VeriSign®

WHITE PAPER

More Lessons Learned—Practical Tips for Avoiding Payment Card Industry (PCI) Audit Failure

CONTENTS

+ Executive Summary 3

+ PCI Compliance—Cost and Benefit 3

+ Compromise Trends 4

+ Analysis of Compliance Failures 5
  - Top 10 Compliance Failures 6
  - Detailed View of Subsection Failures 7
  - Connecting PCI Audit Failures and Threats 8

+ Practical Tips for Avoiding PCI Audit Failure 10
  - Store Less Data 10
  - Understand the Flow of Data 10
  - Encrypt Data 11
  - Address Application and Network Vulnerabilities 12
  - Improve Security Awareness and Training 14
  - Monitor Systems for Intrusions and Anomalies 15
  - Segment Credit Card Networks and Control Access to Them 17

+ Future Considerations 18
  - Application Security 18
  - Mobile Commerce Security 18
  - Proliferation of Multifunction Devices Like the Apple iPhone 19

+ How VeriSign Can Help 20
  - VeriSign Global Consulting Services 20
  - VeriSign Layered Security Solution 20

+ For More Information 22

+ PCI DSS and Related Information 22
  - PCI DSS 22
  - Approved Vendor Requirements 22

More Lessons Learned—Practical Tips for Avoiding Payment Card Industry (PCI) Audit Failure

+ Executive Summary

The expense of compliance to the Payment Card Industry Data Security Standard (PCI DSS) can be substantial, especially for "Level I" (large) companies. The penalties for noncompliance can vary from censure, to fines, to, in the worse case, revocation of card issuance and payment processing capabilities. As recent current events have shown, however, major data security breaches are on the rise—threatening merchants and service providers with far worse financial costs, including litigation and the loss of consumer confidence.

Many companies continue to struggle with the increased complexity associated with PCI DSS—including those who may have achieved compliance in the past. As corporate information technology (IT) infrastructures evolve, new vulnerabilities emerge, such as those affecting corporate wireless networks or more powerful and connected mobile communications devices.

The VeriSign® Global Security Consulting team has performed hundreds of PCI assessments since the program's inception. In addition, VeriSign® Security Services protect some of the world's leading retail companies and financial institutions.

In our experience, the requirement failures and actual compromises that we have observed during these assessments exhibit common themes. This paper identifies proven tactics that help companies achieve and maintain PCI compliance and, more importantly, avoid compromise.

+ PCI Compliance—Cost and Benefit

In December 2004, the major credit card companies—Visa, MasterCard, American Express, Discover, and JCB—agreed on a common, comprehensive set of requirements for enhancing payment account data security. These requirements became collectively known as the PCI DSS. When the standards came into effect in June 2005, many Level I merchants and service providers poured a tremendous amount of resources into becoming compliant.

Compliance is a highly debated topic in the information security world. Some companies embrace compliance as a way to further their own security initiatives while others see the high costs and make the decision to not comply. Normally, noncompliance with a particular standard is a corporate risk that can be evaluated. In the world of credit card issuance and payment processing, PCI compliance is mandatory and part of the operating regulations that all merchants and many service providers contractually agree to. A compromise of a noncompliant entity carries large fines, forcing some small businesses to close their doors. Larger companies risk their contractual relationship with the credit card companies by not complying—which directly impacts their business.

BACKUP TAPES, PCS, AND LAPTOPS: DO YOU KNOW WHERE YOUR DATA IS?

Loss and theft of personal information are making headlines almost daily, as financial institutions, universities, government agencies, and other sectors report losses of backup tapes, PCs, and other physical assets that hold credit card data. Almost half of U.S. states have laws requiring the reporting of security breaches, so the risk of reputation damage for compromised companies is significant.

A review of data breaches reported to the Privacy Rights Clearinghouse reveals sobering information. From the period of February 15, 2005, to July 3, 2007, there were 687 reported data breaches,* representing 158 million compromised records. Of these incidents, 37 percent were due to lost or stolen hardware or backup tapes, accounting for 19.95 million of the records compromised. The high toll underscores the need to understand the flow of data in your organization and to better protect data and the repositories it is stored in.

*Privacy Rights Clearinghouse, "A Chronology of Security Breaches Since the ChoicePoint Incident," April 20, 2005, updated July 3, 2007, www.privacyrights.org/ar/ChronDataBreaches.htm.

Recent current events have revealed increases in the number and scope of data breaches—especially incidents involving credit card data. As the global hacker community becomes increasingly organized, their motivation changes from the desire for notoriety to fraudulent activity for financial gain. Once data breaches are exposed, merchants and service providers face unrelenting press coverage and financial loss—in the tens or hundreds of millions of dollars—due to reduced market capitalization, lost business and consumer confidence, and widespread litigation threats. These potential losses dwarf the cost of any compliance initiatives.

+ Compromise Trends

In analyzing PCI audit failures, it is important to first analyze the actual compromises that occur in the field. Besides conducting PCI assessments, VeriSign is also an approved provider of forensic and investigative services for compromised entities. Based on the experience of our consultants with numerous incidents over the past four years—many of them high-profile—we note the following frequently recurring weaknesses:

- **Wireless Networks**—Many businesses implement wireless technologies as a part of their IT strategy. These technologies range from simple Wi-Fi installations to Global System for Mobile Communications (GSM) or other cell networks to satellite. Because Wi-Fi vulnerabilities can be used to infiltrate the wired network, Wi-Fi should always be segmented away from wired networks with a firewall, and wireless intrusion detection and prevention systems should be deployed to prevent misuse. All wireless communications should be encrypted, regardless of format. Devices that have wireless capabilities should be appropriately hardened as attacks on endpoints increase. For businesses that are not implementing wireless technology, there is the peril of unauthorized, inexpensive, consumer-grade wireless access points being set up by employees or contractors for their convenience. These do not support the level of security required for compliance.
- **Unsecured Physical Assets**—Unencrypted and/or prohibited data may be stored on laptops, backup tapes, and other media that are prone to loss or theft. (See sidebar: Backup Tapes, PCs, and Laptops: Do You Know Where Your Data Is?).
- **Point-of-Sale (POS) Application Vulnerabilities**—Applications may be creating logs that store card track (full magnetic stripe) data. PCI requirements prohibit the storage of this information under any circumstance. Nefarious individuals who are interested in obtaining track data know which applications store this data and where the information is typically stored.
- **Card Numbers in the Demilitarized Zone (DMZ) or Other Public Systems**—Smaller merchants typically have their POS systems remotely accessible and connected to the Internet. This allows attackers to compromise this sensitive data remotely when not properly secured. POS terminals may be storing credit card numbers in the externally facing perimeter network. In some companies, the POS terminal acts as a card-present terminal that sits on the Internet. Because there is no firewall between the system accepting the card-present transaction and the Internet, this arrangement does not comply with PCI requirements (and hackers can easily find credit card data). Frequently, these systems are also storing track data.

