



# Leveraging your Hosting Service Provider to Achieve Compliance

INDUSTRY WHITE PAPER

## Executive Summary

*Businesses with access to sensitive data are acutely aware of the many compliance requirements placed on them. From Sarbanes Oxley to HIPAA, from PCI DSS to the Financial Privacy Act, compliance spans almost every American industry and organization. Outsourcing IT environments to a third party hosting provider who prioritizes customer compliance support is a powerful way to address the many mandates in existence today. However, not every hosting provider has this capability. In fact, if a hosting provider doesn't have proper controls in place, they can actually jeopardize compliance for their clients.*

*This white paper showcases how a hosting provider can assist with compliance. It also provides a methodology for evaluating different hosting providers to determine which ones are capable of supporting and simplifying the compliance process.*

## Background

The Internet age has brought great advances in the way we conduct our business and personal lives. Today, a medical expert can consult with patients and even examine data-intensive medical records nearly instantaneously from hundreds of miles away. Or, in a matter of hours, not only can a business establish an online presence, but they also can sell and accept payment for products to consumers across the globe. As amazing as these advances are, they also bring with them some unfortunate consequences. For example, information transmitted across the internet is susceptible to interception by unintended recipients. This ability to electronically breach security and access confidential consumer data has led to a new age of government regulation.

Failure to protect consumer data can have devastating financial consequences and adversely affect a company's brand equity. The Ponemon Institute estimates the cost of data breach at \$214 per record based on a recent survey of American companies. A few recent examples:

**Sony**—A security breach in April 2011 resulted in hackers gaining access to proprietary information for over 70 million Sony PlayStation Network and Qriocity accounts. Once Sony discovered the breach on April 19, they were forced to

shut down services to their customers for almost a month until the security issues could be corrected to prevent future breaches. While the final impact may not be known for years, the immediate impact is quite clear: massive amounts of negative publicity from media coverage across the globe; internal resources diverted to damage control and cleanup; class action lawsuits in excess of \$1 billion as well as lost revenue for the amount of time service was shut down, plus free game time given to impacted users are all part of the price being paid.

**Alliance Data Systems (Epsilon Division)** – Unauthorized access to electronic records at Epsilon resulted in millions of email addresses being stolen - one of the largest data security breaches in history. Epsilon manages email marketing campaigns for companies such as Best Buy, Target and CitiGroup. Although personal information such as credit card numbers or social security numbers were not stolen, it's expected that scammers will attempt phishing campaigns on the stolen emails seeking to obtain credit card and other personally identifiable information.

What's the bottom line? These days consumers must entrust their proprietary information to businesses. The businesses, in turn, must protect consumers' data. The Federal government has developed myriad regulations to ensure businesses do just that. There are many examples of Federal government regulation across all kinds of industries: HIPAA for the healthcare industry; the Financial Privacy Act for the financial services industry; PCI for credit card transactions; Sarbanes-Oxley for public companies and many others.

Savvy business managers know that compliance with internal and external requirements and regulations can be costly and time-consuming. That's why leveraging all available resources to reduce the impacts of compliance is vital. One of those potential resources is a hosting provider.



# Leveraging your Hosting Service Provider to Achieve Compliance

Some hosting providers are beginning to understand the critical importance of compliance and are taking steps that result in a simplified compliance process for their clients.

This white paper focuses on data privacy and how to determine whether a particular hosting provider will be a help or hindrance in meeting compliance guidelines. Data privacy provides an example of compliance that is relevant to nearly every type of industry as well as foreign and domestic businesses. To help explain data privacy and the regulations that relate to it, we will reference the guidelines established by the Payment Card Industry Council Data Security Standard (PCI DSS). While other regulatory environments such as HIPAA also focus on data security, PCI DSS is generations ahead of HIPAA and many other data privacy related regulations.

