

White paper:

# PCI compliance: A technology overview

**Alan Shimel**

Chief Strategy Officer  
StillSecure®

**Alan Ferguson**

Vice President  
Coalfire Systems®

July 2009



## Table of contents

I. INTRODUCTION.....	3
II. PROVEN PCI MANAGEMENT PRACTICES.....	3
<i>Limit the scope of the PCI environment</i> .....	4
<i>PCI embedded in an overall security program</i> .....	4
<i>PCI compliant policies, procedures, and training</i> .....	5
<i>The need for reporting</i> .....	5
III. PCI AND APPLICABLE INFO-SECURITY TECHNOLOGIES .....	6
IV. STILLSECURE SOLUTIONS – HELPING DRIVE COMPLIANCE .....	12
V. THE IMPORTANCE OF AN AUDIT .....	14
VI. CONCLUSION.....	15
<i>About StillSecure</i> .....	15
<i>About Coalfire Systems</i> .....	15

### **Alan Shimel**

*Chief Strategy Officer, StillSecure®*

As Chief Strategy Officer, Alan Shimel brings a wealth of entrepreneurial experience to his role with StillSecure. Mr. Shimel was most recently SVP of Sales and Business Development of Cachier, a manufacturer of network acceleration appliances. Prior to that, Mr. Shimel was VP of Business Development of Interliant and, in a little more than 3 years, was instrumental in forging relationships and strategic partnerships with such industry players as Dell Computer, Verisign, Microsoft, IBM, Cisco and EMC. He was also a key team member as Interliant acquired 27 companies and completed a successful IPO. A pioneer in the Internet industry, Mr. Shimel was one of the founders of Tri Star Web, a NYC based, early participant in Web hosting. After building Tri Star Web to a multi-million dollar revenue run rate, he sold it to Sage Networks, which later became Interliant. Mr. Shimel is a graduate of St. Johns University with a Bachelor of Arts in Government and Politics, and holds a JD degree from NY Law School.

### **Alan Ferguson**

*Vice President, Coalfire Systems®*

Mr. Ferguson guides Coalfire's sales and marketing team and account management practices. Prior to co-founding Coalfire, he served as Vice President of Centera Information Systems, a leading e-commerce and systems integration firm with clients throughout North America, Europe and Asia. Under his leadership, Centera was repeatedly recognized by Deloitte & Touche as a Fast 50 award winner recognizing companies with superior revenue growth. Mr. Ferguson began his career with IBM, and he has more than 25 years experience in delivering information technology solutions to enterprise and government clients. Under Mr. Ferguson's sales and marketing management, Coalfire has grown rapidly and has successfully delivered more than 500+ IT audit and information security engagements to public and private companies and government clients throughout North America.

[www.stillsecure.com](http://www.stillsecure.com)

All rights reserved. Copyright © 2002-2009 StillSecure®. Confidential © 2009 StillSecure®.

## I. Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) has received widespread praise for its specificity. Where other information security standards, such as HIPAA and GLBA, shy away from spelling out required measures and procedures, the PCI standard is straightforward. Service providers and merchants are given direction on the technologies, policies, and procedures needed to achieve compliance. However, as many service providers and merchants can attest, PCI compliance is not easy or turn-key. It requires extensive thought, planning, and execution.

Even though the standard provides clear guidance, a PCI compliance program can differ considerably for Level 1 merchants and those at levels 2, 3, and 4. As such, detailing the steps required to achieve compliance for an affected organization requires a rigorous approach. The right mix of technologies and procedures is highly dependent on the organization's size, function, and operational approach. This paper provides the background necessary to accurately assess your PCI needs.

