# PROTIVITI FLASH REPORT

## The PCI Security Standards Council Releases PCI DSS Version 3.2

### May 9, 2016

On April 28, 2016, the PCI Security Standards Council (PCI SSC) released PCI Data Security Standard (PCI DSS) version 3.2, which had been available for preview to stakeholders since April 15.

The PCI DSS is a widely accepted set of policies and procedures used to optimize security of credit, debit and cash card transactions and protect cardholders from misuse of their personal information. Version 3.2's April release represents a change of pace in PCI DSS updates, occurring outside the PCI SSC's normal update cycle. (However, Troy Leach, chief technology officer of the PCI SSC, stated that no further revisions to the PCI DSS will occur in 2016.)

As with every prior version or release of PCI DSS, many clarifications have been made, along with clerical changes. But what the industry wants to know is which changes impact their business. Below, we have outlined the more notable changes for affected organizations.

### Major Changes for All Entities

These are changes in which processes or additional technologies will need to be deployed in order for an organization to remain in compliance with PCI DSS. The changes may lead to high levels of effort to achieve compliance and could cause organizations to be out of compliance for an extended period.

1. **Multi-factor authentication** – The term "multi-factor authentication" replaces "two-factor authentication." This in and of itself should not impact compliance for an organization, but a new requirement for use of multi-factor authentication for certain types of local access will do so. This is a two-part update: The first part is effective immediately when assessing compliance with v3.2, and the second part becomes effective February 1, 2018.
    - *Effective immediately*: Multi-factor authentication must be used for all remote access (originating from outside the entity's network), including users, administrators and third parties.
    - *Effective February 1, 2018*: Multi-factor authentication must be used for all administrative access to the cardholder data environment (CDE), even when connecting from an internal corporate network.

2. **File-integrity monitoring (FIM)** – The PCI SSC removed "within the cardholder data environment" from the testing procedures for the 11.5.a requirement. This could significantly impact those organizations that do not have FIM or other change-detection solutions on all in-scope systems (i.e., systems that connect to the cardholder environment). Many organizations do not necessarily have FIM technologies on, for example, point-of-sale or administrative workstations.
3. **Change management** – This is an area in which many entities have difficulty properly implementing a process and successfully documenting changes. The new requirement 6.4.6 adds steps to the existing change management controls. Organizations are now required to verify and document all PCI DSS requirements impacted by the change and to validate that they are still being met.

## Major Changes for Service Providers

The following requirements reveal that the PCI SSC is focusing on service providers and increasing the scrutiny of compliance for this group of organizations. Service providers will need to assess these changes and ensure they are in place in order to stay in compliance with PCI DSS.

1. **Security controls monitoring** – Service providers are required to monitor and report on failures of critical security systems.

   > *"The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline."*[1]

   Incident response/problem management processes need to be updated as applicable to include this process. Critical systems include, but are not limited to, the following:

   - Firewalls
   - Intrusion detection/intrusion prevention
   - FIM
   - Anti-virus
   - Physical access controls
   - Logical access controls
   - Audit logging mechanisms
   - Segmentation controls (if used)

[1] Payment Card Industry (PCI) Data Security Standard, "Requirements and Security Assessment Procedures," Version, 3.2, April 2016, page 94, www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf.

The following processes need to be added to the incident response/problem management program:

- Restoring security functions
- Identifying and documenting the duration (date and time, start to end) of the security failure
- Identifying and documenting the cause(s) of failure, including the root cause, and documenting remediation required to address the root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent the cause of failure from reoccurring
- Resuming monitoring of security controls

2. **Executive management responsibility** – Service providers are now required to assign the responsibility of PCI compliance to a representative of executive management. The PCI SSC defines "executive management" as a C-suite executive, a member of the board of directors or an equivalent individual. While service providers have a designated executive officer who signs the attestation of compliance (AOC), this step formally documents the responsibility.
3. **Operational reviews** – Service providers are required to perform quarterly reviews of operational processes. These include but are not limited to the following:
    - Daily log reviews
    - Firewall rule-set reviews
    - Application of configuration standards to new systems
    - Response to security alerts
    - Change management processes

## Other Notable Changes

1. **Penetration testing** – Service providers are now required to test segmentation controls (if segmentation is used to reduce scope) at least every six months, compared to at least annually in v3.1.
2. **Documented description of cryptographic architecture** – Service providers are required to create a documented description of the cryptographic architecture used in the CDE. This document must include the following:
    - Details of all algorithms, protocols and keys used for the protection of cardholder data, including key strength and expiry date

- Description of the key usage for each key
- Inventory of any hardware security modules and other secure cryptographic devices used for key management

## Migrating from Secure Socket Layer (SSL) and Early Transport Layer Security (TLS)

Migrating away from SSL and early TLS has been an area of discussion for the past few years. Most organizations should have this on their road map already, if not already completed. The PCI SSC released a bulletin on December 15, 2015, updating the migration cutoff date for entities still using SSL or early TLS to June 30, 2018 (previously June 30, 2016). This update is now reflected in PCI DSS v3.2 along with moving the controls into Appendix A-2.

## Key Dates and Deadlines

- The next Payment Application Data Security Standard (PA-DSS) update will be released in approximately one month.
- PCI DSS v3.1 will be retired on October 31, 2016.
- Seven changes have an effective date of February 1, 2018. These changes impact the following requirements:
    - 3.5.1 – Documenting cryptographic architecture
    - 6.4.6 – Assessment of PCI DSS requirements impacted by each change
    - 8.3.1 – Multi-factor authentication for all access to CDE
    - 10.8, 10.8.1 – Detecting and reporting failures in critical security control systems
    - 11.3.4.1 – Penetration testing segmentation controls at least every six months
    - 12.4 – Executive management responsibility for protecting cardholder data
    - 12.11, 12.11.1 – Quarterly reviews of operational processes
- Migrating from SSL and early TLS has been pushed to June 30, 2018.

## In Closing

Companies should review the summary of changes and determine which of them will impact their environment for PCI compliance. Key items would include any controls that have increased in frequency or controls that now have frequency requirements.

## About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Ranked 57 on the 2016 *Fortune* 100 Best Companies to Work For® list, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

## Contacts


**Scott Laliberte**
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

**Mark Lippman**
Managing Director
+1.571.382.7807
mark.lippman@protiviti.com

**Chris Louden**
Managing Director
+1.703.350.4397
chris.louden@protiviti.com

**Michael Porier**
Managing Director
+1.713.314.5030
michael.porier@protiviti.com

**Andrew Retrum**
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com

**Jeff Sanchez**
Managing Director
+1.213.327.1433
jeffrey.sanchez@protiviti.com

**Cal Slemp**
Managing Director
+1.203.905.2926
cal.slemp@protiviti.com

**David Stanton**
Managing Director
+1.469.374.2488
david.stanton@protiviti.com

**David Taylor**
Managing Director
+1.407.849.3916
david.taylor@protiviti.com

**Michael Walter**
Managing Director
+1.404.926.4301
michael.walter@protiviti.com

**Jeff Weber**
Managing Director
+1.412.402.1712
jeffrey.weber@protiviti.com



© 2016 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and
does not issue opinions on financial statements or offer attestation services.


protiviti®
Risk & Business Consulting.
Internal Audit.