TechTarget Windows Media

SearchWinIT.com   SearchExchange.com   SearchDomino.com
SearchWindowsSecurity.com SearchSQLServer.com   LabMice.net
SearchWinComputing.com

SearchWinIT.com E-Guide

PCI Compliance 2007—12 Mandates and how to comply

PCI Compliance, and the 12 mandates to achieve it, are a beginning. Policy enforcement and control complete the security picture. This E-Guide from Bit9 and TechTarget Windows Media Group includes informative original articles to help you navigate through the PCI compliance landscape. In the first article, the 12 mandates are defined. In the second article, focusing on PCI Compensating Controls—a deeper look at 'real world' compliance implementation can be achieved when strict adherence to the mandates is not feasible or even possible. This guide concludes with links to where you can learn more about the solutions that Bit9 provides.

Sponsored By:

SearchWinIT.com E-Guide

PCI Compliance 2007—12 Mandates and how to comply

Table of Contents:

PCI DSS Compliance: Best Practices, Worst Pitfalls

By Carol Weiszmann

Here are some do—and some don'ts—to help those needing to achieve compliance with the PCI DSS credit card security standard.

In the United States alone, the number of credit cards in circulation exceeds 1.3 billion, and as of 2004, 76 percent of Americans had at least one credit card. So it's not surprising that, according to the Federal Trade Commission, credit card fraud was the most common form of reported identity theft, accounting for 26 percent of all cases in 2005.

For credit card issuers, banks, and merchants, the costs of identity theft, fraud, and other kinds of credit card liabilities attributable to lax security reached $48 billion in 2006. This is why major credit card companies have banded together to demand that organizations accepting payment card transactions comply with the Payment Card Industry Data Security Standard—PCI DSS.

Grouped into six 'control objectives,' there are 12 controls mandated by PCI DSS:

CONTROL OBJECTIVES	COMPLIANCE REQUIREMENTS* (CONTROLS)
Build and maintain a secure network	1. **Install and maintain a firewall configuration to protect data** 2. **Do not use vendor-supplied defaults for system passwords and other security parameters**
Protect cardholder data	3. **Protect stored data** 4. **Encrypt transmission of cardholder data and sensitive information across public networks**
Maintain a vulnerability management program	5. **Use and regularly update anti-virus softwarre** 6. **Develop and maintain secure systems and applications**
Implement strong access control measures	7. **Restrict access to 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 processes**
Maintain an information security policy	12. **Maintain a policy that addresses information security**

* PCI DSS includes numerous additional sub-requirements, which can be found at www.pcisecuritystandards.org.

PCI DSS also places merchants into one of four categories based on annual credit card transaction volume, which determines the nature and frequency of assessment audits. All merchants' PCI DSS compliance must be certified by two separate external consultants. Approved scanning vendors (ASVs) perform required network scanning, and qualified security assessors (QSAs) conduct compliance assessments.

The worst pitfalls: noncompliance and complacency

Especially for smaller merchants, PCI DSS may seem complex and daunting. And it may be tempting to delay compliance. After all, the standard is new and not much seems to happen when it's ignored.

But if a noncompliant merchant's credit card data security is compromised—as is occurring with accelerating frequency to large and small merchants alike—then the penalties can be severe: fines of up to $500,000 per data-compromise incident as well as losing the ability to process credit card transactions.

What's more, the PCI DSS requirements are classic security best practices that virtually all businesses should be implementing anyway. So it's worth doing right. That can mean learning some new tricks to avoid these common pitfalls:

- Keeping too much data for too long

- Neglecting to segment the network

- Inadequate protection of stored data

- Weak passwords and/or poor password policies

- Bad logging practices

- Not paying attention to third parties

- Lack of employee training and awareness

Where to begin

Getting familiar with the PCI DSS standard (available at www.pcisecuritystandards.org) is the very first step toward becoming compliant. Next, form a project team (IT, security, legal, sales, admin, HR, etc.) that will work to identify data and transactions at risk. Then conduct an internal gap analysis and get it validated by a certified QSA, scan for vulnerabilities, and develop and implement a remediation plan.

Passing the QSA's onsite audit/assessment gains PCI DSS certification, but in order to avoid problems during ASV network scans, compliance status must be maintained.

Key best practices

PCI DSS compliance will always be a moving target. Some of the best practices currently most useful:

Expect PABP. In 2008, it's likely that Visa's Payment Applications Best Practices (PABP) will be incorporated into PCI DSS standards. Currently a set of recommendations for point-of-sale software security, PABP includes explicit testing procedures covering data retention and storage; password, application, and network security; wireless transmissions; software updates; remote access; encryption; and documentation and training.

