Compliance with the Payment Card Industry Data Security Standard

Overview:

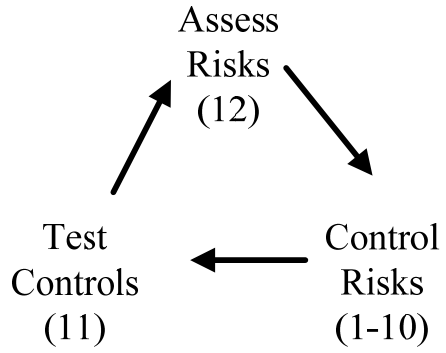
In September of 2006, the Payment Card Industry (PCI) Security Standards Council issued version 1.1 of the Data Security Standard (DSS). This standard specifically requires that organizations handling credit cards use Intrusion Detection Systems (IDS) and conduct formal risk assessment among another 205 required precautions.

Background:

The Payment Card Industry (PCI) Data Security Standard (DSS), like the Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accessibility Act (HIPAA) and other information security regulations, involves three basic steps;

- Conduct a risk assessment
- Design safeguards to control the identified risks
- Test the controls

Repeat steps at least annually.



This process is shown graphically at right for the PCI DSS. Risk assessment is in DSS requirement 12, controls in DSS requirements 1-10 and testing in DSS requirement 11.

The PCI Security Standards Council (SSC) has taken the lead in certifying testing firms, and a list of certified firms is available on their website. However, the SSC has declined to provide guidance in meeting the needs for sections 12 and 1-10 of the DSS. IDS for example falls into sections requirements 10.6 and 11.4 (see PCI DSS).

ACR 2 together with ACR 2 partners such as RLPC and BAI Security can provide regulated firms with services meeting most of the DSS requirements. The ACR 2 leadership presence on the PCI Security Vendor Alliance (SVA) provides a wealth of referrals to reputable vendors covering all of the DSS requirements.

Simplified Step by Step DSS Compliance Approach:

Under the PCI DSS and similar regulations, the link between safeguards and testing of safeguards is the risk assessment. There are three steps to coming into compliance;

1. Use the ACR software to produce an annual risk assessment that meets the requirements of the DSS 12.1.2. as shown.

12.1.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment

2. Implement safeguards identified by the risk assessment.

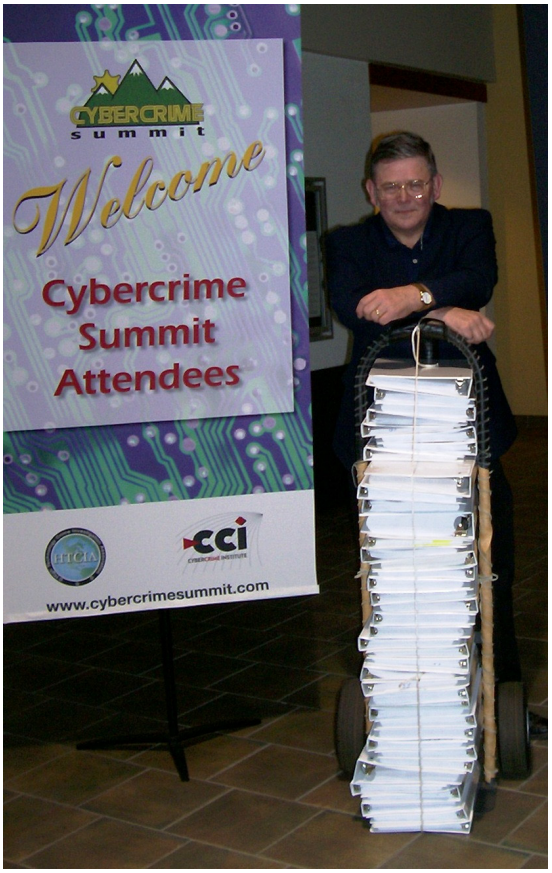
a. Use the Gap Report output of the ACR risk assessment to identify the services offered by ACR 2 partners that meet the specific requirements of DSS sections 1-10.

b. Implement the safeguards needed to plug the identified gaps.

3. After implementing the DSS requirements, obtain a Vulnerability Assessment from one of the SSC certified vulnerability testing groups. This also needs to be done annually.

Incorporate the results of the Vulnerability Assessment into a revised risk assessment and repeat as needed.

Each step is detailed separately.