- **Spreadsheets and Microsoft® Office Access™ Databases**—Users are likely storing card data in spreadsheets, access databases, flat files, or other formats that are difficult to control as they are transferred to laptops, desktops, and wireless devices. A key source of PCI audit failure is storing unencrypted data in Microsoft Office Excel® spreadsheets and Microsoft Office Access databases.
- **Poor Identity Management**—Users and administrators may not be handling authentication properly. Although password-based authentication is one of the easiest authentication methods to implement, it is also the most prone to compromise, because passwords can be easily shared, stolen, or guessed. Many companies also don't take advantage of the added security offered by two-factor authentication methods, including tokens or biometrics.
- **Network Architecture Flaws; Flat Networks**—Many businesses did not develop their IT infrastructure with security in mind. They often fail PCI assessment because they have flat (nonpartitioned) networks in which credit card systems are not segmented from the rest of the network. The lack of a secure network enclave is a serious issue regardless of PCI implications and can be very difficult to remedy. One of the easiest ways to reduce the impact of PCI to your infrastructure is to segment those systems away from the corporate network with a firewall.
- **Lack of Log Monitoring and Intrusion Detection System (IDS) Data; Poor Logging Tools**—Without log information, it is difficult to determine whether processes and security systems are working as expected. In addition, insufficient data makes it more difficult to investigate compromises that do occur. For example, if there were no record of the timeframe of a compromise, it would be difficult to determine the number of credit cards exposed during the compromise. California Senate Bill 1386 (SB 1386) has led the way for many states to enact similar laws. Under many of these laws, not knowing which data was compromised will force you to notify any customer you have done business with that their information may be compromised. (This is called secondary notification).

+ Analysis of Compliance Failures

Now that we understand the trends in threats, we can review the PCI DSS requirements and analyze how audits are most often failed by sampling actual assessments and determining the most often failed requirements.

Including the original Visa® Cardholder Information Security Program (CISP) and MasterCard® Site Data Protection (SDP) programs, VeriSign performed hundreds of PCI–related compliance assessments, averaging more than 100 assessments annually. For this study, we analyzed the results of 60 recent PCI assessments from 50 unique companies. Multiple assessments for the same company were considered, because they represented distinct entities such as, for example, a North American business unit and a Canadian business unit. The 50 unique companies were comprised of 2 card issuers, 21 merchants, and 27 service providers. Most of the companies were considered Level I organizations.

PCI compliance included 12 general requirements which were further divided into 61 subsections and an Appendix. Altogether, there were close to 300 specific detailed requirements. For the purposes of this study, audit failure in any specific requirement or subsection resulted in a failure in the general requirement.

Top 10 Compliance Failures

The following chart, based on a sampling of actual PCI engagements, lists the 10 most commonly failed PCI requirements and the percentage of assessments that were noncompliant with the particular requirement.

Figure 1: Top 10 PCI Audit Failures by Percentage

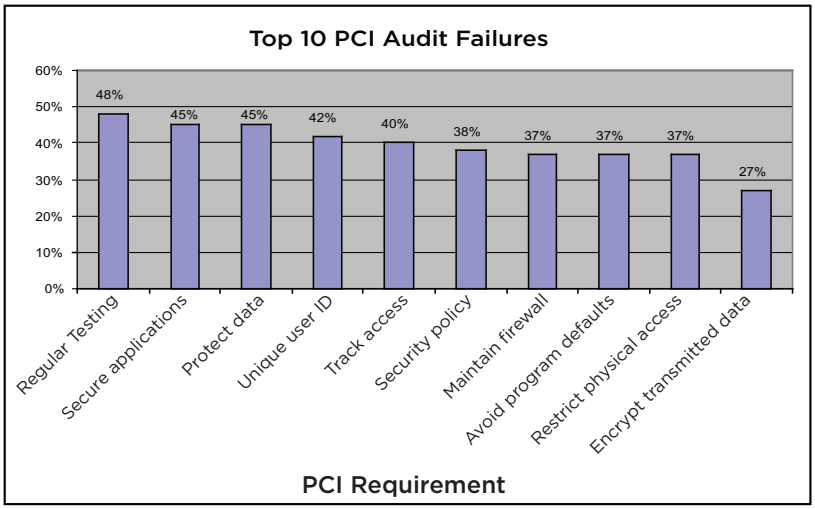


Figure 2: Top 10 PCI Audit Failures by Rank

Rank	PCI Requirement*	Audit Failure Percentage
1	**Requirement 11:** Regular testing	48%
2	**Requirement 6:** Secure applications	45%
3	**Requirement 3:** Protect data	45%
4	**Requirement 8:** Unique user ID	42%
5	**Requirement 10:** Track access	40%
6	**Requirement 12:** Security policy	38%
7	**Requirement 1:** Maintain firewall	37%
8	**Requirement 2:** Avoid program defaults	37%
9	**Requirement 9:** Restrict physical access	37%
10	**Requirement 4:** Encrypt transmitted data	27%

**For more detail on the requirements, please see www.pcisecuritystandards.org.

Though many of the VeriSign PCI assessment customers have robust security programs in place, historically less than 30 percent pass the assessment on their first attempt. Those that did pass were Level II or smaller Level I service providers who have smaller, less complex IT environments.

