



Escaping PCI purgatory.

Compliance roadblocks and stories of real-world successes

Contents

- 2** *Executive summary*
- 2** *Navigating the road to PCI DSS compliance*
- 3** *Getting unstuck*
- 6** *Achieving and maintaining compliance*
- 7** *Capturing compliance opportunities*
- 8** *Why IBM?*

Executive summary

By now, any company driving high volumes of credit card transactions that is not compliant with the Payment Card Industry (PCI) Data Security Standard (DSS) faces steep penalties. Many companies are still working through the 12 requirements for PCI DSS compliance, and many are stuck on certain requirements. Regardless of the roadblock, it's time to get moving again.

But avoiding penalties is not the only reason to forge ahead. Achieving full compliance offers far-reaching business rewards. Many compliant companies have leveraged the compliance process to more effectively align their people, processes and technology or to introduce new capabilities that build a more integrated and effective security infrastructure. They recognize that compliance is an opportunity disguised as a challenge and that by taking a thoughtful approach to addressing this challenge, they can better position their company for the long term.

Navigating the road to PCI DSS compliance

Most companies that store, process or transmit cardholder data have realized that PCI compliance is not just another bureaucratic standard that slows business down. Rather, they understand that the PCI DSS is designed to protect all the stakeholders in the payment card industry, including consumers and businesses. Visa Inc. recently announced that "as of the end of 2007, more than three-fourths of the largest U.S. merchants and nearly two-thirds of medium-sized merchants have now validated their compliance with the Payment Card Industry Data Security Standard."¹ Yet those figures suggest that about 25 to 35 percent of U.S. merchants had not yet validated their compliance with the PCI DSS as of the end of 2007.

PCI compliance is a challenge for midsize and large companies alike, as there are four phases to meeting the PCI DSS requirements: assessment, remediation, compliance and maintenance. Most noncompliant organizations

PCI DSS requirements

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.

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

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.

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Requirement 12: Maintain a policy that addresses information security.

know the requirements; they've had the PCI compliance preassessments; they're aware of the deadlines. But they're stuck. IBM's research and experience working with thousands of such organizations reveal that most businesses experience at least one of five "sticking points" on the path to PCI DSS compliance. Some organizations:

- *Perceive compliance to be costly and overly complex*
- *Aren't sure how to interpret PCI DSS requirements*
- *Don't believe that there is a direct ROI associated with compliance and prefer to focus on other business initiatives*
- *Don't think that the rules apply to them*
- *Don't believe that there's a way to meet all 12 compliance requirements with one initiative.*

Getting unstuck

Fortunately, a business can successfully move beyond any of these obstacles – toward compliance and an improved security posture – with the right knowledge and tools. The following sections present scenarios that discuss some common sticking points with suggested methods for overcoming the challenges.

Sticking point 1: Compliance is expensive and complex

A financial institution perceives compliance as time consuming, complex and resource draining because it has more than 20 data fields and a large amount of stored data that needs encryption. The company is stuck and not sure where to start.

An outside security assessment team quickly determines the root of the problem: The company is collecting more information from each customer than it actually needs. Eliminating unnecessary fields in the company's database helps simplify the encryption process.

Highlights

The security team also recommends a combination of other solutions to help monitor data at the network level. In this case, meeting one PCI DSS requirement fulfills other requirements simultaneously – helping conserve company resources.

Sticking point 2: We're not sure how to interpret the compliance clauses
Some companies misinterpret regulations or lack the internal skills to address PCI mandates properly. In this scenario, a commercial airline conducts an internal audit that reveals that it is not properly protecting stored cardholder data.

The airline attempts to meet the related PCI DSS requirements by performing a "quick" encryption of its customer data – and finds that data is spread over nonintegrated legacy systems and that credit card data is improperly stored. Not only that, but it's also proving difficult to determine exactly where all the data is stored. Suddenly, the quick encryption isn't going so quickly.

Some companies misinterpret the compliance clauses, or fail to see a tangible ROI.

Using customizable and comprehensive solutions, an experienced provider helps the airline determine the amount of data it has stored, as well as where the data is stored across its systems. The provider suggests a solution that includes encryption and data elimination and brings the company's user management systems up to date. Further, once the airline transfers data to an encryption architecture, it is able to use information lifecycle management services to manage the information and help ensure that it is stored, transferred, accessed and disposed of according to compliance requirements.

Sticking point 3: Where's the ROI?

A retailer thinks PCI DSS compliance can't provide immediate ROI. Any benefits appear to be in the distant future. Plus, in struggling to turn compliance into ROI, the company can't afford the risk of downtime or noncompliance, which may decimate its margins.

Highlights

Upon evaluating the effectiveness of the company's current passwords, a security assessment team determines that data must be encrypted and that access management is needed to protect data at the application/system level. In addition, the company needs a layer of defense to help prevent hackers from gaining access to data through Web application vulnerabilities on its public Web site.