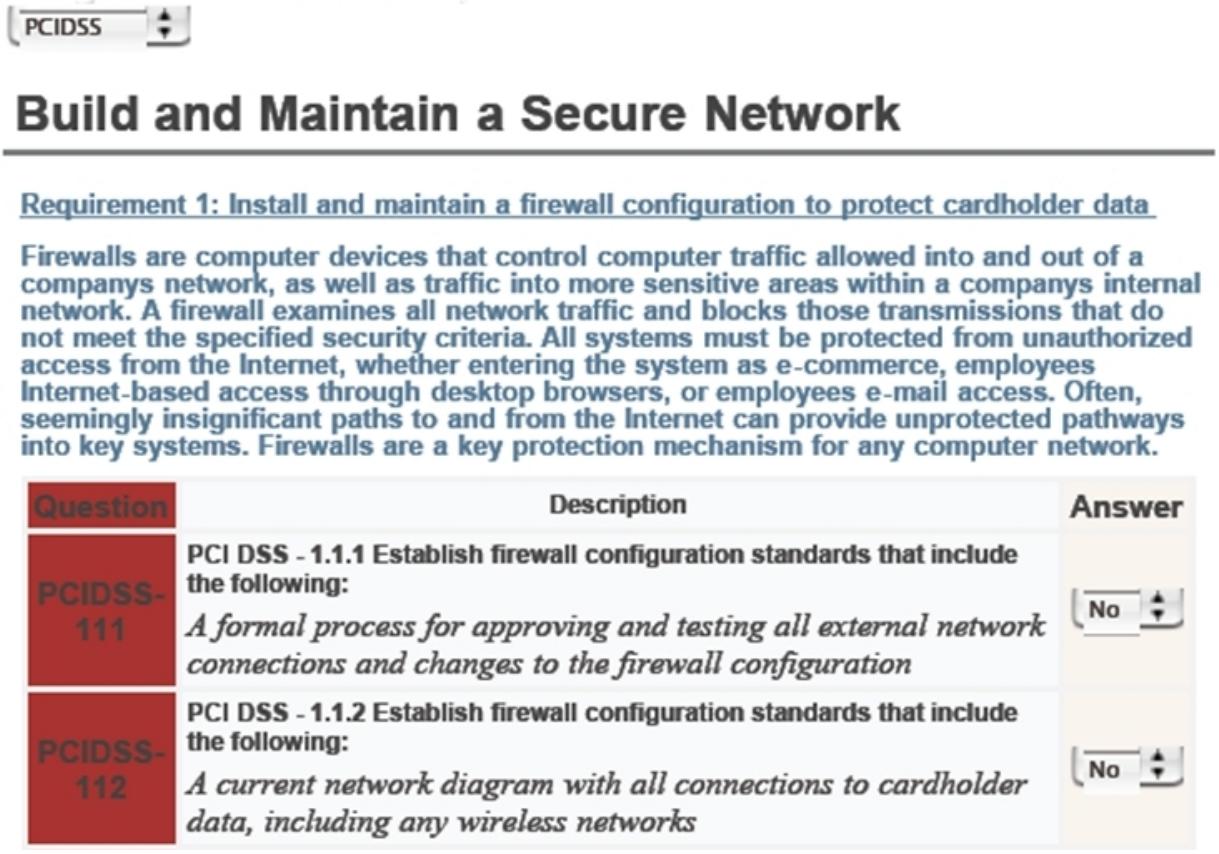


1. Risk Assessment - ACR is a leader in the production of automated risk assessment software, and ACR risk assessments have been audited by a variety of state and federal agencies. The ACR risk assessment program is a restating of US federal protocols. This reduces potential liability, since the regulators are using the same protocols as the regulated organizations. A single copy of the applicable protocols is shown at right.

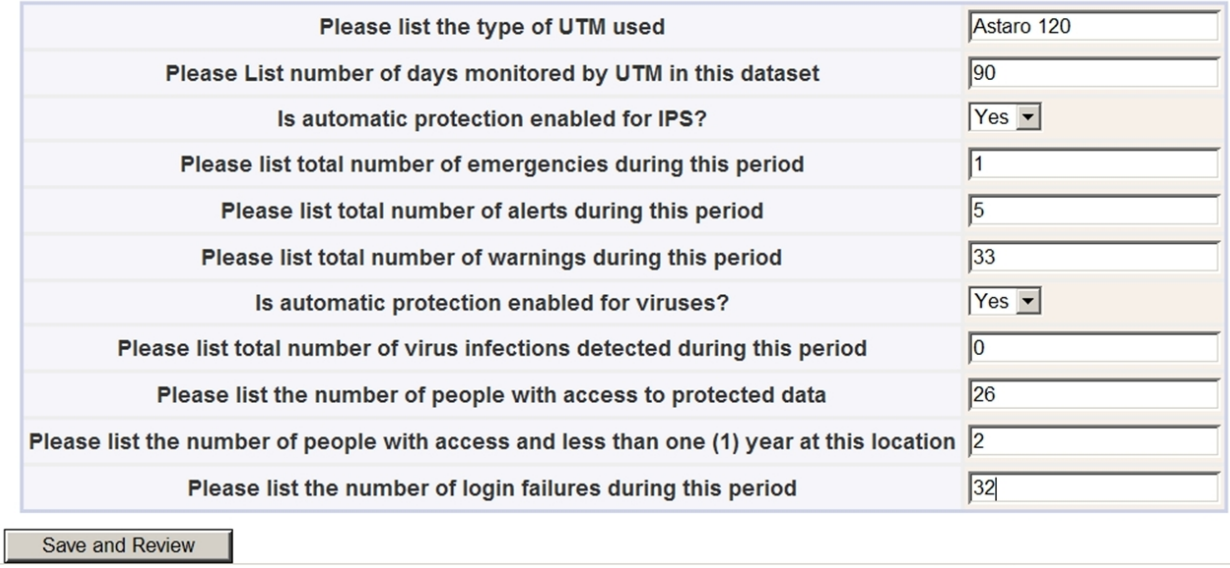
The "Turbo-Tax™" style risk assessment software was originally developed and applied to banks, which are regulated far more stringently than retailers.