Of the 60 sampled full PCI audits, 32 (or 53 percent) of the companies failed in some way. Industry progress is being made, as this contrasts to a 73 percent failure rate from the study published last year (based on 112 assessments from 2005 to 2006). Almost half (48 percent) of assessed companies did not comply with the top failed requirement (requirement 11). To solve this problem, enterprises must regularly scan internal and external devices that store, transmit, or process credit card data—identifying software that is vulnerable to compromise.

Not surprisingly, requirements five and seven are the least commonly failed. They consist, respectively, of regularly updating and using anti-virus programs and restricting access to cardholder data. The security steps implied by these requirements are more straightforward to implement and provide very tangible benefits.

Detailed View of Subsection Failures

As the major requirements are rather broad, we can gain further insight by diving deeper into the results of the most often failed of the 61 requirement subsections.

Figure 3: Top 10 PCI Audit Failures by Subsection Requirement and Rank

PCI Subsection Requirement	Audit Failure Percentage
Requirement 11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.	43%
Requirement 11.5: Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files. Configure the software to perform critical file comparisons at least weekly.	37%
Requirement 6.1: Ensure that all system components and software have the latest vendor-supplied security patches installed.	35%
Requirement 3.4: Render personal area network (PAN) unreadable, anywhere it is stored.	42%
Requirement 3.5: Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.	32%
Requirement 3.6: Fully document and implement all key management processes and procedures.	32%
Requirement 10.2: Implement automated audit trails for all system components to reconstruct the following events: all individual accesses to cardholder data, all actions taken by any individual with root or administrative privileges, access to all audit trails, and invalid logical access attempts.	37%
Requirement 10.7: Retain audit trail history for at least one year, with a minimum of three months available online.	35%
Requirement 2.3: Encrypt all nonconsole administrative access.	33%
Requirement 2.2: Develop configuration standards for all system components.	33%

A single subsection failure can cause an entire requirement to fail, so a requirement with only one subsection above indicates a focused problem area. For example, the issue with requirement six seems focused on the application of vendor-supplied security patches.

On the other hand, multiple subsection failures can point to significant problems throughout the requirement. Fore example, prominent failures in 10.2 and 10.7 relate specifically to data access audit trails (often contained in system logs). In larger companies, a significant number of systems may interact with credit card data, generating a tremendous number of disparate logs. The managing and auditing of these logs is tedious work, yet this is extremely important for compliance and forensics in the case of a data breach.

Connecting PCI Audit Failures and Threats

The following chart maps PCI audit failures to common compromises and recommended security tactics. It's important to note this is not a perfect mapping. In some cases, an organization may pass a PCI requirement and still be vulnerable to compromise. For example, requirement six of the PCI DSS states that companies must develop and maintain secure systems and applications. VeriSign often encounters companies that can pass this requirement, even though their applications are still at risk. Of course, if the company tests the application according to requirement 11, it will be more likely to detect vulnerabilities, and thus the application will be more secure.

This example illustrates the interdependence of the PCI requirements and highlights the importance of a layered security approach to credit card security. A company can have strong policies and state-of-the-art technology, but it must also regularly test its network, firewalls, and applications to ensure that these security measures are working properly and data is secure.

Figure 4: Interdependence of PCI Requirements

Top Five Failed Requirements	Relevant Compromise Example	Recommended Tactics
Requirement 11: Regularly test security systems and processes.	A restaurant is compromised because they are operating vulnerable software without their knowledge.	Regularly scan internal and external devices that store, transmit, or process credit card data. This will identify potentially vulnerable software and configurations (such as blank administrative passwords).
Requirement 6: Develop and maintain secure systems and applications.	An online store is compromised through their shopping cart because of Structured Query Language (SQL) injections.	Regularly test all applications for security flaws. Even commercial off-the-shelf applications can contain vulnerabilities that may compromise your security posture. Home-grown applications should go through a strict software development lifecycle (SDLC) that includes security and tests for items in the Open Web Application Security Project (OWASP) top 10 (at a minimum, input validation).

CREATIVE SOLUTIONS: HOW A MAJOR RETAILER SAVED $250 MILLION

As part of a PCI compliance rapid remediation project, a major retailer analyzed the round-trip data flow between their POS terminals, through corporate offices, to their financial institutions.

The customer planned to overhaul their routers and switches to meet PCI requirements for encrypted nonconsole administrative access (requirement 2.3) and stored data protection (requirement 3.4), using Secure shell (SSH) and data encryption of personal account numbers (PANs). Like most retailers, their as is setup included cleartext card numbers beginning at the POS and remaining in storage. The quote received from their hardware vendor was around $250 million.

VeriSign proposed an alternative way to achieve compliance: Encrypting sensitive data before it was routed through the network. Transactional data is encrypted at the POS terminal using industry accepted algorithms, and the data stays encrypted in the retailer network until passed to the financial institution. PANs are replaced with reference numbers when the transaction data is returned to link back to the original transaction, and risk is mitigated by rendering the data unreadable if intercepted in the transaction process.

This creative alternative saved the retailer over $250 million by eliminating the need for a massive hardware overhaul while still meeting compliance requirements.

Top Five Failed Requirements	Relevant Compromise Example	Recommended Tactics
Requirement 3: Protect stored data.	A financial institution loses a laptop.	Unfortunately, data leaks outside of its intended areas on an hourly basis. Roving machines, such as laptops, should employ whole-disk encryption, and data discovery tools should be used regularly to ensure that the enterprise knows where all of its credit card data and risk are.
Requirement 8: Assign a unique identification (ID) to each person with computer access.	A retailer is compromised due to default passwords.	Many small retailers run stock POS systems that have default or blank passwords in them. This constitutes a significant portion of compromises from small merchants. Ensure that all default passwords are changed and all users must connect with a unique username and password that conforms to the standards.
Requirement 10: Track and monitor all access to cardholder data.	A compromised retailer has trouble telling which numbers are compromised due to insufficient logging on critical assets.	Logging is a mammoth task on any enterprise level. Companies should investigate both managed and in-house solutions and pick one that best fits with their current abilities. Logging is critical to PCI in a compromise, and an enterprise-wide strategy is recommended.

