



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Prioritized Approach – Summary of Changes from PCI DSS Version 1.2 to 2.0**

**April 2011**

# PCI DSS Prioritized Approach

## Summary of Changes from PCI DSS Version 1.2 to 2.0

Type of Change	Details
General	Updated Requirements and Testing Procedures to align with PCI DSS version 2.0.
Milestones	<p>The following milestone changes were made to reflect the evolving risk environment, and to align requirements with milestone control areas:</p> <ul style="list-style-type: none"> <li>▪ PCI DSS Requirement 9.1 moved to Milestone 2</li> <li>▪ PCI DSS Requirement 10.5 moved to Milestone 4</li> <li>▪ PCI DSS Requirement 11.1 moved to Milestone 4</li> <li>▪ PCI DSS Requirement 11.3 moved to Milestone 2</li> <li>▪ PCI DSS Requirement 12.1.2 moved to Milestone 1</li> <li>▪ PCI DSS Requirement 12.5.3 moved to Milestone 4</li> <li>▪ PCI DSS Requirement 12.9 moved to Milestone 4</li> </ul>
Prioritized Approach Tool	Added “Stage of Implementation” column for organizations to track the progress of implementation for non-compliant requirements.
Prioritized Approach Tool	Added “Estimated Date for Completion of Milestone” column for organizations to record target completion dates for each non-compliant requirement. Target dates for non-compliant requirements are then consolidated for each milestone in the Summary table.

### Disclaimer

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. This document does not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation whatsoever regarding the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.