In 2007 ACR developed a PCI version of its banking risk assessment program. The risk assessment program begins with a simple questionnaire of the form shown following. The user answers the questions using the drop down menu to input "No" the safeguard is not used, "Yes" it is in place and effective or "N/A" the safeguard does not apply to this location. The

safeguards listed are minimum standards set by either the PCI DSS or by the NIST under the "compensating controls" appendix of the PCI DSS.



Analog data is input using the form shown below;



At the end of each page of data input, the “Save and Review” button is pressed to save the data. A risk assessment can be done in one sitting, about three hours, or divided into separate authors and an unlimited number of sessions.

The output of the risk assessment includes a tabulated list of risk scores, a graphic showing the same data, and a Gap Report showing the missing safeguards.

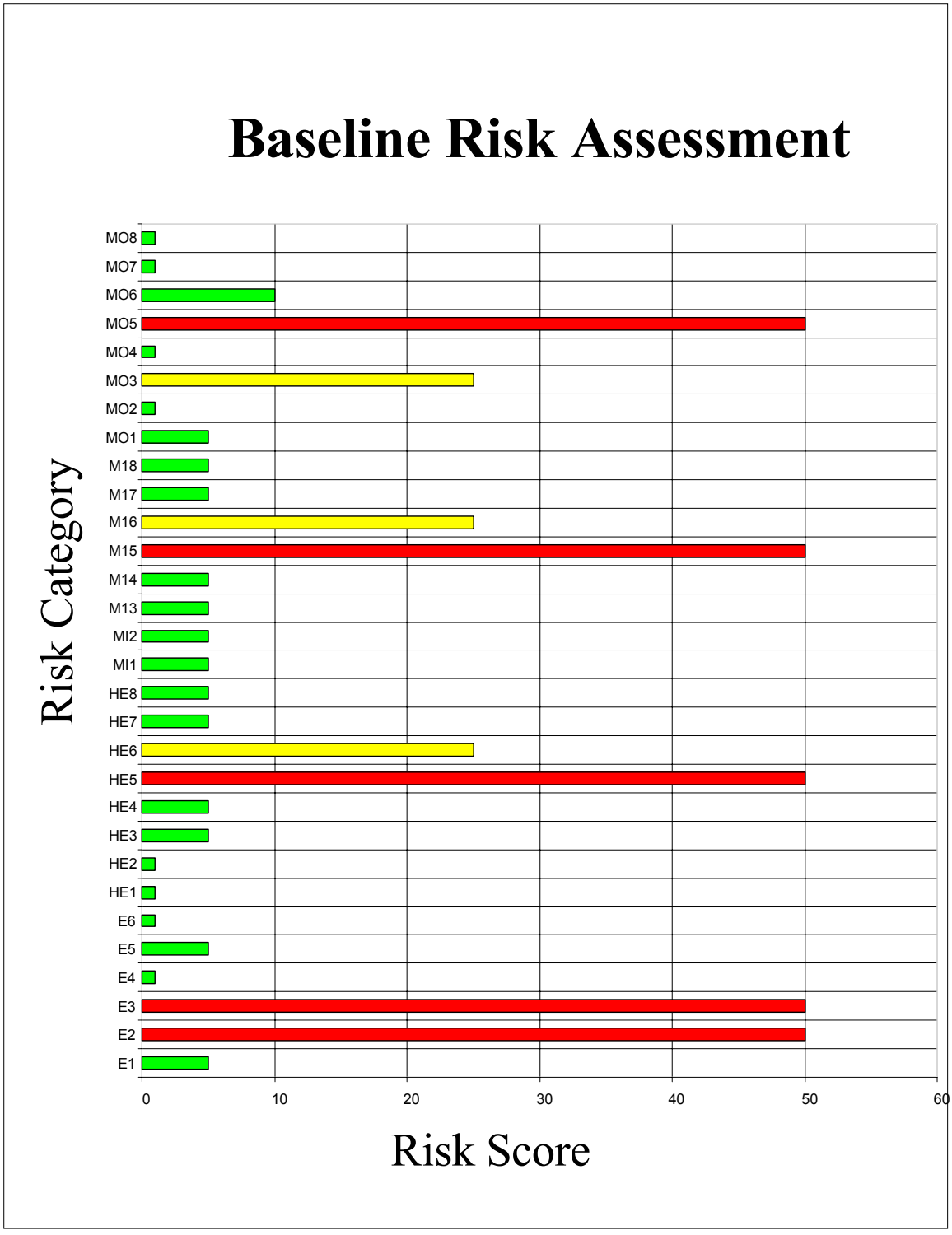
A sample of the risk assessment table is shown below. The risks to protected information include environmental risks, human error, malicious insiders and malicious outsiders.