+ Practical Tips for Avoiding PCI Audit Failure

In conducting PCI assessments and helping companies meet compliance requirements, VeriSign has identified additional tactics that address the core reasons that companies fail PCI audits. These tactics—when applied collectively, consistently, and across the entire enterprise—help create an environment that lends itself to compliance and minimizes the need for piecemeal, reactionary solutions. In addition, these tactics take into account the real-world environments and limitations that many companies face.

Store Less Data

By storing less credit card data, you reduce not only risk, but also the scope of what falls under PCI regulations and auditing. Many companies store card data simply because they have always done so or because they do not regularly purge their systems of information that is no longer needed. Others store credit card data because they believe—often mistakenly—that the information is required for auditing, business processing, regulatory, or legal purposes. Many times, they confuse the need to store the credit card's transaction history with the need to store the number itself.

Increasingly, companies are discovering that they may not need to store credit card numbers at all or that they can remove numbers from the general environment and store them in isolated segments of the network. One-way hashing, truncation, and other techniques allow companies to perform discovery, fraud analysis, audits, chargebacks, and other tasks without storing a credit card number. For more information on using relatively inexpensive one-way hashing to replace credit card numbers, see http://www.verisign.com/strategies_for_pci.

How to avoid PCI audit failure: Justify the storage of credit card data. *Determine where credit card data is stored in your organization, what it is used for, and whether it is needed there. In addition, be sure that legacy reports have been modified to remove data that is no longer needed.*

One large, top-tier VeriSign financial-services customer went a step further: It completely cut off access to credit card data and allowed exceptions only for departments that could prove they needed the data. Doing so forced constituents to develop creative alternatives to storing credit card data.

Understand the Flow of Data

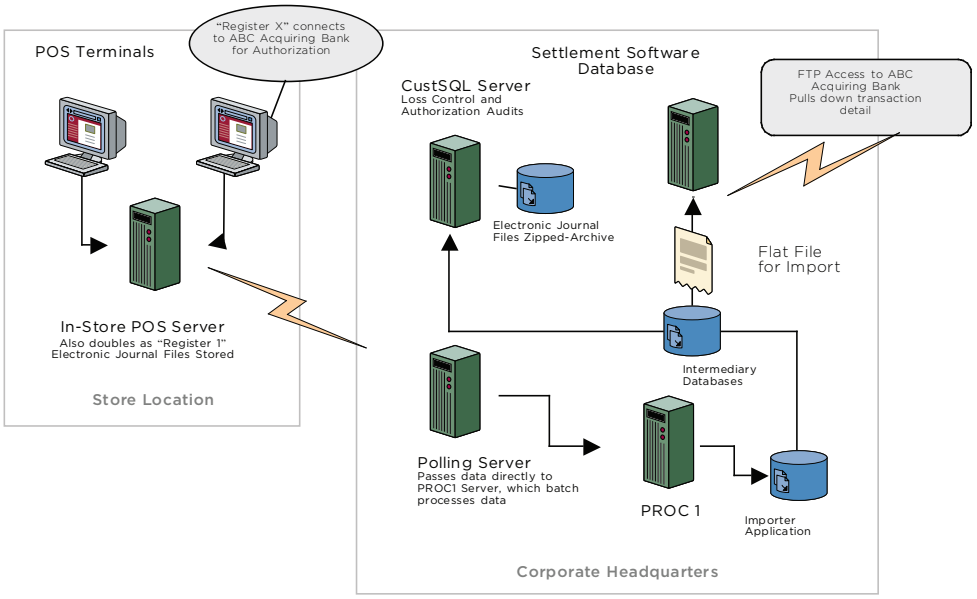
Many companies have no diagrams or documentation showing how credit card data flows through their organization. Unless you have performed a system-wide audit of all data repositories and then continue to perform audits regularly, you have no way of determining where data is stored and transmitted, and whether or not you're complying with PCI standards. Companies can curtail many of the compromises discussed earlier by tracking the flow of data and then correcting the associated problem.

In one PCI engagement, VeriSign tracked the flow of card data to 60 different locations in the company. By removing, scrubbing, or masking the credit card number, VeriSign helped the company reduce the flow of credit card data to just three locations while maintaining full business process functionality for all users who needed transaction data.

How to avoid PCI audit failure: Document the flow of credit card data throughout your organization. *Understand where data goes—from the point where you acquire it (either from a customer or third party) to the point where the data is disposed or leaves your network. Several software companies have created tools to assist in this effort by searching data stores and scanning network traffic for card data.*

The following is an example of a flow diagram for credit card data.

Figure 5: Sample Flow Diagram



Encrypt Data

Encryption is a key component of the layered security or defense-in-depth principle that the PCI attempts to enforce through its requirements. Even if other protection mechanisms fail and a hacker gains access to data, the data will be unreadable if it is encrypted. Unfortunately, many companies store credit card data on mainframes, databases, and other legacy systems that were never designed for encryption. For these companies, encrypting stored data (data at rest) is a key hurdle in PCI compliance. Typically, companies choose one of the following options in order to remediate encryption problems:

- **Retrofit All Applications**—With this approach, encryption is rolled into the coding of the payment application. Instead of writing the credit card number to a database, the payment application encrypts the number first. The database receives and stores the already-encrypted number. This approach is popular with companies that outsource their payment applications to other vendors, such as small banks that provide online banking. In these cases, the vendor handles the encryption. However, the company loses its ability to data mine this information and classify cards by bank, bank identification number (BIN), or card brand. Database alterations may need to be made to store unencrypted things, like the BIN number.
- **Use an Encryption Appliance**—A new class of appliance sits between the application and the database. It encrypts the card data on the way into the database and decrypts the number on the way out. Some companies use this approach because the trade-off between expense and business disruption versus time-to-deployment is attractive.

VeriSign operates the leading public-key-infrastructure platform available today. VeriSign end-user clients and SSL server Certificate Authorities enable secure, encrypted e-commerce and communicates for Web sites, intranets, and extranets. For more information, visit www.verisign.com/ssl/index.html.

