

Outsourcing PCI Compliance

Selecting the Right Service Provider to
Achieve and Maintain PCI Compliance

Whitepaper

Datapipe Managed IT Services

www.datapipe.com

877-773-3306

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is an evolving set of security requirements designed for entities that store, process, or transmit cardholder data. These entities must maintain a secure Cardholder Data Environment (CDE). Compliance with PCI DSS is a sound business practice that also serves to keep sensitive data secure.

As a business grows and conducts an increasing number of annual credit card transactions, it is subject to increasingly complex compliance requirements.

PCI validation requirements are currently organized into four levels which are explained in detail on Visa's web site (http://usa.visa.com/merchants/risk_management/cisp_merchants.html).

Achieving compliance in-house requires a significant level of expertise, and maintaining compliance quickly becomes resource intensive. As a result, outsourcing PCI compliance solutions to managed service providers has become a popular business trend in recent years. An increasing number of businesses outside the payment card industry are also deploying PCI DSS solutions across the enterprise to meet a range of industry requirements.

However, not all PCI DSS service providers deliver a comprehensive compliance solution. In fact, many solutions fail to meet a majority of compliance requirements. For example, some third-party service providers offer services that meet basic security requirements such as ASV scans and antivirus, but their compliance offerings lack advanced security controls such as Web Application Firewalls (WAF), log management, and two-factor authentication.

A comprehensive solution is more than just hardware or software solutions. Achieving and maintaining PCI DSS compliance requires specialized skills and experience that only a few providers can deliver. The right provider will also offer the resources and expertise necessary to accommodate company growth and scale a PCI DSS solution. When selecting a certified service provider look for one with a deep understanding of the specific requirements of PCI DSS, demonstrated expertise in secure network architecture (including proper network segmentation to reduce the number of system components considered in-scope), and security service design and implementation.

It is essential that the service provider deliver a transparent service agreement which clearly defines both the client's and the provider's responsibilities. This ensures that all aspects of the standard are addressed and there are no gaps in responsibility. The organization or merchant that is storing, processing, or transmitting the cardholder data is ultimately liable for any gaps in compliance, which makes it imperative to clearly delineate who is responsible for each aspect of meeting the PCI DSS standard.

As a Visa certified Level 1 PCI service provider, Datapipe’s PCI solution provides industry-proven methodologies and best-of-breed security service offerings. Datapipe’s **high-performance security services include:**

- Patch management
- Intrusion Detection Systems (IDS)
- Anti-malware protection
- Vulnerability assessment
- File Integrity Monitoring (FIM)
- Auditing assistance
- Intrusion Prevention Systems (IPS)
- Log management
- Real time system configuration assessment
- Web Application Firewalls (WAF)
- File encryption
- Transparent Database Encryption (TDE)
- Two-factor authentication
- Advanced Change control

Datapipe delivers the resources, expertise, and services to help established and growing companies achieve compliance and maintain a secure Cardholder Data Environment.

PCI Compliance — An Overview

The Payment Card Industry Data Security Standard (PCI DSS) is an evolving set of requirements designed to ensure that all organizations and merchants that process, store, or transmit credit card information maintain a secure Cardholder Data Environment (CDE). The standard is administered and managed by the PCI Security Standards Council (PCI SSC), an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

Companies that fail to protect consumer credit card data experience serious repercussions including fines and lawsuits.

Complying with the PCI DSS is mandatory but also serves as a sound business practice to keep sensitive data secure. Security measures that are implemented to comply with the standard ensure that consumer account data is safeguarded from theft and identity fraud. Companies that fail to protect consumer credit card data experience serious repercussions including fines and lawsuits from non-compliance, as well as revenue loss, brand damage, and decreased market share due to customer dissatisfaction. Major credit card companies also reserve the right to prohibit the offending merchant from processing credit cards altogether.