Address exposure at the endpoint. PCs are everywhere in bank and retail environments, and they're vulnerable not only to external malware but also to data leakage from unauthorized copying to portable storage devices.

One solution is to lock down PCs to a centrally-controlled 'whitelist'—a configuration of standard software and storage devices—that cannot be modified in the field. Whitelisting audits files copied to or from PCs; stops unautho-rized software from getting onto PCs; controls access to personal storage devices (such as USB memory sticks); and blocks malware, spyware, and rogue applications and devices.

Document! Make sure records of how controls are set up, maintained, and changed are complete. PCI DSS should become internal IT auditors' reference point; this will help sustain compliance.

Train employees. Employees who handle credit card data should be trained in compliance requirements and procedures.

Get the right consultants and auditors. QSAs and ASVs must be certified by the PCI Security Standards Council. Because of the broadness of the PCI DSS standard— as well as the possibility of alternative 'compensating controls'—QSAs have wide latitude in determining compliance. In addition to conducting assessments, many also offer the remediation products and services needed to achieve compliance.

Conduct remote vulnerability scans. These should be done quarterly and cover all incoming and outgoing Internet connections, including dedicated ones handling websites and email. To stay PCI DSS compliant, the scans must be conducted by a certified ASV. Look for one with plenty of experience conducting vulnerability assessments.

Be ready for assessments. Staying PCI DSS-compliant depends on the QSA's annual assessment. Getting the business compliant can take awhile—months, even years when starting from scratch. Even with solid security policies, it's smart to seek guidance from the QSA from the beginning. Look for a QSA with expertise in auditing for all 12 PCI DSS controls as well as experience in compensating controls and the ability to recommend and, if neces-sary, implement customized solutions.

About the author:
Carol Weiszmann is a principal at aimpublications LLC (www.aimpublications.com), where she analyzes and writes about how information technologies impact business value, competitiveness, and risk.

Hitting a Moving PCI DSS Target: How Compensating Controls Can Help

By Carol Weiszmann

For some, meeting PCI DSS credit card security standards can mean completely redesigning existing systems. To ease this burden, the PCI Security Council offers compensating controls. These are not the loophole that some have suggested, but with a little help from an auditor, they can be used to make PCI compliance faster and more cost-effective.

PCI DSS—the Payment Card Industry Data Security Standard—is a work in progress. The group overseeing it—the PCI Security Standards Council—is less than a year old and its mandate is, well, gargantuan: get the world's million retailers (as well as the financial institutions and service providers that work with them) to effectively secure credit card data and transactions.

PCI DSS compliance timelines

The major credit card issuers behind PCI DSS—Visa International, MasterCard Worldwide, Discover Financial Services, American Express, and JCB—are pressuring merchants to comply, though both issuer and regional deadlines vary.

PCI DSS leader Visa has imposed a March 31 deadline for merchants handling large credit card transaction volumes (Level 1 and 2) to show they're not storing full track data, CVV2, or PIN data. Two other key Visa deadlines are approaching fast:

- September 30, 2007: Level 1 merchants must be fully PCI DSS compliant.

- December 31, 2007: Level 2 merchants must be fully PCI DSS compliant.

Experience is showing that PCI DSS compliance takes longer and costs more than initially anticipated, which probably explains why PCI DSS compliance has been lagging. Visa's own numbers indicate that as of last spring just 35 percent of its largest (Level 1) retailers were compliant, though another 51 percent have promised that they're trying. Thus Visa, for one, is offering incentives and has launched an educational campaign to speed things up. Understandably, though, PCI DSS deadlines are not quite cast in concrete.

In June, for instance, Visa and MasterCard stopped insisting that European retailers meet all of the PCI DSS standard. The emphasis is now on putting risk mitigation strategies in place. So far, European retailers have missed two deadlines for PCI compliance.

Compensating controls and the spirit of PCI DSS

One of the ways for some to accelerate PCI DSS compliance is via the standard's 'compensating controls', which, according to PCI Security Standards Council documents, "may be considered when an entity cannot meet a

requirement explicitly as stated, due to legitimate technical or documented business constraints". There are caveats, however: risks must be sufficiently mitigated.

Specifically, compensating controls, which have to be deemed sufficient and signed off on by a qualified security assessor (QSA), must

• Meet the intent and rigor of the original stated PCI DSS requirement,

• Repel a compromise attempt with similar force,

• Be 'above and beyond' other PCI DSS requirements, and

• Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

This makes implementation of compensating controls an exercise in customization. Since each one is designed for the specifics of the environment in which it's deployed, a compensating control that works in one environment may not work in any other.