- **Use an Encrypting Database**—An encrypting database offloads encryption to the storage mechanism itself, so companies don't have to significantly modify their applications or buy an appliance. Several major database companies have provided this type of solution to their customers. Alternatively, some companies will build this functionality from scratch into the databases by using the scripting languages or application programming interfaces (APIs) provided.
- **Obfuscate without Encryption**—Another way around encryption is to use obfuscation—making the credit card numbers unreadable—rather than using encryption. One-way hashing, truncation, tokenization, and other approaches are less costly to implement than encryption, and in many cases, companies can still perform all necessary business functions related to credit card numbers. For more information about one-way hashing in credit card environments, please see http://www.verisign.com/strategies_for_pci.

How to avoid PCI audit failure: Incorporate encryption at the development phase. *Use an encryption framework during development instead of developing applications and then retrofitting them for encryption.*

How to avoid PCI audit failure: Have a company-wide encryption strategy. *A typical company has multiple encryption requirements—for everything from virtual private network (VPN) tunnels using Secure Internet Protocol (IPsec), email secured by Secure/Multipurpose Internet Mail Extensions (S/MIME), and Secure Sockets Layer Certificates (SSL Certificates), to mainframe, database, and disk encryption (e.g., for users with laptops). To minimize costs and avoid problems associated with managing multiple keys, consider a strategy that encompasses not only PCI requirements but also the entire range of encryption requirements within your organization. Then, consolidate key management to the fewest number of points possible.*

Address Application and Network Vulnerabilities

Many application and network vulnerabilities can be remedied by updating POS applications, identifying poorly coded Web applications, and scanning quarterly. The best approach, however, is to develop applications with security in mind.

Update POS Applications

Some POS terminals, Web shopping carts, and other payment applications—especially older versions—automatically generate log files that store track data, card verification value (CVV2) data, and other credit card information, even though PCI regulations prohibit doing so (even if the data is encrypted). Many merchants are unaware that this is occurring.

How to avoid PCI audit failure: Update your software with patches as they are released. *Ask your POS application vendors whether their current- or older-version applications store track data. Validate their statements yourself by testing the application or looking for third-party validation of the output and data stores. Many application vendors are releasing new software versions that comply with Visa's Best Practices program.*

The VeriSign® Security Risk Profiling Service enables you to dynamically generate a risk score for your organization that includes threats, vulnerabilities, network access policies, and financial impacts. Simulation tools show how changes in the environment will affect risk and compliance with internal and external policies and regulations. As a PCI Approved Scanning Vendor (ASV), our highly trained experts utilize best-of-breed technology, unmatched threat intelligence, and structured processes to help you make better business decisions about your information security program. For more information, visit www.verisign.com/managed-security-services/information-security/risk-profiling/index.html.

Identify Poorly Coded Web Applications
Many data compromises occur because of improper coding, especially in Web applications. In fact, Web application vulnerabilities account for the largest percentage of compromise cases that VeriSign sees. Poor coding can result in weak password control or applications that are vulnerable to SQL Injection and other attack vectors. The OWASP, referenced in the PCI Data Security Standard, provides information on these attack vectors. SQL Injection attacks are especially threatening because hackers can penetrate the network simply by using an Internet browser to execute code at the database layer of an application. This code can cause the database to hand over private information to hackers, redirect users to a bogus site without their knowledge, or compromise data in some other way.

How to avoid PCI audit failure: Have a third party conduct an application test and code review to ensure that your custom Web applications are securely coded. *Improve internal software development life-cycle practices by integrating security into these cycles.*

Scan Quarterly for Application and System Vulnerabilities
The PCI standard requires companies to perform quarterly scans, both externally and internally, and whenever changes are made to a system. Scanning should also include wireless systems and devices. In addition, the standard specifically requires scanning for OWASP vulnerabilities. OWASP attacks try to subvert application security by injecting commands directly into databases without the company's knowledge. Currently, there is no good way to scan automatically for these vulnerabilities. The process requires assistance from an analyst, which can be prohibitively expensive when conducted in house. For this reason, some companies outsource this task to a qualified third party that can perform additional manual tests and analyze results for the company.

In our experience, most companies scan their external perimeters, but many do not scan internally. They mistakenly believe that data is secure if their perimeter is well guarded. Frequently, they believe that insider threats are not an issue. In fact, insider threats may present a higher risk in terms of damage or data loss. Employees in accounting or software development, for example, can often do greater damage than an outside hacker, because they know your system; they know what controls are in place, and they know how to beat them. In addition, they often have the authorization to legitimately access secured data.

How to avoid PCI audit failure: Perform quarterly scans as required by the PCI standard.

Implement Strict SDLC Processes
A proper SDLC process is part of a well defined security program and involves well defined phases: risk analysis, prototype design and building, testing, deployment, maintenance, and retirement. Ideally, security is applied at the analysis phase, and then is built in and tested throughout the application's life. Many companies do not have the resources required to implement the rigid processes and detailed documentation that the PCI DSS calls for. Some companies try to cobble together enough documentation to pass PCI, but their efforts are rarely systematic or adequate.

How to avoid PCI audit failure: Avoid ad hoc development, implement replicable processes, and document everything. *If you do not have an on-site expert, at least delegate a representative to be part of the SDLC process. Then document the relevant processes to verify that the application development team performed risk analysis, set security requirements, performed requirements testing, and so forth. Alternatively, outsource the task to a qualified design review service that oversees the development life cycle to ensure that security requirements have been met. This approach not only supports compliance with PCI, but also helps you catch security defects early in the process, when corrections are less costly.*

Improve Security Awareness and Training

It is often surprising to see how many compromises and PCI audit failures could be avoided by improving security awareness. Security awareness is specifically covered in requirement 12 of the PCI DSS but impacts other areas within the standard as well. This is especially true for mistakes related to poor password control, improper data storage, and overly permissive usage policies. Security is defined by three distinct control points: people, process, and technology. People are easily the weakest link and can subvert controls put into place by process and technology.

Many users and administrators don't take password control seriously. They share passwords with other users, leave them in easy-to-find places, or create passwords that can be easily guessed. Part of the problem is that many people simply do not believe that a threat exists. Stronger identity management includes ongoing security awareness programs as well as policies that ensure enforcement.