*"PCI can't be simply tacked onto an existing security program or appended to normal IT operations. Compliance is a complicated process to achieve and maintain—it must be managed proactively."*

This paper interprets the PCI standard from a management and technical perspective. It presents a number of proven management practices that save time and money if incorporated into a PCI compliance program early on. It maps each of the 12 PCI requirements to the specific security technologies and policies that facilitate compliance. The paper closes with an introduction to the StillSecure® suite of security product solutions and managed services, which provide many of the PCI-required basic and advanced security functions: firewall, gateway anti-virus, intrusion detection/prevention, network access control, VPN, and vulnerability management among others. It should be noted that any specific technology compliance must be validated relative to the specific implementation.

## II. Proven PCI management practices

The PCI management practices presented in this section are drawn from the co-author's extensive PCI-audit experience. As a Vice President with Coalfire Systems®, a PCI Qualified Security Assessor (QSA), Mr. Ferguson has participated in dozens of PCI audits for a range of merchants and service providers. Alan Shimel, Chief Strategy Officer for StillSecure, is a noted expert in the field of network security and a prominent speaker on best practices and compliance.

Merchants and service providers that follow the practices presented below are in a better position to achieve compliance. Managing a PCI compliance program is an organization-specific activity. It must be tailored to the unique way each merchant or service provider conducts business. The following practices apply to all affected organizations regardless of industry, size, or complexity of the network.

## Limit the scope of the PCI environment

Almost every functional area within an organization is dependent on network resources. Yet only a portion of the business is involved with the storage or processing of payment card transaction data. PCI compliance is greatly facilitated by architecting (or re-architecting) the network to consolidate all transaction processing functions on a single network segment. PCI-affected devices can then be readily isolated from the rest of the network. This can be easily made possible by adding routers and firewalls to isolate the transaction processing piece of the network. Also, the use of wireless technology within the cardholder data environment can greatly increase the scope of compliance and audit.

There are a number of benefits to doing so:

- **Risk reduction** — Chances of data being compromised are substantially reduced. It is much easier to control and track access to one network where transactions are being processed rather than the entire network. In most business environments, the majority of network users have no need to access such systems, so limiting exposure is an important best practice.
- **Simplification** — Isolating transaction-related systems simplifies management and audits. The need to scour the entire network in search of PCI-affected devices is eliminated; thus, isolating and reporting on a specific device or subset of devices is greatly simplified. An excellent example of this is to segment any wireless networks away from the transaction processing piece. Wireless networks are inherently more vulnerable and therefore require more scrutiny during an audit. Isolating the wireless component can save tremendous time and money.
- **Compartmentalization** — Limiting the PCI environment greatly reduces the chances of a non-PCI-related issue raising a red flag with auditors. If auditors are required to scrutinize the entire network to determine PCI status, the chances increase that they will find issues with other systems. At best this can be an embarrassing distraction; at worst it can result in the organization expending considerable resources responding to issues that were initially outside the scope of the audit.

## PCI embedded in an overall security program

Merchants and service providers need to incorporate PCI in their info-security program rather than approach it as a separate, one-time activity. In short, PCI cannot be simply tacked onto an existing security program or appended to normal IT operations. Compliance is a complicated process to achieve and maintain—it must be proactively managed.

[www.stillsecure.com](http://www.stillsecure.com)

Many organizations must comply with other regulations in addition to PCI such as HIPAA, GLBA, SOX, and/or FISMA, and there are additional internal information security policies. Also, security functions are typically dispersed across the org chart. For example, the IT group may be responsible for desktops, the network group handles infrastructure, and the financial group has responsibility for its own mission-sensitive servers.

This dispersed responsibility for security complicates compliance management. To succeed, organizations should implement a corporate-level security function that has the authority to unify all disparate activities into a cohesive, centralized corporate program. To accomplish this, many organizations have created a Chief Information Security Officer (CISO) position with cross-organizational authority. PCI must be implemented at this level if compliance is to be achieved and sustained.

### **PCI compliant policies, procedures, and training**

Policies, procedures, and training are as important to PCI compliance as any technological solution. The most advanced firewall can be easily rendered ineffective if it is not governed and maintained properly. Network and security administrators must be guided by policies that embed the security standard's requirements into ongoing operational activities.

