securityMETRICS®

White Paper

# NEW PENETRATION TESTING REQUIREMENTS, EXPLAINED

*The most important clarifications made in the PCI Council's penetration testing informational supplement*

© 2015 SecurityMetrics

# NEW PENETRATION TESTING REQUIREMENTS, EXPLAINED

## THE MOST IMPORTANT CLARIFICATIONS MADE IN THE PCI COUNCIL'S PENETRATION TESTING INFORMATIONAL SUPPLEMENT

To ensure minimal confusion with new PCI DSS requirements, the PCI Council also released a much-needed penetration testing informational supplement in March 2015 to replace the original five-page penetration test guidance written in 2008.

In PCI 2.0, penetration test requirements were essentially: perform external and internal penetration testing at least annually and after any significant infrastructure/application upgrade or modification. This included network-layer penetration test and application-layer penetration tests.

There was a short informational supplement released in 2008 by the PCI Council on penetration testing, but its guidance was very general and still left much room for interpreting what a penetration test really was.

PCI DSS 3.0 has expanded requirement 11.3, added clarity, and defined expectations.

The recently released 40-page penetration test informational supplement was created for merchants, penetration testers, and Qualified Security Assessors (QSAs). It mainly focuses on:

- Penetration testing components
- Qualifications of a pen tester
- Penetration testing methodologies
- Penetration testing reporting guidelines

We assisted in the creation of this informational supplement, and are eager to see how it will clarify requirements and assist penetration testers, QSAs, and merchants.

## PENETRATION TEST, VULNERABILITY SCAN, OR BOTH?

In addition to new penetration testing requirements, PCI 3.0 also updated the SAQ requirements for merchants and the applicability of penetration testing.

Based on your SAQ, here's a handy graph that explains exactly who is supposed to receive penetration tests and vulnerability scans to comply with the PCI DSS. (To determine which type of penetration tests apply, see similar graph on page 5)

| SAQ A | SAQ A-EP |
|---|---|
| 🟩 | 🟨 🟨 🟥 |
| SAQ B | SAQ B-IP |
| 🟩 | 🟧 |
| SAQ C | SAQ CVT |
| 🟨 🟧 🟥 | 🟩 |
| SAQ D | SAQ P2PE |
| 🟨 🟧 🟥 | 🟩 |

| | |
|---|---|
| 🟩 | NO SCANNING NEEDED |
| 🟨 | INTERNAL VULNERABILITY SCAN |
| 🟧 | EXTERNAL VULNERABILITY SCAN |
| 🟥 | PENETRATION TEST |

Read this article to better understand:
Difference Between a Penetration Test and Vulnerability Scan

## NEW PENETRATION TESTING METHODOLOGY

Let's review some of the newest and most important changes to PCI 3.0's requirement 11.3 penetration test requirements.