Ongoing training and security awareness programs can also help minimize the following data storage issues:

- Noncompliant storage of CVV2 data or other credit card data
- POS terminals that generate track data
- Potential abuse of data mining related to credit card numbers (hackers can access information online—name, address, and so on—that combined with a credit card number, can be enough to make a purchase)

Finally, users sometimes forget that visitors, cleaning crews, and others may be able to view data that is not intended for them. In one VeriSign engagement, the consultant went to the reception desk to introduce herself. Credit card numbers were displayed on the receptionist's computer screen, in full view of anybody who walked up to the desk.

Clearly, data control decreases as the number of people with access increases. Managers must learn to restrict credit card data to those who truly need the information for legitimate business purposes.

How to avoid PCI audit failure: Continually educate and train internal staff. *Develop processes that ensure adherence to security procedures and policies.*

Monitor Systems for Intrusions and Anomalies

It's hard to make informed security management decisions if you don't have visibility into the network and the over-air communication surrounding it. Effective monitoring entails more than simply looking for known attack signatures. It also involves looking for data anomalies and variations in your normal host and network logs that could indicate a new type of attack or threat. When performed consistently and properly, the following measures help maintain security over time and through changes:

- Intrusion detection and prevention (both wireline and wireless)
- Log monitoring and retention

Allow Intrusion Prevention and Detection Devices to Accumulate Sufficient Intelligence

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) are placed next to key entrances to the network and often act as a last-chance virtual safety net. They monitor network traffic, and when other safety measures (such as firewalls, anti-virus software, and access control) fail to stop suspicious traffic, these systems notify the organization of potential break in, malicious activity, or noncompliant traffic. In the case of IPS, they are able to block or discard offending traffic, keeping it from performing anything malicious against a particular host.

Companies can choose from two types of IPS/IDS technologies: signature- or anomaly-based engines. A signature-based device works much like an anti-virus solution. One drawback is that if it doesn't know about a particular threat, that threat will pass unnoticed and can potentially pass by the implemented security measures. The second type of device is anomaly based. The system learns about traffic and patterns and creates rules to understand how traffic typically looks. If something out of the ordinary occurs, it alerts based on its accumulated knowledge.

Many companies expect these devices to work well out of the box. This is not the case, however, leading companies to a false sense of security. It can take upwards of 6 to 12 months for either type of solution to accumulate enough intelligence to provide useful, accurate information. Furthermore, these devices only provide visibility at the network layer. Other mechanisms are needed (such as application log monitoring) to monitor potential threats at the application layer. Finally, although IPS/IDS requires a substantial investment, it can be leveraged not only for security but also to understand traffic flow and optimize resources.

How to avoid PCI audit failure: Place IPS/IDS near the assets you want to protect. *Doing so helps ensure that they will detect the types of activity you are most concerned with.*

How to avoid PCI audit failure: Establish a centralized server for reviewing, correlating, and managing IPS/IDS logs.

"Renegade" and Proliferating Corporate Wi-Fi Network Access Points

Many companies now have formal programs to roll out Wi-Fi throughout the enterprise. While this brings added convenience and mobility to the corporate information worker, it can result in a nightmare when trying to monitor and manage legitimate, secure wireless access points.

The VeriSign® Wireless Intrusion Prevention Service (WIPS) delivers comprehensive, real-time identification and analysis of wireless security events that require immediate action. This service provides continuous awareness of wireless-based attacks on your company's IT infrastructure and offers the identification/location of rogue access points that expose the wireless network to unauthorized parties. The VeriSign® Managed Public Key Infrastructure (PKI) service can also be leveraged to issue certificates to ensure that only authorized devices can access your legitimate wireless infrastructure. For more information, visit www.verisign.com/managed-security-services/information-security/wireless-intrusion-prevention/index.html.

One challenge to both companies with formal Wi-Fi programs and those with formal no-wireless policies is the renegade access point—sometimes from the most unlikely sources (i.e., senior management). Corporate lore is filled with tales of the senior vice president who brings in a $59 wireless router, plugging it into a corporate Ethernet port just to enjoy a little private mobility capability on his floor. Rank and file employees and contractors are less ballyhooed in security lore, but they are also threats to set up their own wireless access points.

Another challenge is the proliferation of Wi-Fi networks. If your office is on the 80th floor of an office complex in Singapore, you probably have to sort through hundreds—or thousands—of wireless access points to manage, legitimate, and reengage access points into your corporate network. Being able to recognize which are authorized parts of your network, which are nonthreatening neighbors, and which are threats is no easy task. This increases the danger of associating with "evil twins" and other threats.

How to avoid PCI audit failure: Place dedicated wireless IPS devices near the assets you want to protect. *Doing so helps ensure that they will detect types of activity you are most concerned with.*

Improve Log Monitoring and Retention

The PCI DSS requires companies to track all access to credit card data and maintain a record of that access. This particular aspect of security is so important that requirement 10 of the PCI DSS is dedicated entirely to logging.

Tracking and logging access is difficult because it often involves looking at massive databases that have live credit card numbers in them. For each access, logs must record who accessed the data and from where, the authentication mechanism used, the date, the time, and other data elements listed in requirement 10.2.

Some products help companies set up this process, but they can be costly and labor-intensive to manage. Depending on how the logs are generated and whether they are meaningful, companies can gain significant visibility into a particular machine. Many companies fail PCI audits because of improper log monitoring and retention.

From a logging perspective, the following issues are particularly daunting:

- **Scattered Log Collection**—Many companies do not point all their logs to a central location for collection and analysis. This results in piecemeal log analysis and almost always creates voids.
- **Complexity of Application Logging**—Operating system logs are difficult enough to collect and analyze; application logs are even more so. Many applications do not store the quality of information needed for PCI compliance or for investigating an incident. In addition, application logs are almost always in plain text; this is a problem, because they frequently store credit card data, leaving it vulnerable to compromise.

VeriSign® Log Management Service collects, aggregates, and prefilters raw logs from monitored sources to forward potentially significant events and alerts to VeriSign® TeraGuard, an information management architecture. There, a VeriSign analyst determines whether the event represents a legitimate threat, and then notifies the customer, who can either approve them or flag them for further investigation—thereby allowing customers to track workflow and create an audit trail for compliance purposes. Additionally, the system is configurable to automatically generate reports that meet Requirement 10. For more information, visit www.verisign.com/managed-security-services/information-security/log-monitoring/index.html.