A loophole? Those who argue against the effectiveness of PCI DSS in its current incarnation point to a certain squishiness in the standard in general. When, for instance the standard says, "Remove all unnecessary functionality …" it invites all sorts of interpretations of what constitutes "unnecessary". Requirement 3.6 states: "Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data …" But what, exactly, is "full documentation"?

This range of interpretation grows broader still with compensating controls, which some regard as loopholes for avoiding certain PCI requirements, notably data-at-rest encryption.

… Or a necessity? Others argue that without compensating controls, many organizations face prohibitive PCI DSS compliance costs. Compensating controls are needed so companies can leverage existing security controls toward achieving PCI DSS compliance. Why not be able to use already-deployed, perfectly proper and effective security rather than implement new controls that do not improve security simply to meet PCI DSS specifics?

Consider a retailer storing credit card data on a large IBM server running RACF security management that monitors and logs all user actions and is protected from rogue attacks by an intrusion prevention system. To become strictly PCI DSS compliant, the server-resident data would have to be encrypted. But is this necessary, or do the existing controls already sufficiently protect the data?

The need for wiggle room

There are a variety of reasons to seek the relief of compensating controls—notable among them is to achieve compliance at the retail endpoint. But topping the list is data encryption, which is difficult because it often causes problems for applications and is therefore costly. This places it at the center of much of the discussion about PCI DSS compensating controls.

Appendix B of the *Payment Card Industry (PCI) Data Security Standard Version 1.1,* (available at the PCI Security Standards Council website, www.pcisecuritystandards.org) describes several technical requirements for alternatives to the standard's encryption mandate. It is, in effect, an acknowledgement that encryption of credit card data at rest is beyond the reach of significant numbers of merchants.

Thus Appendix B describes what amounts to a different sort of perimeter around databases containing credit card data and requires that all of the following compensation control conditions—all carefully evaluated and document-ed—must be met:

  • Provide additional segmentation/abstraction (for example, at the network-layer);

  • Provide ability to restrict access to cardholder data or databases based on the following criteria: IP address/Mac address, application/service, user accounts/groups, data type (packet filtering);

  • Restrict logical access to the database—control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP);

  • Prevent/detect common application or database attacks (for example, SQL injection).

Those undertaking this approach can testify that it's no loophole. There are potential impacts on operational appli-cations, database maintenance, and connectivity. But done right it can effectively protect readable credit card data.

Compensating control hints

If you can't encrypt data at rest, an alternative is to narrow segmentation of cardholder data, implement strong access controls, and monitor database activity.

  • If you can't log all application activities, an alternative is to log enough to be able to recreate activities dur-ing a potential data breach analysis.

  • If you can't patch, an alternative is to pressure the vendor to provide one, or place network intrusion pre-vention in front of the unpatchable systems or host-base it on the systems.

About the author:
Carol Weiszmann is a principal at aimpublications LLC (www.aimpublications.com), where she analyzes and writes about how information technologies impact business value, competitiveness, and risk.

Bit9 Parity™

Achieving PCI Compliance at the Point of Sale
Using Bit9 Parity™ to Protect Cardholder Data

PCI: Protecting Cardholder Data
As the technology used by merchants and their partners has evolved, card fraud has become more sophisticated. Any business that stores or transmits cardholder account data is a potential target, and recent data indicates that 4 out of 5 cardholder breaches occur at the point of sale.

In response to this evolving threat, the major credit card companies (American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International) have created a set of security standards to protect their customers from security breaches and identity theft.

What are the PCI Data Security Standards?
The Payment Card Industry Data Security Standards (PCI DSS) includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

By following the standardized, industry-wide procedures of PCI DSS, organizations can:

- Protect their customers' personal data.
- Boost customer confidence through a higher level of data security.
- Insulate themselves from financial losses and remediation costs.
- Maintain customer trust and safeguard the reputation of their brand.
- Provide a complete 'health check' for any business that stores or transmits customer information.

The Pressure to Comply
Retailers are under heavy pressure to comply with PCI, and it does not look like that will ease any time soon. If anything, the payment industry is more intent on enforcement than ever before. And while only a third of the largest companies were considered compliant at the end of 2006, that number is expected to grow to between 50% and 75% by the end of 2007, with smaller companies following suit.