The PCI standard organizes compliance requirement levels according to the number of credit card transactions a merchant processes annually. For example, Visa’s merchant level designations place merchants into one of four levels based on Visa transaction volume over a 12-month period.

Level ¹	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region ²	<ul style="list-style-type: none"> • Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”) • Quarterly network scan by Approved Scan Vendor (“ASV”) • Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire (“SAQ”) • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"> • Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"> • Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer

¹ – Compromised entities may be escalated at regional discretion

² – Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exception may apply to global merchants if no common infrastructure and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.

The other major credit card brands maintain similar criteria. Further details are available on their respective websites.

http://www.mastercard.com/us/sdp/merchants/merchant_levels.html

<http://discovernetwork.com/fraudsecurity/disc.html>

The Case for Outsourcing

Companies often underestimate the time, resources, and efforts required to continuously and rigorously maintain compliance in-house. Security systems require significant capital investments in hardware and software and are costly to implement, maintain, and monitor. Outsourcing to the right provider enables businesses to achieve and maintain compliance while controlling costs.

Other companies turn to outsourcing because their current business volume has outgrown existing compliance resources. As illustrated in the chart above, merchants are subject to increasingly complex compliance requirements as the annual number of credit card transactions processed grows. Meeting those requirements becomes extremely resource intensive which makes outsourcing an attractive option.

Outsourcing to the right provider enables businesses to achieve and maintain compliance while controlling costs.

Managed services providers offer a range of PCI solutions and services for businesses seeking to outsource compliance. These providers offer a deeper level of expertise and experience in PCI compliance than most businesses typically have in-house. Depending on their clientele, a service provider may have experience working with Level 3 or Level 4 validation requirements only, or they may have a stronger range of experience from serving clients who are subject to Level 1 or Level 2 audits. Expertise and security credentials will also vary among providers. While most service providers can deliver basic security controls, many lack the specific knowledge or advanced expertise required to architect and properly manage a complex PCI DSS compliant solution.

PCI solution offerings will vary depending on the service provider. Some just offer the tools necessary to meet a few aspects of compliance rather than a complete fully managed solution that achieves and maintains PCI compliance. These differences are not always readily apparent, but often come to light upon close examination of the provider's service agreement. If the service provider fails to clearly define which PCI requirements are being met *and* who is responsible to meet them (the provider and/or the client), a business may falsely believe they are compliant simply because they purchased a PCI toolbox. Although automated tools are one step toward meeting compliance, several PCI DSS requirements demand careful vigilance and analysis to continuously interpret logged data. Providers who do not have appropriate data retention and analysis components in their PCI DSS solution fail to enable their clients to meet PCI requirements.

The next section of this white paper defines the criteria that companies should look for in a PCI service provider and also explores Datapipe's PCI solution as an example of a provider delivering best-practice processes and controls to ensure PCI DSS compliance.

Service Provider Selection Criteria

As illustrated above, not all PCI service providers or compliance solutions are the same. This is an important point because it determines liability. If consumer data is compromised and a mandatory forensic investigation by the card brands reveals that the PCI solution was in a compliant state, the company will not be fined for the security breach. Choosing the right provider is paramount in ensuring compliance requirements are met.

Deep Knowledge of the PCI DSS

Choose a provider with deep understanding of the PCI standard and its specific requirements. Many companies today offer solutions and services that do not adequately meet the requirements of the current version of the PCI standard, so it is unlikely these providers will be able to manage compliance as subsequent versions of the standard are released. One way to assess the prospective provider's knowledge level is to ask how many Level 1, on-site audits they have undergone. An additional consideration is how many PCI ISA-certified members they have on-staff. ISA certification requires qualifications equivalent to that of a Qualified Service Assessor (QSA). These are two key indicators that the provider's staff possesses a solid working knowledge of the PCI DSS.