## What is PCI DSS?

PCI DSS version 2.0 is the current global data security standard adopted by the major payment card brands that applies to all organizations—regardless of size or number of credit card transactions—that store, process or transmit cardholder data. PCI DSS provides a framework for developing robust security processes. Compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

GOAL	PCI DSS REQUIREMENT	PROVIDER SUPPORTED
<b>BUILD &amp; MAINTAIN A SECURE NETWORK</b>	<ul style="list-style-type: none"> <li>» 1. Install and maintain a firewall configuration to protect cardholder data</li> <li>» 2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>	<ul style="list-style-type: none"> <li>» 1. Available</li> <li>» 2. No</li> </ul>
<b>PROTECT CARDHOLDER DATA</b>	<ul style="list-style-type: none"> <li>» 3. Protect stored cardholder data</li> <li>» 4. Encrypt transmission of cardholder data across open, public networks</li> </ul>	<ul style="list-style-type: none"> <li>» 3. No</li> <li>» 4. Available</li> </ul>
<b>MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM</b>	<ul style="list-style-type: none"> <li>» 5. Install and maintain a firewall configuration to protect cardholder data</li> <li>» 6. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>	<ul style="list-style-type: none"> <li>» 5. Available</li> <li>» 6. No</li> </ul>
<b>IMPLEMENT STRONG ACCESS CONTROL MEASURES</b>	<ul style="list-style-type: none"> <li>» 7. Restrict access to cardholder data by business need to know</li> <li>» 8. Assign a unique ID to each person with computer access</li> <li>» 9. Restrict physical access to cardholder data</li> </ul>	<ul style="list-style-type: none"> <li>» 7. No</li> <li>» 8. No</li> <li>» 9. Yes</li> </ul>
<b>REGULARLY MONITOR &amp; TEST NETWORKS</b>	<ul style="list-style-type: none"> <li>» 10. Track and monitor all access to network resources and cardholder data</li> <li>» 11. Regularly test security systems and processes</li> </ul>	<ul style="list-style-type: none"> <li>» 10. No</li> <li>» 11. No</li> </ul>
<b>MAINTAIN AN INFORMATION SECURITY POLICY</b>	<ul style="list-style-type: none"> <li>» 12. Maintain a policy that addresses information security for all personnel</li> </ul>	<ul style="list-style-type: none"> <li>» 12. Yes</li> </ul>

Table 1 Source: *Payment Card Industry Security Standards Council, PCI DSS v2.0, October 2010*



# Leveraging your Hosting Service Provider to Achieve Compliance



Although organizations of all sizes are impacted by PCI DSS, the way in which compliance is demonstrated varies by the number of transactions that an organization processes. Very large organizations that process over 6 million transactions per year as well as those organizations who have experienced a data breach have the highest proof of compliance which includes an annual on-site assessment by a Qualified Security Assessor (QSA), a quarterly network scan by an Approved Scan Vendor and an Attestation of Compliance. At the other end of the spectrum, for companies processing less than 20,000 transactions per year, Level 4 merchants simply have to complete an annual Self-Assessment Questionnaire (SAQ), a quarterly network scan as determined by the SAQ, and any other compliance requirements required by the merchant's acquirer. Regardless of the level, all merchants are expected to maintain compliance with PCI DSS.

## How Does a Hosting Provider Fit into the PCI Compliance Equation?

By outsourcing an IT environment to a hosting provider two key aspects of data security become the responsibility of that provider:

1. Physical control and security over the data center and everything inside it
2. Processes, policies and procedures that are used to operate the data center

As described earlier in Table 1, PCI DSS has twelve different requirements that must be met in order to be in complete compliance. A hosting provider with proper controls in place should be able to provide to its clients a document called a PCI Report on Compliance (PCI ROC). The PCI ROC results from an audit by a Qualified Security Assessor and represents the firms' opinion that the hosting provider has met the PCI Data Security Standard requirements. This document will directly support a client in meeting the criteria for the following two of the twelve different PCI DSS requirements:

### **PCI DSS Section 9 - Restrict Physical Access to Cardholder Data**

- As the title states, this requirement addresses physical security. Any physical access to data or systems that contain cardholder data provides an opportunity for individuals to remove that data and must be restricted. This refers to employees of the client company, the hosting company and any other clients of the hosting company.

Means of addressing this section include utilizing multiple levels of physical security such as badge readers, biometric scanners, video surveillance and restricting access only to those areas which are authorized for each client or employee.

### **PCI DSS Section 12 - Maintain a Policy that Addresses Information Security for All Personnel**

- Having an information security policy that informs personnel what is expected of them and sets the security tone for the business is essential for this section. This section addresses employees of the client business as well as employees and contractors of the hosting provider business who might have access to the cardholder data environment. Other areas may also be supported based on the services that are purchased.

## Evaluating a Hosting Provider's Ability to Support Compliance Objectives – Audit Reporting

Any hosting provider has the opportunity to have their processes audited by an independent auditing firm and provide the audit results to its clients. By doing so, the hosting provider demonstrates its commitment to clients by having independent verification of their own policies and processes. The resulting audit report provides clients with an objective view into the effectiveness of the providers' methodologies.