- **Poor Monitoring, Reporting, and Review Capabilities**—Some companies collect logs, but do not handle and process them in ways meeting requirement 10. This is often because it is time consuming and difficult to configure products to generate PCI–compliant reports and then track the regular review of those reports in a way that can be demonstrated to PCI assessors. If logs are collected, normalized, and aggregated at a single point, analysis becomes easier, report generation becomes more straightforward, and review occurs more frequently. Besides reviewing the logs, companies must be able to track when and if reviews are being done and how often the logs are reviewed. Although one option is to sign off manually on a form, log solutions should allow users to mark in the log itself what has (or has not) been reviewed.

How to avoid PCI audit failure: Configure PCI–relevant systems to log the data elements specified in requirement 10.2, and use a system to centralize log collection, aggregation, and reporting. *Log management technology, security information management technology, and managed log services provide some or all of the required functionality. Centralized solutions also enable monitoring who has access to credit card data and, in ideal cases, track the workflow of log review activities.*

How to avoid PCI audit failure: Hold people accountable for monitoring logs. *Log monitoring can be tedious, but someone has to do it. Some of the log collection, normalization, and correlation can be outsourced, but at some point, someone from the company must review the reports to determine whether there are any risks to credit card data.*

How to avoid PCI audit failure: Watch the applications. Many problems occur in application logs. *Make sure that you can get to the logs easily and that they are tracking necessary access data. In addition, be sure that they do not store credit card data in cleartext. These application-level controls are core requirements of the PCI Payment Applications Best Practice (PABP) framework. By either purchasing PABP–certified applications or having your applications certified, you can further ensure proper logging.*

Segment Credit Card Networks and Control Access to Them

Experience has shown us that companies with the least-segmented networks suffer the most when compromises occur. Although network segmentation is a complex, time-intensive task, companies should design and build their network so that credit card data is protected, even if another part of the network is compromised. Start by isolating credit card data in its own segment, where connections are separate from the rest of the corporate network, especially the development and testing network. Conversely, from a network availability perspective, out-of-band management and continuity capabilities should be provided for credit card systems. This setup helps ensure business continuity should Internet-facing systems undergo a denial-of-service (DoS) attack. DoS attacks can be very damaging, and although companies cannot fully prevent them, there are certainly ways to lessen their impact. Good router configuration management and additional bandwidth capacity are a good start. You may also want to consider secure backup servers and other technology to keep your systems available during an outage or attack.

VeriSign® Unified Authentication provides a single, integrated platform for provisioning and managing all types of two-factor authentication credentials. This service reduces the cost of deployment by leveraging an enterprise's existing infrastructure and delivering a flexible, future-proof solution built on known, open standards. The combination of VeriSign infrastructure, technology, data, and intelligence puts you in control of your security environment, leaving you free to focus on running and expanding your business. For more information, visit www.verisign.com/products-services/security-services/unified-authentication/index.html.

Finally, companies should use a multilevel network authentication strategy to control access to the credit card network. First, disable network ports that could potentially connect to credit card systems in nonsecure areas such as conference rooms or even employee cubicles. Second, limit the number of people who can access the credit card systems. Third, use mandatory access control (MAC) address filtering, reverse proxies, network access controls (e.g., 802.1x), and even strong authentication to allow IP connectivity to your systems.

For remote access, the PCI standard requires two-factor authentication. You can leverage this capability inside the network to maximize your strong authentication investment and further protect access to critical credit card data. Two extremely popular solutions for two-factor authentication are one-time passwords (OTPs) and PKIs. Both are available in a number of form factors, including tokens, credit card formats, and software solutions on desktops and mobile devices.

+ Future Considerations

The PCI standards are a living document that will continue to evolve as network and application threats become more sophisticated and new credit card technologies emerge. As an example, current compromise trends have resulted in new PCI requirements related to application security and wireless device security, but mobile commerce security is an area that has yet to be addressed in the PCI standards.

Application Security

As discussed earlier, application vulnerabilities are already a significant issue and will only increase in focus as new applications are developed. Requirement 6.5 of the PCI DSS may see the introduction of a variety of new application-related topics; this relatively new requirement specifically addresses Web applications and has 10 subrequirements. As companies deploy new applications, the ideal course is to use only CISP–validated payment applications (see URLs at the end of this paper) and a strict SDLC process when developing custom applications in house. Referring to OWASP is a great start as this standard is updated to reflect current trends in application attacks.

Mobile Commerce Security

Wireless devices used as payment instruments present even greater security and compliance challenges. Even so, some leading-edge companies are already experimenting with embedding credit card numbers, virtual cash, and other personal data into wireless devices. The basic idea is to embed one or more payment methods into a mobile device and use the device itself like a virtual wallet. Instead of swiping a credit card through a POS terminal, for example, consumers could simply wave their wireless device across the terminal. Radio-frequency technology would transmit the transaction data to the terminal, which would then tender the charge and respond with an appropriate confirmation to the device. Commercial deployment of mobile payment capabilities can already be seen in Japan, South Korea, Singapore, and several European countries, such as Austria, Norway, and Spain, with trials evolving rapidly in the U.S. market.

These early deployments have had their limitations. In 2004, Japan's NTT DoCoMo launched its first wallet phone, which can store up to $450 in virtual cash. If the phone is lost or stolen, the phone can be locked, preventing unauthorized use. However, the virtual cash cannot be replaced.[1] Protection from such loss, as well as security and identity management, are of paramount concern for consumers as this technology quickly matures. As recently as September 2005, Kiyoyuki Tsujimura, NTT executive vice president of products and services, cited security as a key stumbling block for consumer adoption.[2]

These shortcomings aside, Juniper Research predicts that person-to-person (P2P) fund transfers and mobile payments in the developing world, together with the commercialization in 2009 of Near Field Communication– (NFC) based mPayments will generate transactions worth approximately $22 billion by 2011.[3] These projections, along with the increased availability of the required technology, illustrate a bright future for mobile payment options.