Proven Expertise

An experienced PCI DSS solution provider will demonstrate expertise in network architecture and implement sound security designs to help achieve compliance. This expertise should be grounded in industry recognized security certifications which should include, PCI ISA, CISSP, CISA, CISM, MCSE: Security, and CEH. Achieving and maintaining PCI compliance is mission critical. Therefore the provider should take the time to gain an in-depth understanding of your overall business before proposing a solution. The most knowledgeable and best qualified providers can help devise compensating controls if a company's business requirements conflict with PCI DSS requirements.

If consumer data is compromised and an audit reveals that the PCI solution was correctly deployed, the company will not be fined for the security breach.

Compliance Reporting Assistance

The right provider has procedures and mechanisms in place to generate the critical information and data required for clients to complete significant portions of the Self Assessment Questionnaire (SAQ) and/or the on-site audit process which is involved in evidence collection for a Report on Compliance (ROC).

Clearly Defined Responsibilities

It is best to find a provider that offers transparency into their operations and a clear definition of responsibilities to ensure the client and the provider clearly understand who is responsible to meet each aspect of the PCI DSS. These responsibilities should be specifically outlined in all service agreements relating to the PCI DSS solution delivered by the managed services provider.

Administrative Controls

Choose a provider that demonstrates excellence in administrative controls, including sound policies, procedures, and workflow to ensure compliance is being met. A qualified provider is audited regularly by reputable outside auditors and demonstrates adherence to comprehensive change control policies and procedures. Administrative controls are especially vital for maintaining a hardened security stance. The right provider defines and implements a coordinated process to address the discovery, identification, remediation, and prevention of security threats that can increase risk and endanger ongoing compliance.

Positioned for Growth

The capital expenditures required for an in-house PCI compliant infrastructure can be prohibitive. In addition to equipment expenses, there is a substantial cost to hire, train, and retain qualified security staff to deliver continuous monitoring.

Choose a provider that is positioned to scale your compliance solution with the growth of your company.

This is a solid reason to choose to outsource. But it does not make sense to outsource to a provider that can't support the growth of your company in the long-term. Look for a PCI service provider that can demonstrate a proven ability to deliver constant attention and analysis regardless of what merchant level your business reaches. The right provider is positioned to scale with the growth of your company and meet the demands of increasingly complex PCI solutions. Review the resources and experience level of your current provider - are they ready to support a Level 1 or Level 2 solution?

PCI Certified Facilities

PCI certified facilities are an important, but sometimes misunderstood, part of PCI compliance. Some companies mistakenly believe that because their solution is hosted in a *secure* data center, their solution must be PCI compliant; however, this may not be the case. For example, PCI DSS Requirement 9.1.1 dictates that security video must be retained for 90 days. Not all data centers or hosting facilities comply with this requirement. Be sure your provider's facilities are PCI Certified.

At the same time, it's important to remember that your business is not PCI compliant simply by locating your servers or IT infrastructure in a PCI Certified facility. PCI requirements go well beyond the physical infrastructure that servers are housed in and the right provider will clearly communicate any limits of their facility's certifications.

The Datapipe Solution

Datapipe is a Level 1 PCI DSS Validated Service Provider offering a solution set based on industry-proven methodologies and best-of-breed service offerings. As one of the first Level 1 certified providers, Datapipe's security professionals have a deep level of experience and knowledge of PCI DSS and its specific requirements in security and network architecture. Datapipe's security experts hold leading security certifications including CISSP, CISA, CISM, MCSE: Security, CEH, ISA, and Security+. Datapipe is a PCI SSC Participating Organization, and plays an active role in helping to define protection strategies for cardholder data and determine the future of the standards setting process. Datapipe has broad experience with clients from a range of industries who require solutions to meet even the most complex PCI requirements.

Datapipe delivers the resources and expertise to scale with a growing company.