The audit results explain the effectiveness of a hosting provider's processes. Although providers appear on the outside to be similar, each has its own set of methodologies that are used to operate key infrastructure (power, HVAC, security, network and physical access). In some cases the methodology is an unwritten set of rules that are loosely followed. In other cases, processes and procedures exist but aren't well documented or consistently applied. Although any firm can have their methodologies audited, only providers that have controls in place that are: 1) documented and consistently used in operation of the data center, 2) suitably designed to meet the objectives, and 3) operating effectively can assist its clients in meeting their compliance objectives.

The PCI ROC was specifically designed to address PCI DSS compliance and is an important audit tool for hosting providers to have for the broad array of clients that must follow its guidelines. Most other compliance arenas do not have an audit report that is as direct in addressing client compliance.



# Leveraging your Hosting Service Provider to Achieve Compliance

Prior to June 15, 2011, the most common audit used to determine whether a hosting provider had proper controls in place was the Statement on Auditing Standards (SAS) 70 report. Before this date, SAS 70 Type 1 and Type 2 audits were the best available option for use in confirming the operational controls of a hosting service provider. By providing a client with the auditors' SAS 70 report, a client enterprise could utilize the report content to support general internal and external compliance requirements.

Unfortunately, SAS 70 controls were not adequate for evaluating operational compliance of a hosting provider. With its roots embedded in financial compliance, SAS 70 was overextended in its use for evaluating hosting operational controls. Furthermore, it did not require

management to make any kind of affirmative statement that the business had effective controls in place. Recognizing the deficiencies in SAS 70 and seeking to provide a stronger means to obtain assurance over compliance and operations, the American Institute of Certified Public Accountants (AICPA) developed a new reporting framework for service auditors (CPAs). The new framework enables auditors to examine and opine on internal controls for service organizations. This allows them to provide clarity and greater transparency to its customers on both its controls relevant to financial reporting as well as its controls relevant to their IT system attributes such as security, availability, processing integrity, confidentiality and privacy. Referred to as Service Organization Control reports, there are three different reporting options illustrated in the following table:

	SOC 1	SOC 2	SOC 3
<b>PURPOSE</b>	<ul style="list-style-type: none"> <li>» Report on controls relevant to user entities' internal control over financial reporting.</li> </ul>	<ul style="list-style-type: none"> <li>» Report on controls for security, availability, processing integrity, confidentiality and privacy.</li> </ul>	<ul style="list-style-type: none"> <li>» Report on controls for security, availability, processing integrity, confidentiality and privacy.</li> </ul>
<b>DISTRIBUTION</b>	<ul style="list-style-type: none"> <li>» Restricted to existing user entities and their auditors.</li> </ul>	<ul style="list-style-type: none"> <li>» Generally restricted use.</li> </ul>	<ul style="list-style-type: none"> <li>» General use. Can be used by current and prospective customers (SysTrust Seal for web site).</li> </ul>
<b>DETAIL</b>	<ul style="list-style-type: none"> <li>» Type 1 – A report on management's description of the organization's systems and suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.</li> <li>» Type 2 – Same as type one except that it also evaluates whether the controls were operating effectively over a specified time period.</li> </ul>	<ul style="list-style-type: none"> <li>» Type 1 – A report on management's description of the organization's systems and suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.</li> <li>» Type 2 – Same as type one except that it also evaluates whether the controls were operating effectively over a specified time period.</li> </ul>	<ul style="list-style-type: none"> <li>» A SOC 3 report is the same as SOC 2 except the service auditor's tests of controls are excluded from the report.</li> </ul>
<b>MANAGEMENT STATEMENT</b>	<ul style="list-style-type: none"> <li>» Affirmative statement by management is required for fair presentation and design of controls (Type 1) or fair presentation, design and operating effectiveness of controls (Type 2).</li> </ul>	<ul style="list-style-type: none"> <li>» Affirmative statement by management is required for fair presentation and design of controls (Type 1) or fair presentation, design and operating effectiveness of controls (Type 2).</li> </ul>	<ul style="list-style-type: none"> <li>» Affirmative statement by management for fair presentation and design of controls.</li> </ul>

While a SOC 1 is necessary to support financial statement audits, SOC 2 and SOC 3 reports are relevant for providing information and assurance on IT system attributes and hence very applicable reports for a hosting service provider.