As of June 30, 2007, the PCI Data Security Standards are scheduled to be enforceable. This means that companies who are not compliant with the standard could face financial penalties. At an expected rate of $10,000 to $100,000 per month, these fines will place a heavy burden on organizations that have not complied.

Learn More

\>See a product demonstration
> **http://www.bit9.com**

\> Browse our resource library
> **http://www.bit9.com/resources**

\> Watch a recorded webinar
> **http://www.bit9.com/webinars**

\> Contact Bit9 today!
> **http://www.bit9.com/contactme**

PCI Data Security Standards (DSS)

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

Facts About Data Protection

- Recent data indicates 4 out of 5 cardholder data breaches occur at the point of sale.
- As of October 2006, only about one-third (100) of the largest (Level 1) retailers were compliant with the PCI standard.
- Fines for non-compliance with PCI range from $10,000 a month to $100,000 a month depending on circumstances.

Sponsored by: **Bit9**

Bit9 Parity™

■ Achieving PCI Compliance at the Point of Sale *(Continued)*

Protecting Data Where It's Most Vulnerable

The PCI Data Security Standards are designed to thwart identity theft and fraud by establishing controls around how customer data is handled within a company's information architecture. These guidelines place requirements on systems that stretch from the central data repository all the way to the point of sale.

As companies work their way through these guidelines, many are discovering their greatest exposure is at the endpoint. PCs deployed in the field, at stores and retail outlets, and at remote locations are more susceptible to hackers and malicious software.

Computers in stores are often used for many different purposes—not just transactions— and therefore need to provide access to a wider group of individuals. These PCs are frequently offline making centralized patching or auditing difficult, and other systems management processes are hindered by the simple lack of on-site IT resources. All of this creates a difficult environment for establishing security.

Whitelisting: Ease the Security Burden

Let's face it—your store employees are just not data security experts. Your security policies must be simple if you want them to be implemented effectively. This will make it easier for both your field staff and your central IT department to achieve your compliance requirements.

Bit9 protects data at these endpoints where it is most vulnerable by locking down PCs to a standard software configuration known as a "whitelist." Any and all unauthorized software is prevented from running and access to personal storage devices is brought under control. Malware, spyware, and rogue applications and devices are all blocked to ensure the integrity of the computer and its critical data.

Because this whitelist is controlled centrally, your PCs can not be modified in the field. And your store personnel never need to be given responsibility for complex IT tasks xuch as updating signatures, patching systems, or manipulating security configurations.

■ How Bit9 Helps You Comply with the PCI Data Security Standards

Here's how Bit9 addresses the PCI Data Security Standards.

Build and Maintain a Secure Network	
PCI DSS Specification	**Bit9 Functionality**
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).	By controlling the installation and execution of software, systems are prevented from drifting from their desired state. From a central console, vulnerable software can be centrally identified, making it easy to prioritize patch activity.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	By creating a whitelist of approved software, Bit9 ensures only approved services and software are allowed to run on any Windows-centric device.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	By creating a whitelist of approved software (scripts, drivers, subsystems, web applications), Bit9 ensures only approved services and software are allowed to run on any Windows-centric device.

Sponsored by:

Bit9 Parity™

How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Maintain a Vulnerability Management Program	
PCI DSS Specification	**Bit9 Functionality**
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers). **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	Bit9 blocks any software that is not pre-approved to run. A cryptographic hash (a unique identifier) is taken for each new file that is written to disk. Before this file is allowed to run, the hash is created and then compared to a list of approved hashes that were created by an automated software approval process. If the hash is on the list of approved hashes, the file is allowed to run. If the hash is not on the list of approved hashes, it is completely blocked from execution. If a file is changed, it changes the cryptographic hash for the file and because the hash is no longer on the list of approved hashes, it too will not run. While there are obvious benefits to Bit9's approach to preventing viruses, spyware, and adware, there are also significant benefits from preventing illegal and unlicensed software from running.
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Unlike traditional anti-virus solutions that need constant signature updates to stay effective, Bit9's non-signature antivirus approach continuously blocks all unwanted software without the burden of keeping signature files up to date. Ultimately, Bit9's non-signature antivirus approach eliminates zero-day attacks.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Because Bit9 has a software inventory of all software currently installed on Windows computers, a Bit9 user can centrally identify the presence or absence of vendor-supplied security patches.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	Every new file is looked up in the Bit9 ParityCenter™ knowledgebase of more than 2 billion file records and hundreds of thousands of known vulnerabilities to determine the threat level of the newly discovered software. Bit9 ParityCenter is updated daily with legitimate and potentially malicious software.
6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security. • Installing an application layer firewall in front of web-facing applications.	Bit9 has the ability to act as an application firewall on web-facing applications. Any new application or program that is not pre-approved is blocked from installing or executing. This ensures the highest levels of system and application security. This whitelisting approach is the safest way to ensure only approved software is allowed to run.