Auditors require that policies address all the relevant requirements of the PCI standard. Maintaining this documentation is critical. Auditors also verify that documented policies and procedures are actually implemented in the production environment and in daily operations. All affected staff must be trained on PCI and related policies.

The key here is that the policies, procedures, and training are specifically adapted to the organization's business. Each network is unique, and the policies and procedures governing its security must reflect this.

### **The need for reporting**

Reporting is required throughout the PCI compliance process—not only to pass an annual audit, but as a management tool. It is difficult to over-emphasize the importance of robust, comprehensive reporting. You can deploy state-of-the-art technology and develop in-depth policies and procedures, but without the ability to report, you cannot gauge the effectiveness of your program.

All security technologies deployed should have strong reporting capabilities. Management wants to know that the network is secure and that identified problems are being addressed and corrected. Reporting on vulnerability management, access attempts, attacks detected and

thwarted, system logs, etc. is needed on a continuous basis. Robust reporting provides management with the confidence they need to sign off that the network is secure.

Clear reporting is also a necessity for meeting the needs of auditors. An organization must respond to the specific reporting requests—ranging from corporate-wide overviews to specific details on individual devices, vulnerabilities, and repair histories. Being able to do so can greatly affect the direction and success of an audit.

### III. PCI and applicable info-security technologies

The PCI standard does an excellent job of specifying the info-security technologies that merchants and service providers need to consider for compliance. In general, applicable technologies fall into two categories: Standard technologies and advanced technologies. Standard technologies are those that may already be in place, but which may not be configured or managed optimally for PCI compliance. They include:

#### **Standard technologies**

- Firewall
- Antivirus
- Encryption / VPN
- Authentication
- Application-level access control
- Data back-up

Advanced technologies are powerful security applications or systems that are being increasingly mandated and adopted to defend against today's sophisticated threats. They include:

#### **Advanced technologies**

- Network access control
- Vulnerability management
- Intrusion prevention
- Patch management
- Change management
- Log management and analysis

There is a strong move afoot that both basic and advanced technologies are being outsourced to Managed Security Service Providers (MSSPs). MSSPs have the technology, resources, and processes in place to help organizations meet the stringent compliance requirements of PCI.

[www.stillsecure.com](http://www.stillsecure.com)

Furthermore, they deal with compliance issues daily with many different auditors, and are thus well versed in PCI compliance issues.

Table 1 presents these standard and advanced security technologies as they apply to each of the 12 PCI requirements. Applicable policies and procedures are also presented. Table 1 gives the reader a head-start on assessing the status of their current info-security program and provides guidance in areas where deficiencies may exist. Applicable technologies need to be validated with the specific implementation in mind.