While the security team is able to help the company reposition its existing technologies in encryption and access management to achieve compliance, the company must implement a Web application vulnerability scanner to perform periodic tests. These solutions allow the retailer to continue processing credit card payments (an immediate benefit of the solution), avoid compromised data and fines for noncompliance, and support high availability by keeping systems running during updates. All of which contributes to a rapid ROI on compliance-related investments.

Sticking point 4: These rules don't really apply to our organization

Many companies think that their compliance with strict, federally mandated standards means that they are automatically compliant with the PCI DSS. Or they think that they are too small of a business to be vulnerable to the risks addressed by the PCI mandate. Neither of these perceptions is true.

In this scenario, a company that follows the ISO 27001 standard and maintains stringent security policies is not sure what else it needs to do to comply with the PCI DSS. A security team helps the company create a remediation plan – including products, processes, user education and firewalls – to achieve PCI DSS compliance in a way that enhances the business. To protect data against malicious viruses, the company uses various intrusion prevention tools, provisioning management solutions and security compliance management to automate updates to anti-virus software and help ensure proper installation.

Some companies think that they are automatically compliant with the PCI DSS.

Highlights

It can be a scary proposition to allow a third-party assessor to sift through your company's data—so choose a provider carefully.

Companies that successfully reach full PCI DSS compliance share common characteristics.

Having become PCI DSS compliant, the company can now offer enhanced, security-rich interface capabilities to its customers worldwide.

Sticking point 5: Nobody can help us with all 12 requirements

It can be a scary proposition for a company to allow a third-party assessor to sift through its data—so it's important that the company choose a trusted, experienced, certified provider that understands the PCI DSS in the context of the company's industry. Ideally, the provider would have the ability to handle all phases of PCI compliance validation and remediation. This way, the company can avoid management challenges caused by working with multiple providers. And if it does have a multivendor environment, the company needs a provider that can also work with other vendors' equipment.

Here's an example of the benefits of engaging a one-stop provider. A company with a legacy multivendor IT environment hires a provider to address the security assessment that is part of satisfying PCI DSS requirement 11. During the assessment, the security team finds that the company needs help with four more requirements.

This organization benefits from working with a provider that can help with security remediation and ongoing assessments—even within a multivendor environment. In the end, the security team enables the client to meet the five requirements it is lacking—helping the company better secure its infrastructure without rebuilding the entire IT environment.

Achieving and maintaining compliance

Companies that have reached full PCI DSS compliance seem to share some common characteristics:

- *They take a phased approach—following a roadmap that includes having an initial assessment to identify gaps; engaging with the right partner to develop a remediation plan; implementing the plan; reaching compliance; and developing a maintenance plan.*

Highlights

Achieving PCI DSS compliance does not guarantee that you will never have a security breach—compliance is an ongoing initiative.

The goal of compliance should be a more integrated, more effective, more secure IT infrastructure that also meets PCI DSS requirements.

- *They mitigate security risks efficiently and effectively.*
- *They leverage compliance as an opportunity to create a professional culture of security, often realizing a healthier and more cost-effective IT security model.*
- *They consider maintenance from the beginning, selecting a plan that can assist them in maintaining compliance on an ongoing basis.*

Of course, once compliance is achieved, this does not guarantee that a company won't ever have a data breach; initial PCI DSS compliance is really just the beginning of an ongoing initiative. The company must continually ask, "Now I'm PCI compliant, but am I really secure? Will I continue to be secure?" In addition, any time a company changes or updates its network, it should reassess its security.

Successful companies have realized that this cycle of assessment and refinement is best tackled with the assistance of a trusted security provider that can help them evolve their security and protect their business into the future. The appropriate provider can also help companies capitalize on the compliance process to reap the lasting business benefits of a healthier IT security model. The provider should deliver access to a compelling combination of depth of experience and capabilities that can help a company meet all 12 PCI DSS regulations—and prepare for upcoming challenges.

Capturing compliance opportunities

The goal of compliance should be a more integrated, more effective, more secure IT infrastructure that also meets PCI DSS requirements. Enhancing security and lowering the risk of a breach can certainly save an organization—and its customers—time and money in the long run. But beyond those rewards, as companies work through PCI sticking points to reach compliance, they realize an invaluable natural side effect: Along the way, they have enhanced their overall security stance and improved the health of their business.



Why IBM?

IBM is perfectly positioned to work with you on these initiatives. We leverage our experience and IT leadership to help strengthen your overall security posture and to help ensure the proper alignment of compliance and technology for your business. IBM offers a comprehensive program designed to take businesses through the entire PCI compliance process—from assessment, to compliance, to certification, to maintenance. IBM offers a combination of services, hardware and software to help companies stay compliant and continue to meet new requirements, supporting the next level of security.

For more information

To learn more about how IBM can help businesses build a stronger security infrastructure during the PCI DSS compliance process, as well as the security solutions and expertise offered by IBM, please contact your IBM representative or IBM Business Partner, or visit:

ibm.com/security/PCI

© Copyright IBM Corporation 2008

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
04-08
All Rights Reserved

IBM and the IBM logo are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

¹ Visa Inc., "PCI Compliance Continued to Grow in 2007," press release, <http://corporate.visa.com/md/nr/press753.jsp>.