So far, mobile payment technology is so new that the PCI has not instituted requirements to govern it. However, it's logical to assume that any new technology will have to adhere to existing standards. At the same time, new standards will likely evolve to support the new technology. For now, the best course is to adhere to existing standards. In addition, if you're interested in deploying mobile technology, get involved in industry associations such as the Mobile Payment Forum, Mobey Forum, NFC Forum, or Open Mobile Alliance. Doing so will give you more insight into future trends. It will also allow you to participate in and possibly influence early-stage discussions of these technologies so that you can potentially benefit from the end results.

Proliferation of Multifunction Devices Like the Apple® iPhone™

Managing security for mobile PCI–related activities is becoming more and more complex with the advent of increasingly powerful multifunctional devices, such as the iPhone™ mobile digital device. At many companies, there will be pressure on corporate IT to enterprise-enable these new devices.

By combining quad-band supported mobile phone service, complete wireless Internet access, multimedia playback, and a 2.0 megapixel camera, the iPhone seems to be a lock to become the newest tech toy of many professionals—guaranteeing its appearance in enterprises worldwide. While it seems destined to become a consumer favorite, the iPhone has a long way to go in order to match enterprise security measures found in such high-security devices like the BlackBerry® handheld mobile device.

Because the iPhone is equipped with fully-functioning Internet capabilities, it offers users access anywhere and anytime to the Web—including sites with malicious code or malware specifically targeting common first-generation platform launch vulnerabilities. Although early attacks will most likely be done for publicity and annoyance, more nefarious individuals will be following right behind to support identity theft, password capture, and other malicious uses.

1 CBS.com, "Cell Phones & Cash," July 22, 2004, www.cbsnews.com/stories/2004/07/22/tech/main631231.shtml.

2 The Sydney Morning Herald, "Big cash is being tucked into wallet phones," September 15, 2005, www.smh.com.au/news/technology/big-cash-is-being-tucked-into-wallet-phones/2005/09/14/1126377378315.html.

3 Marketwire, "Mobile Payments to Generate Almost $22bn of Transactions by 2011 and Be Adopted by 204m Mobile Users," July 9, 2007, www.marketwire.com/2.0/release.do?id=749418.

According to Gartner Research, the iPhone primary security defense rests on a restricted configuration that prevents user-installable applications, conceals the file system, and limits port access. Although this is by design, users are already seeking ways to gain access to its file system, leaving the iPhone open for major enterprise data leakage possibilities—troublesome because it does not come with tools for IT to secure the data through encryption.[4] Any mobile device that will store business-critical information must be capable of security-policy enforcement, either innately or through add-on products—neither of which are available for the iPhone at this time.

+ How VeriSign Can Help

The VeriSign PCI solution is based on the VeriSign® Layered Security Solution, comprised of consulting services for assessment and remediation advice and programs, as well as related network security and authentication services to meet ongoing compliance requirements.

VeriSign® Global Consulting Services

For more information on PCI assessment and remediation services, as well as other security compliance and certification programs, see www.verisign.com/global-consulting/security-consulting/index.html.

VeriSign® Layered Security Solution

Most security technologies address just one layer of business assets, leaving weak points in other layers vulnerable to attack. The layered approach to security has a cumulative effect that offers the best protection possible for securing end-to-end confidential data and transactions, using the following products and services:

VeriSign® Managed Security Services:

- PCI scanning services
- VeriSign® Managed Firewall Service
- VeriSign® Log Management Service
- VeriSign® Intrusion Prevention/Detection Management Service
- VeriSign® Wireless Intrusion Prevention Service

VeriSign Managed PKI for SSL

VeriSign Unified Authentication for OTP

VeriSign Managed PKI for client

4 eWeek, "iPhone's place in the enterprise unclear," July 9, 2007, www.eweek-digital.com/eweek-lookinside/20070709_stnd/?pg=22&liid=b34a8bcc9d&search=iphone+place+unclear+in+enterprise.

Figure 6: The VeriSign Layered Security Solution to Common PCI Compliance Requirements

Required Controls	Applies to	How VeriSign Helps
Requires annual assessment for Level 1 merchants, annual penetration testing, and application testing for Level 1 and 2 service providers.	Merchants, service providers, and banks	Merchants, service providers, and banks Enterprise Consulting Assessments
Requires logging of all access to credit card data.	Credit card processing systems	VeriSign Log Management Service
Requires quarterly scans and annual penetration tests. External scans are conducted by an approved vendor. Requires policy, personnel, and systems to handle security alerts.	Credit card processing systems and network devices	PCI scanning service Technical Security Assessment
Requires host and/or network intrusion detection or prevention.	Credit card transmission networks, processing, and storage systems	VeriSign Intrusion Prevention/Detection Management Service VeriSign WIPS
Requires an appropriately configured and managed firewall.	Firewalls providing access to credit card processing and storage systems	VeriSign Firewall Management Service
Requires two-factor authentication.	Remote access to credit card processing environments	VeriSign Unified Authentication for OTP VeriSign Managed PKI for client
Requires 128-bit SSL encryption and effective management of crypto key transmission and storage.	Databases, Web servers, and applications that store or process credit card data	VeriSign Managed PKI for SSL

+ For More Information

For more information about these services, please contact a VeriSign representative at 650-426-5310.

Additional information on the VeriSign PCI compliance solution is available at www.verisign.com/verisign-business-solutions/compliance-solutions/business-partner-solutions/payment-card-industry/index.html.

+ PCI DSS and Related Information

PCI DSS

For more information about the PCI Security Standards Council (governing organization for PCI DSS) see www.pcisecuritystandards.org.

The full text of PCI DSS can be downloaded at www.pcisecuritystandards.org/tech/download_the_pci_dss.htm.

A full glossary of terms related to the PCI DSS can be found at www.pcisecuritystandards.org/tech/glossary.htm.

Approved Vendor Requirements

The PCI Security Standards Council maintains high standards and programs for certifying vendors of PCI–related services, including the Qualified Security Assessor (QSA) and ASVs. For more information:

- **QSA**—Visit www.pcisecuritystandards.org/programs/qsa_program.htm.
- **ASV**—Visit www.pcisecuritystandards.org/programs/asv_program.htm.

Visit us at www.VeriSign.com for more information.

00025041 08-15-07