PCI DSS

An Evolving Standard
The Payment Card Industry Data Security Standard (PCI DSS) was established in 2006 by the major card brands (Visa, MasterCard, American Express, Discover Financial Services, JCB International). As threats to card processing have changed, so has the standard. In fact, there have been 5 different versions of the PCI DSS, including PCI DSS 3.1 that was released in April 2015.

PCI DSS Version 3.1
While PCI 3.1 includes minor clarifications and additions, PCI version 3.1 was primarily released to address the insecurity of Secure Sockets Layer (SSL) and some Transport Layer Security (TLS) encryption protocols. Effective immediately, all SSL and early TLS versions are no longer considered to be strong cryptography. From April 15, 2015 on, merchants must not implement new technology that relies on SSL or early TLS (version 1.0 and sometimes 1.1, depending on use and implementation). Merchants already using systems and devices that utilize SSL and TLS must discontinue the use of those systems and devices before June 30, 2016.

The PCI DSS v3.1 requirements directly affected are:

- **Requirement 2.2.3** Implement additional security features for any required services, protocols, or daemons considered insecure.
- **Requirement 2.3** Encrypt all non-console administrative access using strong cryptography.
- **Requirement 4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

We made a list of 19 new PCI requirements and a quick breakdown of each of them to act as a reference point when complying with the new standard.
Web Redirection

Requirement 0 – PCI Intro

When a website redirects to a payment page, such as a third party shopping cart, PCI DSS 3.0 classifies this as a web redirection system and places it under the umbrella of PCI DSS compliance.

There are a couple forms of redirection. Traditional redirection is the idea of when a website points users to a third party that collects and processes all card data. Another form of redirection is client side redirection, in which a customer types card data into a web form generated by the merchant, and is then sent directly to a third party. Either way, card data will not pass through the original website.

In the past, these forms of redirection were validated using SAQ A, but new emphasis in PCI DSS 3.0 changes that.

The new SAQ-A EP form is designed for e-commerce merchants using client side redirection.

This direction will affect many merchants who were previously completing an SAQ A and now must move to an SAQ A-EP, which is significantly longer and includes things such as external vulnerability scans and penetration testing.

Why is this requirement important? If a hacker is able to manipulate redirection code, he could direct your customers to a fake payments page that looks identical to the one you had originally outsourced.
Data Flow Diagrams

Requirement 1.1.3
A cardholder data flow diagram should show how cardholder data enters your network, the systems it touches as it flows through your network, and any point it may leave your network (e.g., sent to a payment processor). You’ll want to maintain a diagram for each varying card flow that exists within your card-processing environment. Most businesses will have just one flow, but you might have an additional flow if your website processes payment cards.

You need to get the right people in the room to discover your different flow processes. This may include your web development team, accounting, third-parties, etc. Interview them meticulously, and most importantly document, document, document. You may also need to employ the use of a card data discovery tool that searches networks for unencrypted card data. SecurityMetrics has a tool called PANscan to assist in this process and has found over 780 million unencrypted payment cards to date.

Physically creating a document that explains the processes will help you better understand where card data lives on your network. The purpose? If you know how your organization handles payment card data, you’ll be able to protect it. Boiled down, you may just find some unnecessary or dangerous ways of handling card data to eliminate.
Encrypt Satellite Communications

**Requirement 4.1**

In addition to GSM (cellular) connections and wireless Internet, the PCI DSS requires encryption of any communication that includes cardholder data sent over satellite. Depending on your business, this may not have much impact.

However, SecurityMetrics has many large retail chain clients (e.g., gas stations, hospitality, restaurant chains) that do use satellite communications between chains and even as a backup connection. According to the PCI Council, it’s no longer good enough to rely on the link provider’s system security. It’s your responsibility to keep this data secure.

Once you’ve selected an encryption solution, you need to test if it works. The process would be to capture the traffic and visually verify that no cardholder data is passed in the clear.

Evaluate Emerging Threats

**Requirement 5.1.2**

For systems not commonly affected by viruses that don’t have anti-virus software installed, you are required to implement and document a new process that shows you periodically evaluate these systems against emerging threats.

The point of Requirement 5.1.2 is to acknowledge hackers invent new ways to hack into systems every day. It requires you to conduct research on your systems and pay attention to security notices from PCI vendors. If a new attack method is deemed a threat to your system, evaluate if the threat requires anti-virus.
Managerial Approval For Anti-virus

**Requirement 5.3**
This requirement states that anti-virus can’t be altered without managerial approval. Often, anti-virus needs to be turned off to do system maintenance. During maintenance, who knows what could slip past your unguarded system.

An effective method is if you are updating an application that requires disabling an anti-virus, don’t. Instead, take that system off the network or cut off its Internet connectivity for that updating period. As a side note, it’s not OK for system admins to just give all users admin access to get around the requirement. That’s missing the point entirely.

Software Development Practices

**Requirement 6.3**
Any custom software application for a cardholder environment (whether in-house or commissioned by a third party developer) is under your jurisdiction. It’s ok to outsource your software development, but it’s not OK to outsource your responsibility to ensure secure development practices are followed. If you’re planning to use the application, remember that it’ll be part of your PCI assessment…not your third party developer’s.

Broken Authentication

**Requirement 6.5.10**
This requirement to protect against broken authentication addresses common application vulnerabilities. You should create/add/adjust your application code to mitigate any exposure to vulnerabilities. This can be done by not exposing session IDs in URLs, using secure cookies, and enforcing appropriate session timeouts.