**Table 1. PCI compliance technologies and procedures**

PCI Requirement	Technologies Standard technologies Advanced technologies	Policies/procedures	Notes/Keys for compliance
1. Install and maintain a firewall configuration to protect cardholder data	<ul style="list-style-type: none"> <li>• Firewall (network)</li> <li>• Router (network)</li> <li>• Firewall (personal)</li> </ul>	<ul style="list-style-type: none"> <li>• Connection testing</li> <li>• Firewall placement</li> <li>• Roles and responsibilities</li> <li>• Ports and protocols</li> <li>• Rule specification and review</li> <li>• Configuration standards</li> </ul>	<p>Filter inbound data and restrict access to the network core to authorized individuals. Use “default deny” permissions (rather than “default permit”) to further scrutinize inbound traffic. Segment any wireless technology away from the cardholder data environment if possible.</p> <p>Establish documentation for all ports and services utilized for business operations.</p> <p>Maintain current network diagrams.</p>
2. Do not use vendor-supplied defaults for system passwords and other security parameters	<ul style="list-style-type: none"> <li>• Network access control</li> <li>• Vulnerability management</li> </ul>	<ul style="list-style-type: none"> <li>• Pre-production modifications</li> <li>• Configuration standards</li> <li>• Removing/disabling insecure/unnecessary services, protocols and functionality</li> <li>• Encrypting access</li> </ul>	<p>The identified technologies serve as a safety net to ensure default-related best practices are followed. They can help systematically test devices to ensure that the organization is in compliance. Expanded testing is required if wireless capabilities are utilized.</p> <p>Vendor defaults (network, wireless, system, database, operating system) are inherently a business risk because access components are published and easily accessible to the public and those with malicious intent.</p>
3. Protect stored cardholder data	<ul style="list-style-type: none"> <li>• Encryption</li> <li>• Backup / data retention</li> </ul>	<ul style="list-style-type: none"> <li>• Duration of data retention</li> <li>• Data types retained</li> <li>• Display masking</li> <li>• Safe storage</li> <li>• Encryption key management</li> </ul>	<p>Restrict access to stored data and dispose of it properly (e.g., do not dispose of old tapes in the trash; limit access to only those who need it; shred old paper-based sensitive materials).</p> <p>Development of an encryption key management program is critical. Acceptable confidential data may be stored, but it must be protected at all times against unauthorized access.</p> <p>Encryption may seem like a straightforward requirement, yet many organizations do not deploy, apply, or manage encryption properly, which can dramatically diminish the effectiveness of the technology and reduce the risk of data loss.</p> <p>Organizations may need to bring in the expertise, either full-time or on a contract basis, to design and guide a PCI-compliant encryption program. Organization should run “scenarios” to ensure that they are protected from situations such as lost laptops, theft, lost back-up tapes, etc.</p>

PCI Requirement	Technologies Standard technologies Advanced technologies	Policies/procedures	Notes/Keys for compliance
4. Encrypt transmission of cardholder data across open, public networks	<ul style="list-style-type: none"> <li>• Encryption</li> <li>• VPN</li> <li>• Network intrusion detection / prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Minimum standards</li> <li>• Wireless standards</li> </ul>	<p>Cardholder information must be protected as it crosses open, publicly accessible networks, such as the Internet. If possible, segment wireless networks to reduce audit requirements. Utilize SSL or IPSEC VPNs where appropriate. Network intrusion detection / prevention solutions should be used to detect any PAN data leaving the cardholder data segment.</p> <p>The secure handling of cardholder information by commercial websites and internal employees is key. As stated in Requirement 3, seek outside assistance if this area is not a strength.</p>
5. Use and regularly update antivirus software	<ul style="list-style-type: none"> <li>• Antivirus (network)</li> <li>• Antivirus (endpoint)</li> <li>• Network access control</li> <li>• Vulnerability management</li> </ul>	<ul style="list-style-type: none"> <li>• Antivirus validation</li> </ul>	<p>Prevention is much cheaper than deferred maintenance, particularly as viruses spread and cause damage quickly. In addition to data loss and theft, viruses and malware often contribute to lowered productivity due to increased latency, network downtime and corrupted data.</p> <p>Antivirus components must be capable of operating and logging on a daily basis; they must not be modifiable by company employees.</p> <p>While not currently a requirement, anti-spyware technology is often embedded in the leading anti-virus solutions. The threat from spyware can at times be greater than viruses and other malware. Forward thinking organizations will require their anti-virus solutions to include anti-spyware.</p> <p>A good network access control solution will verify that antivirus and anti-spyware is running on connected devices and that virus definitions are up to date.</p>
6. Develop and maintain secure systems and applications	<ul style="list-style-type: none"> <li>• Vulnerability management</li> <li>• Network access control</li> <li>• Patch management</li> <li>• Change management</li> </ul>	<ul style="list-style-type: none"> <li>• Patching and patch validation</li> <li>• Vulnerability identification and management</li> <li>• Secure application development</li> <li>• Change control</li> <li>• Code reviews</li> </ul>	<p>Change management and change controls are crucial to guard against accidental as well as misinformed network changes.</p> <p>Organizations must establish sound processes for handling patch and vulnerability management.</p> <p>The development of secure application systems and components must be specified in a documented process to continually validate and remove insecure components from custom-developed code.</p> <p>Code reviews are important to validate the design and implementation as well as maintain consistency.</p>