Automated Baseline Report

Risk Assessment Number 11-15-06-1163616439 - Report Generated January 22, 2007 - www.acr2solutions.com

Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
Wind	Roof damage	M	M	25
Fire	Smoke damage	M	M	25
Flood	Facility damage	M	M	25
Power loss	Loss of operations	H	M	50
Power loss	Damage to building	H	M	50
Vehicle collision	Facility damage	M	M	25
Human error	Data acquisition	M	M	25
Human error	Data storage	M	M	25
Human error	Data retrieval	M	M	25
Human error	Data modification	M	M	25
Human error	Data transmission	M	M	25
Human error	System design	M	M	25
Human error	Procedure implementation	M	M	25
Human error	Internal controls	M	M	25
Malicious insider	Data acquisition	M	M	25
Malicious insider	Data storage	M	M	25
Malicious insider	Data retrieval	M	M	25
Malicious insider	Data modification	M	M	25
Malicious insider	Data transmission	M	M	25
Malicious insider	System design	M	L	5
Malicious insider	Procedure implementation	M	M	25
Malicious insider	Internal controls	M	M	25
Malicious outsider	Data acquisition	M	M	25
Malicious outsider	Data storage	M	M	25
Malicious outsider	Data retrieval	M	M	25
Malicious outsider	Data modification	M	M	25
Malicious outsider	Data transmission	M	M	25
Malicious outsider	System design	M	M	25
Malicious outsider	Procedure implementation	M	L	5
Malicious outsider	Internal controls	M	L	5

This information can also be shown graphically, as in the following example from a different risk assessment. The risk assessment graph provides a easy to review output allowing the customer to see their strong and weak points at a glance. The risk assessment can be updated at any time, so that progress in meeting standards is easy to communicate to managers and staff.



2. Gap Report - The Gap Report, with a partial sample following, closes the loop for the client. This report identifies specific requirements that are not in place at the client's location and matches them up to specific service providers.

The Gap report provides both a solutions provider web page and an optional compensating control, as provided for in the PCI DSS.

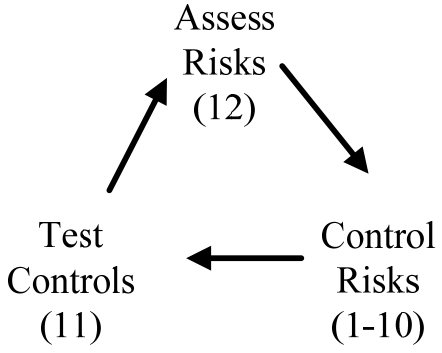
	Products and Services Required Under the PCI DSS and Missing From This Location	Solutions Provider Web-pages	Compensating Controls
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
	4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:		
	o Use with a minimum 104-bit encryption key and 24 bit-initialization value	Vendor	IA-1, IA-3
	o Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS		
	o Rotate shared WEP keys quarterly (or automatically if the technology permits)		
	o Rotate shared WEP keys whenever there are changes in personnel with access to keys		
	o Restrict access based on media access code (MAC) address.		
Requirement 5: Use and regularly update anti-virus software or programs			
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)			
	5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	Vendor	SI-8, AC-20
Requirement 12: Maintain a policy that addresses information security for employees and contractors			
12.5 Assign to an individual or team the following information security management responsibilities:			
	12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	Vendor	IR-1, IR-6
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.			
	12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	Vendor	AT-3

Following vendor negotiations and safeguards installation, it is usually good to have a period of weeks of "normal operations" before testing the upgraded system.

3. Vulnerability Testing - The SSC has provided a list of approved scanning vendors. This list should be updated before contracting for a vulnerability scan, since annual re-approval is required for scanning vendors.

Summary

Compliance with the PCI DSS is a straightforward three step process. Assess risks, control risks and test the controls at least annually. Repeat as needed. Using the correct tools, the time and expense of PCI compliance can be minimized while reducing the potential for catastrophic loss of customer data.



For more information, contact ACR 2 at sales@acr2compliance.com.