Role-based Access Control

**Requirement 7.1.1**
A role-based access control system means access to card data and systems should only be granted on a need-to-know basis. PCI 3.0 requires a defined list of the roles within your organization that have access to the card data environment.

On this list, you should include each role, definition of each role, access to data resources, privilege level, and what privilege level is necessary for each person to perform normal business responsibilities. Users must fit into one of the roles you outline. The less unnecessary access an employee has the better it is for your organization.
Password Policy

Requirement 8.4
It’s one thing to document policy, it’s another to implement it. Organizations are required to not just document, but also train their users on how to implement password policies. This training should include guidance on how to select a strong password, how to secure it, and instructions not to reuse it.

It’s also crucial that you communicate password policy to your users. This will help them understand how to change their passwords and also not use the same password between work and home.

Service Provider Remote Access

Requirement 8.5.1
This requirement is targeted specifically towards service providers who have remote access into a customer environment. This is common practice with vendors who do remote support or software training.

Any service provider with access to multiple customer systems is required to maintain unique credentials for each customer environment. The PCI Council knows this requirement in particular will take some time to change, so they’ve given until July 2015 before this is officially required.

Authentication Mechanisms

Requirement 8.6
The use of alternative authentication mechanisms (e.g., logical tokens, smart cards, certificates) must be tied to an individual user account and not shared among user accounts. To ensure this is met, every merchant must implement a control to enforce those authentication methods can only be used by the intended user (e.g., requiring a PIN, password, or biometric scan in addition to the token to validate the person is authorized).
Sensitive Area Access

**Requirement 9.3**
This requirement addresses the need to control employee access to sensitive areas, which must be related to an individual’s job function. To meet this requirement, we suggest documenting exactly who has access to these environments and their business need. A process should then be added to keep this information up to date, especially when individuals are terminated or their job role changes.

POS Hardware

**Requirement 9.9**
This is a very important requirement for the PCI standard. Organizations that use point of sale systems, PIN pads, mobile devices etc., are required to do three things:

1. **Maintain an up-to-date list of all devices (9.9.1)** including physical location, serial numbers, make/model.

2. **Periodically inspect devices (9.9.2)**. That means looking at device surfaces to make sure they haven’t been tampered with, making sure the serial numbers match, checking that seals haven’t been broken, etc. This could be a very large task depending on the size of your organization. Whether you inspect devices every day or month is based on how at risk you are of tampering (e.g., publically accessible 24/7 gas station terminals vs. a behind-the-counter card swipe device). Make sure you document what you find.

3. **Provide staff awareness training (9.9.3)** for staff that interact with card present devices on a day-to-day basis (e.g., cashiers), and record the who, what, and when for future reference. Ideally, the training will help staff detect any suspicious activity around a payment device. Training should include how to report suspicious behavior and what to do when third parties claim they need to work on the system. For example, rather than assuming IT came in last night to install a new device on the side of her terminal, an employee should question if its supposed to be there and notify appropriate persons.
Review Logs

**Requirement 10.6.2**
Depending on its size and complexity, this requirement could have a large impact on your environment. In addition to the logging requirements in 10.6.1, you’re now required to review logs of all other system components periodically, based on your policies and risk management strategy.

Many different systems in your environment may impact your payment security. As part of your annual risk assessment, you need to identify systems that pose risk and define a process to periodically look at their logs to determine suspicious activity.

Wireless Access Points

**Requirement 11.1.1**
It’s difficult to determine which wireless devices to remove if you don’t have an accurate list of them to begin with. That’s why the PCI Council requires you create a total list. If you’re a small ecommerce provider and all your systems fit into a single rack in your data center, this requirement should be pretty easy. If you’re a widespread organization, it will take a bit more time.

Maintaining a complete list of authorized wireless access points will require extra documentation, especially in large environments. This list should include a documented business justification for each wireless access point.

Penetration Testing Guidance

**Requirement 11.3**
This section provides guidance to both merchants and penetration testing organizations on penetration testing's intended coverage.

Penetration testing organizations are required to have documented and standardized testing methodologies that meet industry accepted standards, such as NIST 800.115. In addition, guidance is provided on how best to scope the penetration test and identify critical systems.
The PCI Council knows this requirement in particular will take some time to change, so they’ve given until July 2015 before the changes in the penetration testing requirement become official. However, this doesn’t mean you can wait to receive a penetration test until July 2015. The guidance provided in PCI DSS 2.0 for penetration testing is still valid until then.

Third Party Compliance

Requirement 12.8.5
Not only should merchants maintain a list of all their third-party service providers, but they must also maintain a list of all PCI requirements their service provider currently meets and is required to meet. This task may be revealing about who you choose as partners. If your partner doesn’t want to play, try shopping elsewhere.

Service Provider Disclosure

Requirement 12.9
In conjunction with Requirement 12.8.5, service providers are now required to provide written documentation to all customers stating which PCI requirements they cover on their behalf. These two requirements attempt to avoid past miscommunication problems between service providers and merchants.

Summary

Overall, PCI DSS 3.0 and 3.1 focus on detecting, rather than reacting to, security vulnerabilities. With improved aspects like documentation and system monitoring, these changes will increase proficiency among merchants, service providers, and PCI vendors alike.
About SecurityMetrics

SecurityMetrics has tested over one million payment systems for data security and compliance mandates. Its solutions combine innovative technology that streamlines validation with the personal support you need to fully understand compliance requirements. You focus on the business stuff—we’ve got compliance covered.

For questions about your PCI DSS compliance situation, please contact SecurityMetrics at sales@securitymetrics.com or 801.705.5656.