Datapipe's service agreement clearly defines the responsibilities of all parties in ensuring compliance. Their standard agreement assigns responsibility for each component of the PCI DSS and these roles are explained during the initial client consultation process. Datapipe's consultative approach with clients ensures that PCI DSS requirements are clearly understood prior to implementation. Their team of experts provides full lifecycle support which enables clients to realize even greater value from their compliance solution investment. Datapipe delivers the resources, expertise, and the following built-in processes and high-performance security services to enable merchants to achieve and maintain PCI-DSS compliance at any merchant level:

Patch Management

Security patches provide fixes to known software vulnerabilities. Datapipe's patch management solution provides notification, identification, testing, and deployment of operating system, application, and network device patches in accordance with the PCI specification. Datapipe delivers real-time notification of newly published security bulletins, patch testing, scheduled remediation, and verified deployments of supported applications and operating systems. When vulnerabilities are discovered, and a patch becomes available, Datapipe automatically takes action in accordance with pre-defined criteria including installation scheduling, configuration changes, and rebooting if necessary.

Intrusion Detection Services

An Intrusion Detection System (IDS) monitors and detects malicious network activity that can compromise computer system security. Datapipe provides a dedicated team of trained IDS experts that analyze real-time attack data and events. When a threat notification is received, an incident ticket is created for investigation and escalation when necessary. Datapipe's solution utilizes a network based

intrusion detection system that receives a copy of all network traffic from a span port on your own dedicated switch removing the possibility of a single point of failure.

Intrusion Prevention Services

An Intrusion Prevention System (IPS) is used to monitor, detect, and block malicious traffic while allowing legitimate traffic to pass unhindered. Datapipe delivers maximum host-level protection using non-intrusive network traffic reconstruction, protocol analysis, and patented sandbox technology to detect and block 'zero-day' attacks that bypass standard signature-checking solutions. Since implementation, this approach has successfully stopped every remote intrusion.

Anti-malware Protection

Malware is software designed to infiltrate or damage a computer system for malicious purposes and includes viruses, worms, rootkits, key loggers and trojans. Datapipe's anti-malware tools detect and quarantine malware and then immediately contact Datapipe Security via email and central console alerts. Datapipe's security professionals then follow a client's individualized incident response plan for appropriate escalation procedures.

Vulnerability Assessment

Because remote hackers frequently try to exploit network vulnerabilities, Datapipe's vulnerability assessment service identifies known security vulnerabilities and assists in prioritizing threats for remediation. Datapipe delivers rapid, accurate, and non-intrusive scanning and can cross-check vulnerabilities against a comprehensive, up-to-date vulnerability database. Datapipe's services proactively protect against new and emerging threats with real-time updates and detailed remediation guidance which future-proof sensitive data and harden security risk posture.

Managed Firewall

Firewalls are security devices that position a security layer between computer networks and the Internet by restricting inbound and outbound flows based on specific rule sets. Datapipe offers dedicated firewall appliances with custom-tailored policies that permit or deny network traffic based on compliance standards and business needs. The firewall also enables network segmentation to isolate the Demilitarized Zone (DMZ) from the internal network as well as other Virtual LANs (VLANs).

Web Application Firewall

Security flaws in web applications are one of the greatest attack vectors utilized by attackers today. As such, a Web Application Firewall (WAF) serves as a critical line of defense against a multitude of threats such as injection and cross-site scripting. Datapipe's WAF is deployed as an in-line proxy loaded directly into the web server. The WAF inspects all web traffic, including encrypted traffic, for known and unknown attacks, and then blocks the threats in real time.

Transparent Database Encryption

Datapipe delivers Transparent Database Encryption (TDE) for column level encryption and decryption of sensitive data in a manner completely transparent to the web application. This alternative is provided if an application is not currently using encrypted cardholder data—particularly if a client’s past provider or in-house team lacked the expertise or source code to add encryption.

Two-factor Authentication

Two-factor authentication provides an extra layer of security identification that uses two different authenticating factors (something you have, something you are, and something you know) to verify a user’s identity to a system. Datapipe's VPN solution dictates that access is granted only upon successful authentication of two factors - something you have and something you know. Datapipe's service combines traditional password authentication with certificate authentication as the second factor. Requiring a second factor of authentication significantly increases system security by removing the risk of unauthorized access using a compromised password. In keeping with this best practice, Datapipe's internal remote management systems and data center access systems require a minimum two-factor authentication.

