



# IT Infrastructure Compliance of the Payment Card Industry Data Security Standard (PCI DSS)

---

**October, 2011**

This guide offers general information regarding compliance with the PCI DSS. Please consult PCI DSS materials for complete requirements (web resources are included below).

## Overview of the PCI Data Security Standard (DSS)

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. The standard is managed by the PCI Security Standards Council (PCI SSC). It consists of common sense steps that mirror security best practices. If your organization accepts credit cards, you must be PCI DSS compliant, and must complete the compliance questionnaire annually.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

*Source: PCI DSS Quick Reference Guide*

The Self-Assessment Questionnaire (SAQ) is a validation tool for eligible merchants and service providers who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance. The SAQ includes a series of yes-or-no questions for compliance. There are five SAQs, designed for different business environments. The PCI DSS Self-Assessment Questionnaire Guidelines and Instructions document provides more details on each SAQ type (see [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)).

As of January 1, 2011, the current version of PCI DSS is 2.0. The current lifecycle for changes to PCI DSS is 36 months, but the PCI Security Standards Council will continuously evaluate evolving technology and threats, and if necessary, make mid-lifecycle changes to the standards or provide ongoing supplemental guidance about these issues. Unfortunately, there is no single program, firm, or device that can make you PCI compliant.

## The Role of CRU Solutions in Supporting Your Organization’s PCI DSS Compliance Effort

Many of the PCI DSS compliance standards are directly related to your IT infrastructure, and that’s where CRU Solutions comes in. To date, most CRU clients would complete Self-Assessment Questionnaire “C”, so those are the questions we will address here. If you are a CRU Managed Services client, please contact your CRU representative for assistance in determining your SAQ level.

CRU has taken several proactive measures to help all our clients achieve PCI DSS compliance. As part of your Managed Services package and based on the structure of your network, CRU will advise you in the following areas (highlighted in yellow) that are specifically required by PCI DSS. We will recommend steps to be compliant in the other areas:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

### Goal 1: Build and Maintain a Secure Network

*Requirement 1: Install and maintain a firewall configuration to protect cardholder data*

- Proper Internet security is a top priority for CRU Managed Services clients, and suitable firewall configuration is part of our normal service. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

*Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*

- CRU advises our clients to change vendor-supplied default passwords. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

## **Goal 2: Protect Cardholder Data**

*Requirement 3: Protect stored cardholder data*

- This only applies if you are storing cardholder data at your location rather than using an online service or an online credit card processor. While this can be a bit confusing, the “storing at your location” means that the card number can be found within your four walls in writing or electronically. Please refer to PCI DSS SAQ for instructions on properly completing this section.

*Requirement 4: Encrypt transmission of cardholder data across open, public networks*

- There are a lot of “moving parts” in this requirement. CRU will work with you to see how this applies to you. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

## **Goal 3: Maintain a Vulnerability Management Program**

*Requirement 5: Use and regularly update anti-virus software or programs*

- If your company uses CRU KES anti-virus, it meets the specifications of Requirement 5, including audit log specifications. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

*Requirement 6: Develop and maintain secure systems and applications*

- CRU monthly patch management helps meet the specifications of Requirement 6. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

## **Goal 4: Implement Strong Access Control Measures**

*Requirement 7: Restrict access to cardholder data by business need to know*

- Consult your organization’s personnel policies to complete this requirement.

*Requirement 8: Assign a unique ID to each person with computer access*

- Unique login IDs are considered “best practices” and recommended for all CRU Managed Services clients. If you have questions about how this applies to your network, contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

*Requirement 9: Restrict physical access to cardholder data*

- Consult your organization’s personnel policies to complete this requirement. If you need to update your policies or you don’t have a thorough policies handbook, CRU Solutions can refer you to a firm that can help.

## Goal 5: Regularly Monitor and Test Networks

*Requirement 10: Track and monitor all access to network resources and cardholder data*

- Consult your organization's personnel policies to complete this requirement.

*Requirement 11: Regularly test security systems and processes*

- This specification requires quarterly internal and external vulnerability scans. CRU can monitor for some items and can help you pick an outside source to test your security for compliance. Contact CRU Solutions technical support and we will collect and provide you with the correct information specific to your network.

## Goal 6: Maintain an Information Security Policy

*Requirement 12: Maintain a policy that addresses information security for all personnel*

- This specification defines the types of policies that must be included within your organization's personnel policies to address information security. CRU can refer you to a specialist or consult your human resources advisor to ensure that these requirements are met.

### Summary

While we cannot complete the PCI-DSS compliance questionnaire for you, the team at CRU Solutions will do all we can to assist you by providing the technical information you need to complete it. We will continue to monitor PCI DSS requirements and implement new services to help make compliance easier, as well as delivering the ongoing support you expect to ensure that you remain in compliance. Unfortunately, there is no single program, firm, or device that can make you PCI compliant.

### Additional Web Resources

PCI Security Standards Council Web site, including Frequently Asked Questions (FAQs):  
[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Webinars:

[www.pcisecuritystandards.org/news\\_events/events.shtml](http://www.pcisecuritystandards.org/news_events/events.shtml)

The Standard:

[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

Supporting Documents:

[https://www.pcisecuritystandards.org/security\\_standards/documents.php](https://www.pcisecuritystandards.org/security_standards/documents.php)

Approved Assessors and Scanning Vendors:

[https://pcisecuritystandards.org/approved\\_companies\\_providers/index.php](https://pcisecuritystandards.org/approved_companies_providers/index.php)

Navigating the Standard:

[https://www.pcisecuritystandards.org/documents/navigating\\_dss\\_v20.pdf](https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf)

Self-Assessment Questionnaire:

[https://www.pcisecuritystandards.org/merchants/self\\_assessment\\_form.php](https://www.pcisecuritystandards.org/merchants/self_assessment_form.php)