PCI Requirement	Technologies Standard technologies Advanced technologies	Policies/procedures	Notes/Keys for compliance
7. Restrict access to cardholder data by business need-to-know	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• Application-level access control</li> </ul>	<ul style="list-style-type: none"> <li>• Need-to-know requirements</li> <li>• Role-based access</li> </ul>	<p>This prevents accidental exposure and decreases vulnerability/risk through limited distribution of data.</p> <p>Allowable access should be specified on job descriptions and within employees' functional requirements.</p>
8. Assign a unique ID to each person with computer access	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• Application-level access control</li> <li>• VPN</li> <li>• Encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication and password management</li> <li>• Employee termination</li> <li>• Vendor access</li> <li>• Password policies and procedures</li> </ul>	<p>Provides the ability to link transactions back to a specific source to establish individual accountability for actions. Procedures must be maintained on access granting, employee termination, and permissions modification.</p> <p>All users with access to the cardholder environment should have a unique username and password. Administrative accounts should be tightly controlled, and actions logged and monitored.</p> <p>Password and authentication management are also essential to limit business risks.</p>
9. Restrict physical access to cardholder data	<ul style="list-style-type: none"> <li>• Physical security controls</li> </ul>	<ul style="list-style-type: none"> <li>• Facility entry control</li> <li>• Visitor site access</li> <li>• Media storage</li> <li>• Media distribution</li> <li>• Media inventory</li> <li>• Media destruction</li> </ul>	<p>If a machine is physically reachable/accessible, security risk increases significantly.</p> <p>All access to the cardholder environment must have adequate physical security controls to reduce the business risk of exposure. Often organizations choose to house key information technology systems in secure outsourced data center facilities. Any wireless access points should be physically secured.</p> <p>The destruction of media within the cardholder environment, both physical (fax, printed documents) and electronic (hard drive, backup tapes) must be managed in such a way to ensure that cardholder information is permanently destroyed.</p>
10. Track and monitor all access to network resources and cardholder data	<ul style="list-style-type: none"> <li>• Log management and analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Audit requirements</li> <li>• Audit trail specifications</li> <li>• Audit management and controls</li> <li>• Archive management</li> </ul>	<p>The organization must ensure that logging is enabled on all devices within the cardholder environment, according to the data retention (legal, regulatory) needs of the organization. The PCI council's recent revision has dramatically emphasized this area.</p> <p>Logs must be reviewed on a daily basis to identify and resolve problems expeditiously. Technology automation and outsourcing in this area are virtually required in order to fulfill this requirement.</p>