Continuous Audit

At Datapipe, client solutions are evaluated and hardened against industry-standard benchmarks, such as the PCI DSS, for operational, regulatory, and security policy compliance. Datapipe also provides archived log protection and verifiable integrity as an important aspect of PCI compliance and as a way of helping clients manage the time and labor-intensive process of compliance maintenance. File and system integrity monitoring further strengthen this service, and real-time alerts are generated if settings or files are altered to endanger compliance or if servers deviate from hardening baseline security policies. Comprehensive reporting is also included to demonstrate the current state of compliance and serve as feedback to ensure only authorized changes are being performed.

Audit Assistance

Datapipe's audit assistance service provides the relevant policies and data evidence that clients require to satisfy PCI DSS requirements. Evidence collected also serves as an opportunity for clients to evaluate their configuration for potential changes. PCI DSS requires an annual validation process, which is satisfied in part with a ROC or SAQ. The determination is made based on annual transaction volume and acquiring bank requirements. If the hosted solution requires an SAQ, Datapipe can provide the information necessary to help complete the questionnaire. If a QSA has already audited policies and procedures, a hosting provider’s ROC may help answer the SAQ or contribute evidence of policies and procedures to a QSA when creating a ROC. Sometimes, a QSA audit eliminates the need for

Datapipe can enable a remote assessment with a QSA for major cost savings over an on-site assessment.

an on-site assessment, even if a business falls into compliance Level 1. Datapipe can enable a remote assessment with a QSA for major cost savings over an on-site assessment.

Event Management

Event Management is the process of transmitting, storing, analyzing, correlating, and issuing security alerts based on log data. Some providers claim to offer event management; however, few provide an offering comprehensive enough to fully cover compliance requirements. Datapipe offers real-time log management, behavioral analysis, and compliance management in a single solution. An event collector agent or syslog daemon forwards events to an event collector appliance in real time. Datapipe retains these records for at least one year, with a minimum of three months online availability.

Advanced Change Control

Change control describes the procedures followed throughout the change lifecycle to ensure that all change requests are documented, assessed for impact, approved, and tested. Datapipe provides the necessary internal procedures required to document and enforce change control in a regulated, secure environment. Datapipe follows the four change control procedures as outlined by PCI DSS specifications, including document impact and rollback procedures, receive management approval, and operational testing.

Conclusion

As businesses seek to thrive in a digital economy, safeguarding consumer credit card data has become mission critical. PCI DSS provides a set of guidelines to protect cardholder data and minimize the risks of a security breach. Selecting the right provider to enable achievement and ongoing compliance with PCI DSS is critical. With broad expertise in delivering turnkey security solutions, a deep understanding of PCI DSS specifications, and industry leading security tools, Datapipe is uniquely positioned as the right provider to help secure sensitive data to maintain business integrity.

About Datapipe

One of the first service providers to achieve Level 1 PCI Certification, Datapipe is an active member of the PCI Security Standards Council. PCI-ISA and CISSP-certified professionals designed Datapipe's PCI solution based on industry-proven methodologies and best-of-breed service offerings to help merchants and other businesses meet their PCI requirements. As a key element of its turnkey solution, Datapipe employs a unique, consultative approach with clients to ensure that the dual requirements of PCI DSS are clearly understood prior to implementation. In-depth experience with both small business and enterprise level clients from a range of industries enables Datapipe to architect complex solutions for companies to achieve and maintain PCI compliance. Datapipe's physical security and policies and procedures meet or surpass PCI requirements and are audited annually by a Qualified Security Assessor. Clients can also leverage Datapipe's Report on Compliance to fulfill on-site audit requirements.

For more information about Datapipe, please visit <http://www.datapipe.com/>.