliance (AOC).

CTI is a Qualified Security Assessment Company (QSAC). That makes us experienced, qualified experts in meeting the requirements for all your Payment Card Industry Data Security (PCI DSS) initiatives.

MEET YOUR PCI MONITORING REQUIREMENTS

CTI PCI SERVICE HIGHLIGHTS

- Expert advice and guidance to understand and meet PCI requirements
- Scoping assessments to ensure proper segmentation to minimize PCI costs and risks
- Gap assessments to review network architecture and controls to identify impediments for successful audits
- Penetration testing
- Internal/external vulnerability scans
- Thorough audit against current PCI DSS by a team of Qualified Security Assessors (QSAs)
- Report on Compliance (ROC)
- Attestation of Compliance (AOC)

LOG MONITORING, ANALYSIS & ALERT MANAGEMENT

Enterprises can generate millions of log alerts every day, making the recognition and analysis of meaningful alerts in real-time a complicated, resource-consuming challenge.

Today, security teams already struggle to stay focused on simply managing resource bandwidth. But there's a solution that can put you in control.

CTI security monitoring solutions, managed by our team of certified security analysts, offer the focus and expertise required to meet your objectives in place, on point, 24/7. That means peace of mind, and the time and resources to concentrate on your business goals.

PCI IS A CONTINUOUS PROCESS



ABOUT CTI

CTI solves business problems by providing services spanning business advisory, technology, and advanced analytics. We help companies envision, design, implement and manage complex data-centric business solutions. Our approach is to understand your business strategy before evaluating how data can strengthen your goals. We focus on producing meaningful insights from your data asset. We expose those insights, embedding them into your business processes while guiding user adoption for a more data-driven culture.

CONTACT US

CTI is located in Burlington, Mass., serving customers in New England, Metro New York, Metro Atlanta, and beyond.

Corporate Office:

78 Blanchard Road
Suite 304
Burlington, MA 01803
Tel: 781-273-4100
800-932-4249
Fax: 781-273-7351