PCI Requirement	Technologies Standard technologies Advanced technologies	Policies/procedures	Notes/Keys for compliance
11. Regularly test security systems and processes	<ul style="list-style-type: none"> <li>• Network access control</li> <li>• Vulnerability management</li> <li>• Network intrusion detection/prevention</li> <li>• Host-based intrusion detection/prevention</li> <li>• Log management and analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Testing security measures</li> <li>• Vulnerability scanning and management</li> <li>• Penetration testing</li> <li>• File change monitoring</li> </ul>	<p>A periodic security assessment for all networked components within the cardholder environment must be conducted to identify and close information security gaps.</p> <p>The organization should deploy an intrusion detection/prevention system to identify and terminate potentially suspicious or malicious events. Regular network vulnerability scanning needs to be conducted along with network and application based penetration tests. An on-going program to find any rogue wireless networks must be implemented.</p> <p>File integrity monitoring of systems within the cardholder environment should be enacted to identify any unauthorized changes to systems outside of the change management process.</p>
12. Maintain a policy that addresses information security for employees and contractors	<ul style="list-style-type: none"> <li>• Network access control</li> <li>• Vulnerability management</li> <li>• Intrusion detection/prevention</li> </ul>	<ul style="list-style-type: none"> <li>• PCI compliance policy</li> <li>• Risk assessment</li> <li>• Policy review and updating</li> <li>• Daily policy enforcement</li> <li>• System usage</li> <li>• Roles and responsibilities</li> <li>• Employee training</li> <li>• Third-party adherence to policies</li> <li>• Incident response</li> </ul>	<p>Information security policies to address all business risks should be developed.</p> <p>Risks to the business should be addressed within the process and updated on an annual basis.</p> <p>Roles and responsibilities for oversight and monitoring should also be established. Outsourced service providers are often a source of help and support for incident handling and 24x7 monitoring.</p> <p>The organization should implement an incident response policy, complete with responsibilities and a process flow to identify and classify incidents and then take adequate remediation steps to limit business risk.</p>

## IV. StillSecure solutions – helping drive compliance

StillSecure has helped numerous organizations comply with PCI and other info-security regulations. StillSecure product solutions and managed security services provide PCI Compliance coverage for 8 of the 12 top-level PCI requirements and dozens of specific sub-requirements, as shown in Table 2.

*"...the basic and advanced security technologies in the StillSecure suite of solutions allow organizations to meet 6 of 12 top-level PCI technology requirements...."*

A detailed matrix mapping PCI sub-requirements listed in Table 2 to specific StillSecure products and services is available on our web site at [www.stillsecure.com/pci/matrix.php](http://www.stillsecure.com/pci/matrix.php). A hardcopy of this matrix can be downloaded at [www.stillsecure.com/PCI\\_StillSecure\\_Requirements-Solutions\\_Matrix.pdf](http://www.stillsecure.com/PCI_StillSecure_Requirements-Solutions_Matrix.pdf).

The StillSecure solution set for PCI Compliance provides merchants and processors with the basic and advanced security technologies in a number of required areas:

- Firewall (StillSecure ProtectPoint® managed services)
- Gateway anti-virus (StillSecure ProtectPoint managed services)
- Intrusion detection prevention (StillSecure Strata Guard® and ProtectPoint managed services)
- Network access control (StillSecure Safe Access®)
- Routing services (StillSecure ProtectPoint managed services)
- VPN (StillSecure ProtectPoint managed services)
- Vulnerability scanning (StillSecure VAM® and managed services)

**Table 2. Specific PCI requirements met by the StillSecure suite**

<b>StillSecure solution</b>	<b>PCI DSS requirement met</b>
<b>ProtectPoint</b>	1.1.1, 1.1.2, 1.1.3, 1.1.5, 1.1.6, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.8, 1.4, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3, 4.1, 6.1, 6.6, 8.3, 11.2, 11.3, 11.3.1, 11.3.2, 11.4, 12.2, 12.5.1, 12.5.2, 12.9.3, 12.9.4, 12.9.5, 12.9.6
<b>Safe Access</b>	1.4, 2.2, 2.2.3, 5.1, 5.2, 6.1, 12.2, 12.5.1, 12.5.2
<b>Strata Guard</b>	11.4, 12.5.2, 12.9.5
<b>VAM</b>	1.4, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3, 6.1, 6.2, 6.6, 11.2, 11.3, 11.3.1, 11.3.2, 12.2, 12.5.1, 12.5.2



StillSecure product solutions and managed services can cover a large number of the basic and advanced security technologies required for PCI Compliance. The suite of solutions is policy-driven, allowing organization-specific security policies to be configured and followed. All StillSecure products and managed services are open-standards based solutions that can share and act on data between solutions and with other systems in the IT environment – a key factor to success in any PCI compliance program. In short, StillSecure can be a key part of your PCI compliance strategy – and, work well with your other components to achieve full compliance.