Table 2 Source: AICPA



# Leveraging your Hosting Service Provider to Achieve Compliance



The key differences between a SOC report and a SAS 70 report are as follows:

1. **Written Assertion by Management** – Management will now be required to provide a written assertion in the SSAE 16 report supporting their system's description. This assertion must include the suitable criteria used for management's assessment.
2. **More Inclusive Description of the Service Organization's System** – In addition to the controls description, it must also include a description of the services provided and classes of transaction processed; a description of the procedures by which services are provided; a description of the process for capturing and addressing other significant events and conditions; and a description of the process for preparing reports and providing information to customers.
3. **Clear Identification of Risks that Threaten the Achievement of Stated Control Objectives** – In a SOC report, service organizations must identify the risks that threaten the achievement of the control objectives and evaluate if the described controls would provide reasonable assurance that those risks would not prevent the control objectives from being achieved.

## Evaluating a Hosting Provider's Ability to Support Compliance Objectives - Dedicated Compliance Support

Audit reports are only a portion of the compliance solution that a hosting provider can provide to benefit clients in their efforts to meet compliance objectives. By having a dedicated compliance department, a hosting provider demonstrates that compliance support is a high priority supported by an expert with responsibility for executing against a compliance plan. When compliance is one among several responsibilities of a product or operational manager, support of client compliance issues can receive insufficient attention. A dedicated team can help clients address compliance issues, concerns and questions in a way that a part-time resource cannot.

## Key Takeaways

There are a few key points that are important for businesses to consider in evaluating data center providers and their ability to support their clients' compliance objectives:

1. **Nearly every business has compliance issues.**  
Businesses that operate within healthcare or financial services industries and those businesses that accept payment for goods or services via credit cards most definitely have some level of regulatory compliance that they must consider.
2. **Compliance can be a complex and expensive undertaking, but it can be simplified if your hosting provider can demonstrate that they have proper operational controls in place.**
3. **Hosting providers with proper controls in place can help in meeting compliance objectives. Those that do not have proper controls in place can actually put a business' compliance objectives at risk.**
4. **Validate that your hosting provider has proper controls in place by obtaining a copy of their SOC and PCI reports. If they do not yet have a SOC report, obtain a copy of their SAS 70 report and confirm that they will produce a future report in accordance with the AICPA standards.**
  - a. Clients conducting international business should also confirm that their hosting provider's report follows SSAE 16 as well as ISAE 3402 standards.
5. **Closely scrutinize hosting providers that rely on outdated SAS 70 reports or do not utilize any type of compliance audit. The most likely reasons for not adapting a SOC audit are:**
  - a. Management's unwillingness to affirmatively state that they have adequate processes and controls in place
  - b. Internal belief that the additional rigor provided by SSAE 16 will result in a negative audit opinion
6. **Question prospective hosting providers to determine the extent of their internal resources devoted to supporting and assisting with client compliance needs. A lack of a dedicated compliance resources is a signal that future client compliance issues may receive inadequate attention.**



# Leveraging your Hosting Service Provider to Achieve Compliance

## Conclusion

The ongoing burden of compliance is only going to grow over time. The time and expense of maintaining compliance can be daunting, especially for small to medium sized firms with limited resources dedicated to compliance. However, by utilizing a third party hosting provider that is capable of addressing their compliance needs, the process of compliance is actually simplified for their clients.

The key issues of physical security and security policy are already addressed by the hosting provider thus reducing the administrative, human and financial resources that would otherwise be required by businesses attempting to internally host their IT environments or host them with non-SOC audited providers.

## About ViaWest

ViaWest has archived PCI DSS sections 9 and 12 compliance for specific data center locations. ViaWest has obtained a dual-standard Service Organization Controls 1 (SOC 1) Type 2 report. The report and accompanying audit was conducted in accordance with the AIPCA's replacement for the SAS 70 standard, SSAE 16, and the international assurance standard ISAE 3402. ViaWest has obtained the SysTrust seal for service organizations on the Trust Services Principals and Criteria, also known as a SOC 3 report.

ViaWest is one of the largest privately held data center service providers in North America. They provide colocation, complex hosting, cloud and managed services to businesses of all sizes nationwide. ViaWest owns and operates 22 enterprise-class data center facilities in Colorado, Texas, Oregon, Utah, and Nevada, delivering high-quality, flexible solutions designed to support customers' unique business needs. For additional information on ViaWest, please visit [www.viawest.com](http://www.viawest.com) or call 1-877-448-9378.