### USE INDUSTRY-ACCEPTED APPROACHES

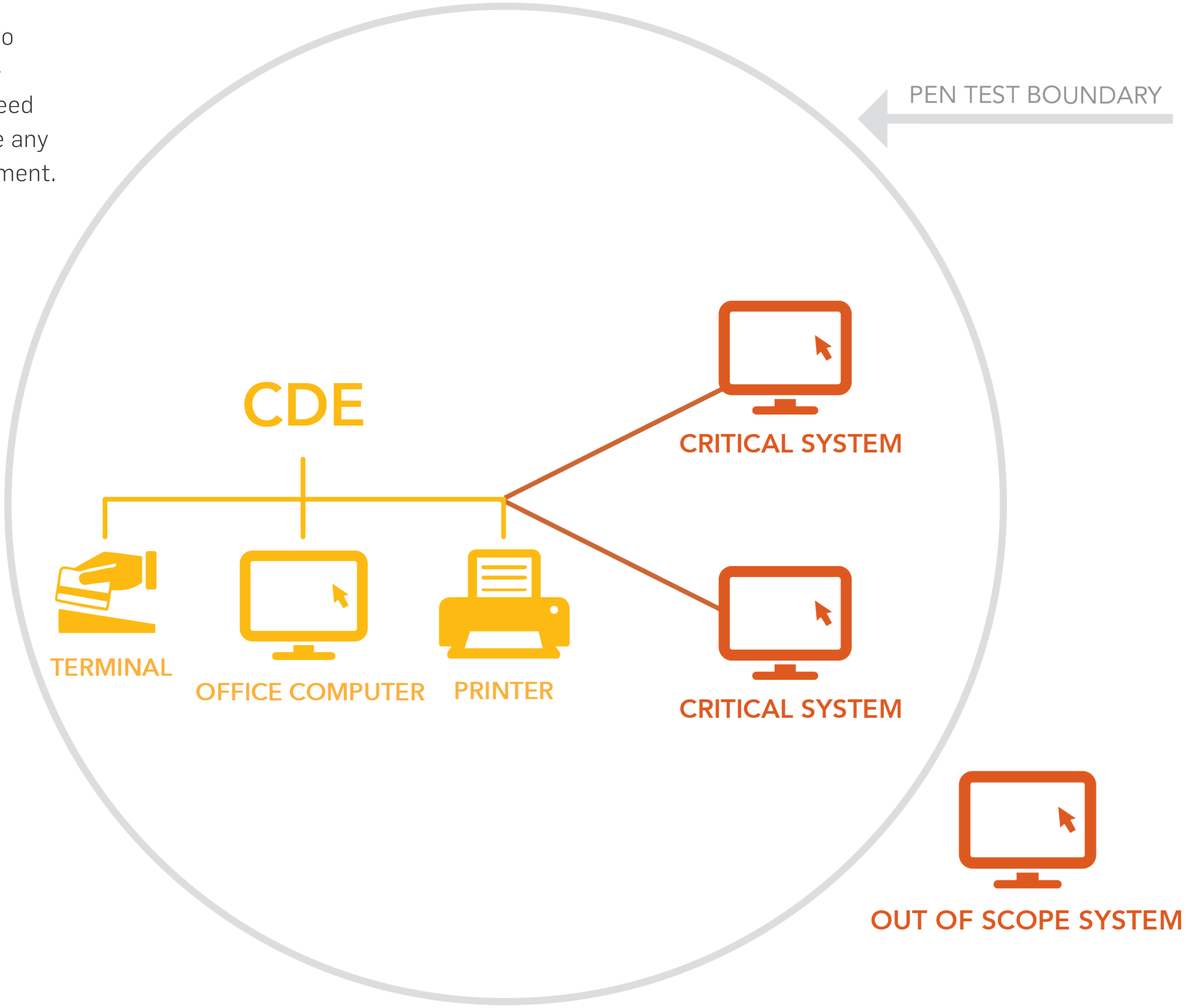
(Informational Supplement 4.4)
This clarification, included in Req. 11.3, helps us understand an industry-recognized methodology must be used when conducting a penetration test. Remember, the informational supplement was created for merchants, pen testers, and QSAs. This new methodology requirement applies to each of those audiences, but in different ways. Here's what we mean:

- **If you're a merchant:** you must make sure that the penetration tester you select uses the correct methodology and that you act on the report they give you (i.e., fix the problems they find.)
- **If you're a penetration tester:** you must use the correct pen testing methodology when conducting your test (e.g., NIST 800-115, OWASP Testing Guide, etc.).

## INCLUDE CRITICAL SYSTEMS IN THE PENETRATION TEST

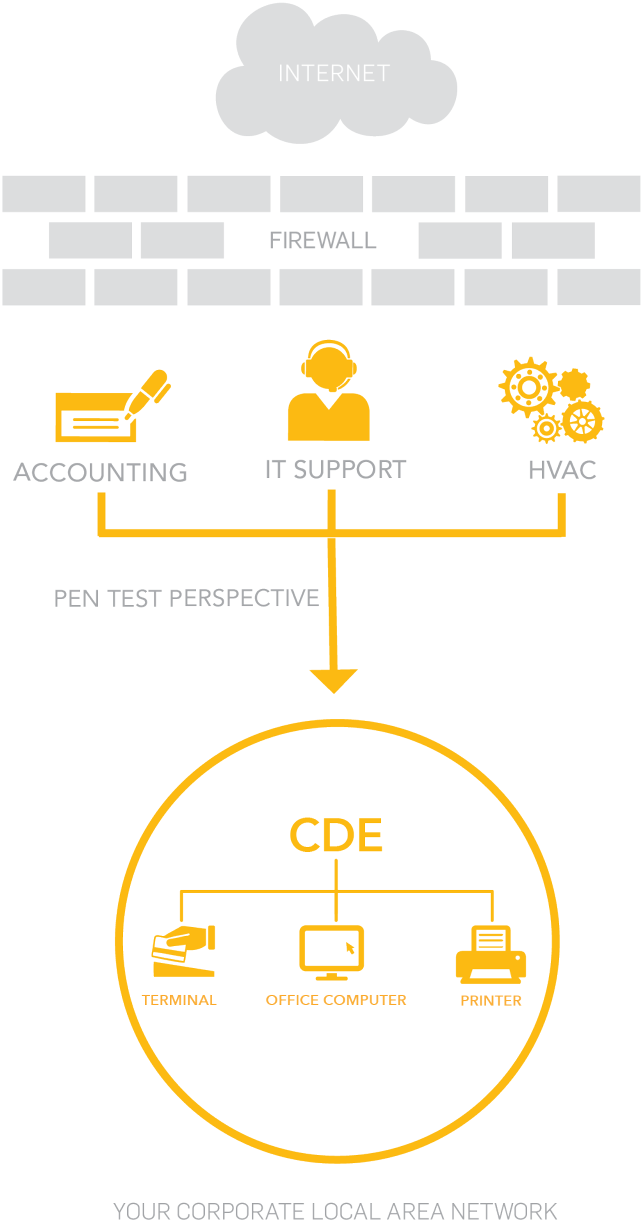
(Informational Supplement 2.2.1)
A critical system is any additional system outside of the card data environment boundary that could affect card data security. For example, firewalls, IDS, authentication servers, etc. Basically, any assets utilized by privileged users to support and manage the card data environment.