Sponsored by:

Bit9

Bit9 Parity™

■ How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Implement Strong Access Control Measures

PCI DSS Specification	Bit9 Functionality
7.1 Limit access to computing resources and cardholder information only to those individuals whose jobs require such access.	Portables storage devices can be an easy source of data leakage and loss. Bit9 can set controls on the ability to read/write/execute software on portable storage devices, preventing information leakage and accidental loss of sensitive, confidential information.
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	When a user logs into a system, the user will be restricted to run only the applications that have been pre-approved. All other applications will be restricted from use based on the user's policy and need to know.
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.	Bit9's device control policies ensure only authorized staff are allowed to copy cardholder data to portable storage devices, helping to control the distribution of cardholder data.
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	Bit9's device control policies ensure only authorized staff and computers are allowed to copy cardholder data to portable storage devices, controlling the storage, accessibility, and portability of confidential information.

Regularly Monitor and Test Networks

PCI DSS Specification	Bit9 Functionality
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	To prevent malicious software, every executable that is introduced (downloaded/installed/copied) to a Windows computer is tracked to a specific user on a specific computer. To prevent data leakage, every file (executable or data file) that is copied to and/or from a portable storage device is tracked to a specific user on a specific computer.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Installing an application layer firewall in front of web-facing applications.	Bit9 will log all activity related to new software and alert should an application begin to propagate across a number of computers over a time period. All new applications that get written to a system get logged and then compared to the Bit9 ParityCenter knowledgebase of 2 billion database records to gauge the threat level of the file.
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files and configure the software to perform critical file comparisons at least weekly.	With Bit9, only approved software is allowed to run. Should a hacker tamper with the bits of an application, it would change the cryptographic hash of the file and therefore render the new application inoperable. Ultimately, this protects hackers from tampering with applications to make them perform malicious activity.

Sponsored by:

SOLUTION

Bit9 Parity™

How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Maintain an Information Security Policy	
PCI DSS Specification	**Bit9 Functionality**
12.5.5 Monitor and control all access to data.	Data leakage is a serious problem and difficult to control. Only approved users should have access to data. By controlling who can and cannot read/write data to portable storage devices, a layer of control is added to prevent data leakage. Malicious applications and spyware can also gain unauthorized access to data. Bit9 allows only approved software to run and malicious software is therefore unable to gain access to confidential information.

To learn more about how Bit9 can help your organization become PCI compliant, contact us at 617.393.7400 or contact@bit9.com.

About Bit9, Inc.

Bit9, Inc., the leading provider of application and device control solutions, centrally controls which applications can and cannot run. Bit9's award-winning, patent-pending technology delivers the easiest and most effective way to achieve Windows lockdown, enabling IT professionals to realize the highest levels of desktop security, compliance, and manageability. Founded in 2002 by the founders of Okena (acquired by Cisco Systems (NASDAQ: CSCO)) and headquartered in Cambridge, Massachusetts, Bit9 is a privately held company. For more information, visit www.bit9.com.

Bit9

Bit9, Inc.
Ten Canal Park
Suite 201
Cambridge, MA 02141

p: 617.393.7400
f: 617.393.7499
www.bit9.com

Sponsored by:

Resources from Bit9

Whitepaper: Comparing Approaches for Desktop Software Lockdown

Whitepaper: AntiVirus is Dead: The Advent of the Graylist Approach to Computer Protection

Case Study: Cooley Group manufactured a better security solution with Bit9 Parity

Case Study: Ringgold Telephone Company Calls in Better Application Control

Datasheet: Control Your Desktops with Bit9 Parity

Datasheet: Achieving Sarbanes-Oxley Compliance with Bit9 Parity

Webinar: A Retail Case Study in Locking Down Desktops & Devices

Webinar: Achieving PCI Compliance at the Point of Sale (POS)

Webinar: CIO Outlook: Simplifying Your Compliance Projects

Library: Bit9's Resource Library: eBooks, Newsletters, Research, and More

About Bit9

Bit9 provides the easiest and most effective way to lock down the software and devices on your Windows PCs. Bit9's ultra-flexible application and device control policies ensure the best prevention against malicious software and data leakage.

www.Bit9.com