StillSecure's suite of products and managed services include:

**Intrusion detection/prevention:**

**Strata Guard®** —Strata Guard is an award-winning network-based intrusion detection/prevention systems (IPS/IDS) that provides real-time, zero-day protection from network attacks and malicious traffic. Strata Guard also can be utilized in a “post-connect” NAC scenario to quarantine devices generating malicious traffic.

**Managed security services:**

**ProtectPoint™** —Best-in-class managed security services that protect you from internet attack, stopping unauthorized access and preventing worms, trojans, and viruses from taking down your network. Subscription-based ProtectPoint services deliver both the technology and the round-the-clock expertise needed to protect your network and bring you into compliance with data security policies. Services include managed intrusion detection/prevention, gateway anti-virus, VPN, content filtering, anti-spam, and many others.

**Network access control:**

**Safe Access®** —Awarded the Best Endpoint Security Solution 2008 (and 2006) by SC Magazine (and named an SC Magazine ‘Best Buy’), Safe Access protects the network by ensuring endpoint devices are free from threats and in compliance with security policies before they are allowed on the network.

**Vulnerability management:**

**VAM®** —An award-winning vulnerability management platform that identifies, tracks, and manages the repair of network vulnerabilities across the enterprise, VAM manages the vulnerability management lifecycle from end to end, mitigating the risk of network exploitation and compromise.

Compliance validation of StillSecure technologies is implementation specific. Please contact your StillSecure or Coalfire representative for assistance in ensuring that the implementation will meet PCI DSS requirements. Visit [www.stillsecure.com](http://www.stillsecure.com) to learn more about StillSecure managed services and network security products.

## V. The importance of an audit

Compliance is mandated by the PCI standard; the required methodology to validate compliance differs based on level (1-4) within the PCI hierarchy. Beyond the PCI mandate, business risk mitigation and improved security are driving principles for conducting an audit:

- Reduce the risk of unauthorized access to sensitive data
- Reduce the potential for disruption to critical IT services
- Support company image as a trusted business partner
- Provide management specific guidance for resolving vulnerabilities resulting from these services.

## VI. Conclusion

The PCI standard specifies required technologies, policies, and procedures, but each affected organization must create and govern a secure network environment according to its unique business practices. By proactively adopting compliance best-practices an organization can come into compliance with PCI quickly and efficiently.

It is imperative to complement best practices with the proper mix of security technologies. A number of technologies—such as firewalls, antivirus, authentication—may be in place, but these solutions must be configured and managed in conformance with PCI-specific policies. The PCI standard also calls out specific advanced security technologies such as a vulnerability management, network access control and intrusion prevention. StillSecure's suite of products and managed security services provide extensive coverage of the PCI standard and allow organizations to realize highest value and levels of security from their technology investments.

### About StillSecure

StillSecure delivers comprehensive network security that protects organizations from the perimeter to the endpoint. Offering both products and managed security services, StillSecure enables customers to affordably deploy the optimal blend of technologies for locking down their assets and complying with security policies and regulations. StillSecure customers range from mid-market companies to the world's largest enterprises and agencies in government, financial services, healthcare, education, and technology. For more information please call (303) 381-3830, or visit <http://www.stillsecure.com>.

### About Coalfire Systems

Coalfire Systems ([www.coalfiresystems.com](http://www.coalfiresystems.com)) is a national Compliance Auditor whose clients include the Fortune 100, banking, government, educational institutions, healthcare, and the private sector. Practice areas include:

- PCI
- Sarbanes-Oxley
- Gramm-Leach Bliley
- Forensic services
- FFIEC, FISMA, US Patriot Act
- HIPAA

For more information, visit our website or call Alan Ferguson at (303) 554-6333 x7002, [alan.ferguson@coalfiresystems.com](mailto:alan.ferguson@coalfiresystems.com).