In PCI 3.0, penetration testers are not supposed to neglect the critical systems in a merchant's environment. Their scope for the pen test should exceed outside of the card data environment, and include any critical systems present in the merchant environment.

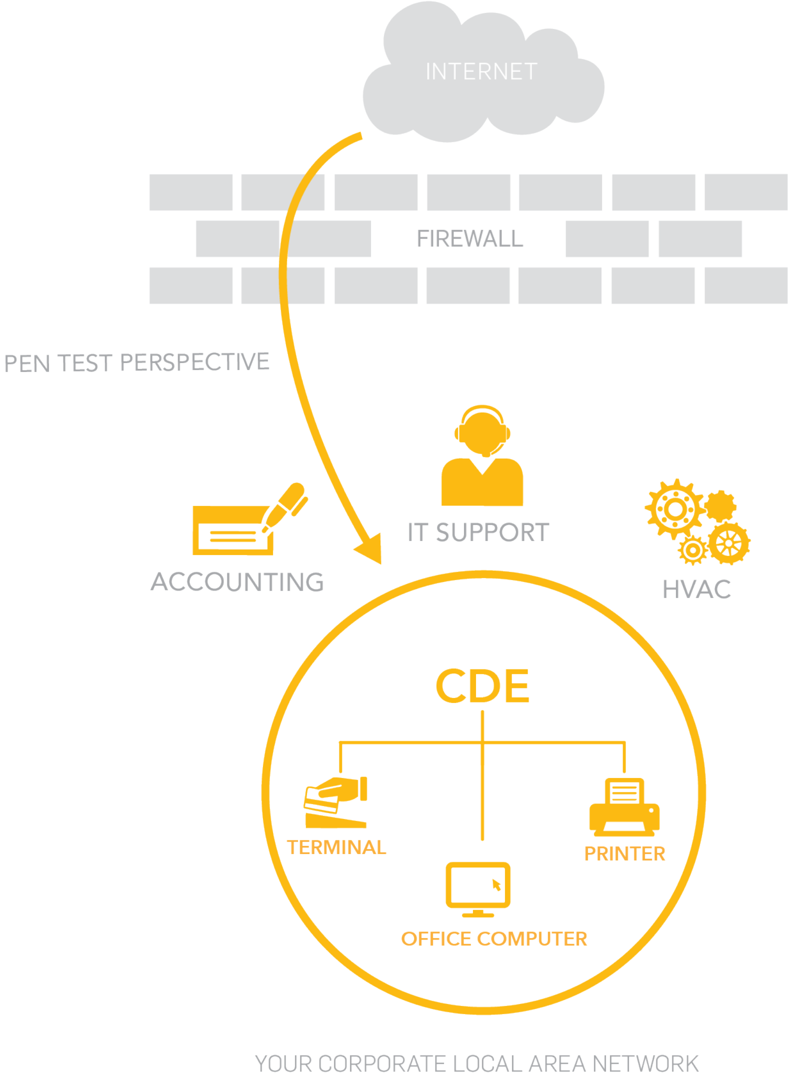


## CONTINUE EXTERNAL AND INTERNAL TESTING

(Informational Supplement 2.2)
An **internal penetration test** is when penetration testers test from the perspective internal to your corporate network, but outside of your card data environment.



An **external penetration test** is when penetration testers test from a perspective of an open public network (Internet) outside of the card data environment.



SAQ A-EP

🟡 🟠

SAQ C

🟠

SAQ D

🟢 🟡 🟠

🟢 INTERNAL PEN TEST

🟡 EXTERNAL PEN TEST

🟠 SEGMENTATION CHECK

The definition of internal and external testing didn't change in 3.0, but the merchants required to have an external or internal test did. Here's a quick graphic that explains which penetration tests are required based on your SAQ.

## PROVIDE AUTHENTICATION IN APPLICATION-LAYER AND NETWORK-LAYER TESTING

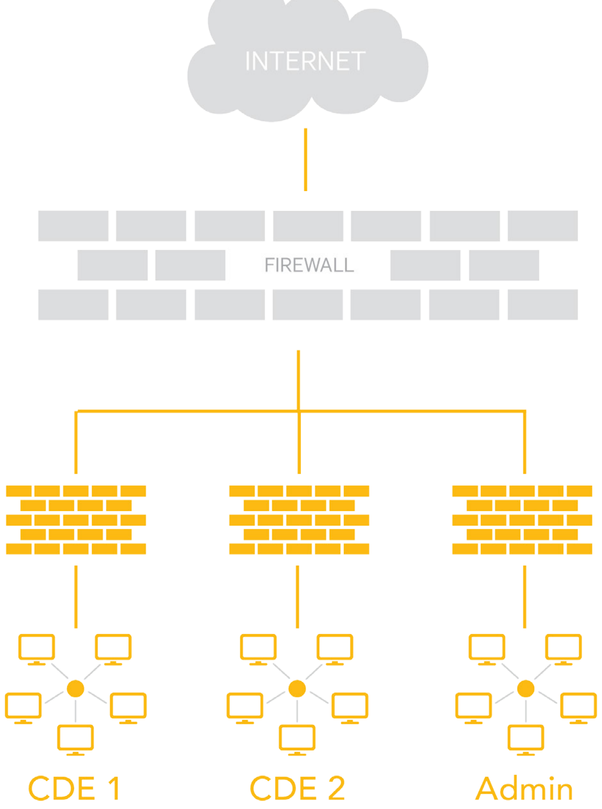
(Informational Supplement 2.3.1)
One of the clarifications detailed in this section is that penetration testers need to conduct an authenticated pen test. This means the customer must provide the penetration tester with credentials to access the system, instead of requesting that he try to penetrate their system blindly.

With credentials, the penetration tester can test the system via an administrator role, manager role, or cashier role, etc. and test if someone with a lesser privilege can get information that should only be accessible to someone with a higher privileges.

## START TESTING NETWORK SEGMENTATION

(Informational Supplement 2.4)
This is another big change to PCI 3.0 penetration test requirements. When merchants segment their network, they usually do so to take the network segments not involved in card processing totally out of scope for PCI. Segmentation checks are penetration tests that make sure the network segment outside of the Card Data Environment (CDE) is actually out of scope.

Penetration testers validate segmentation by running a port scan (often using NMAP) inside the out of scope network segment to try and discover an IP address inside the card data environment. If they can't see any IP addresses inside the CDE, that network segment is validated as properly segmented (or isolated from the CDE).



*MANY COMPROMISED MERCHANTS THOUGHT THEY WERE SECURE AND COMPLIANT, BUT OBVIOUSLY, THEY WEREN'T.*

### REVIEW OF PAST VULNERABILITIES AND THREATS

(Req. 4.1.6)
This brand new requirement explains that both merchants and penetration testers are responsible for reviewing a merchant's past vulnerabilities.

- **Merchant responsibility**: have you experienced a vulnerability in past 12 months? Like POODLE? Did you make changes? Tell your penetration tester about it so they can design tests to validate your changes.
- **Penetration tester responsibility**: Be aware of general vulnerabilities and threats prevalent in the industry and design tests to check for issues in customers' networks and applications.

### PENETRATION TESTS CAN MAKE ALL THE DIFFERENCE IN YOUR DATA SECURITY

A penetration test is the MRI for your business. It's the real-world security testing of the requirements you believe are in place. It's a way to actually see evidence of problems your security systems may have. If compromised merchants had tested their environment through a penetration test, they might have found the vulnerability that allowed attackers into their system, before it happened.

We encourage you to familiarize yourself with the informational supplement recently released by the PCI Council. When it comes time to comply with the penetration testing requirements, you'll better understand the who, what, when, where, and why.

securityMETRICS®

## ABOUT

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:

SALES@SECURITYMETRICS.COM OR 801.705.5656