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.

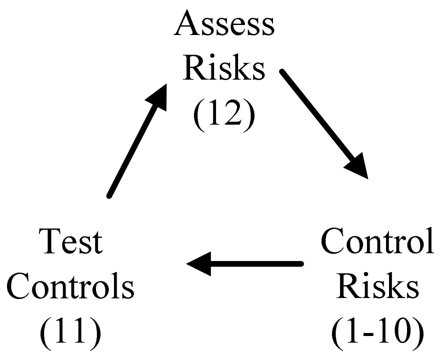
Background:

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.

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.

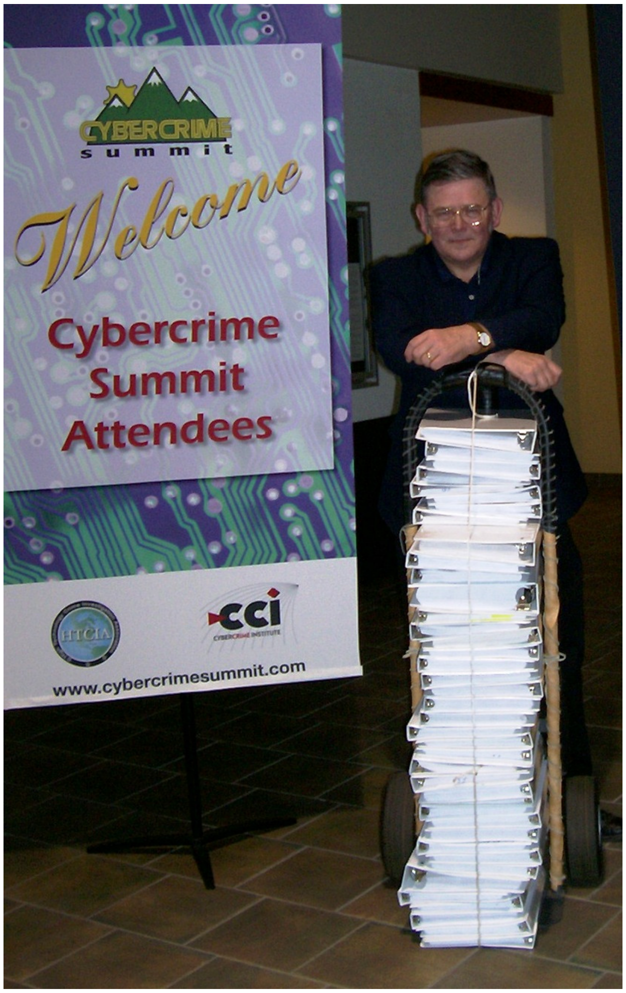
b. Implement the safeguards needed to plug the identified gaps.

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.



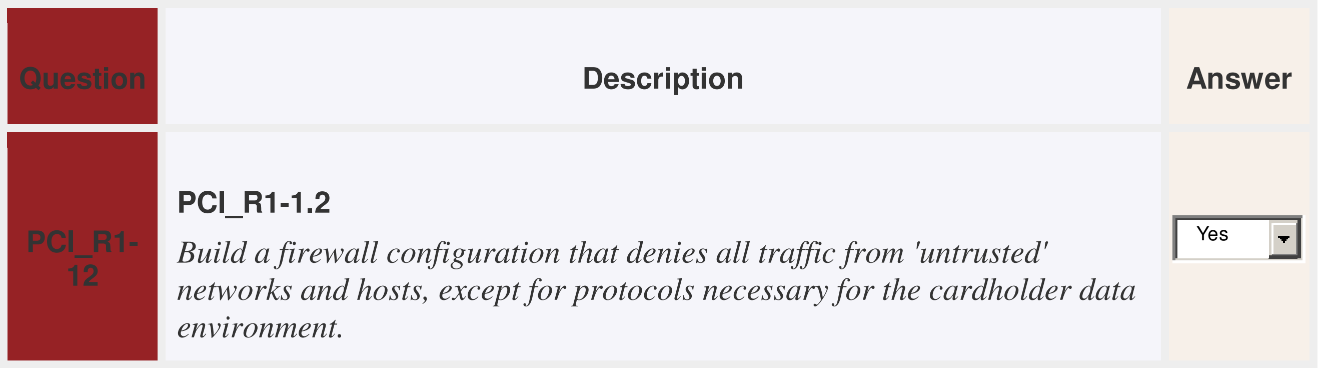
This artificial intelligence expert system risk assessment software was originally developed and applied to banks, which are regulated far more stringently than retailers.

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.

Build and Maintain a Secure Network

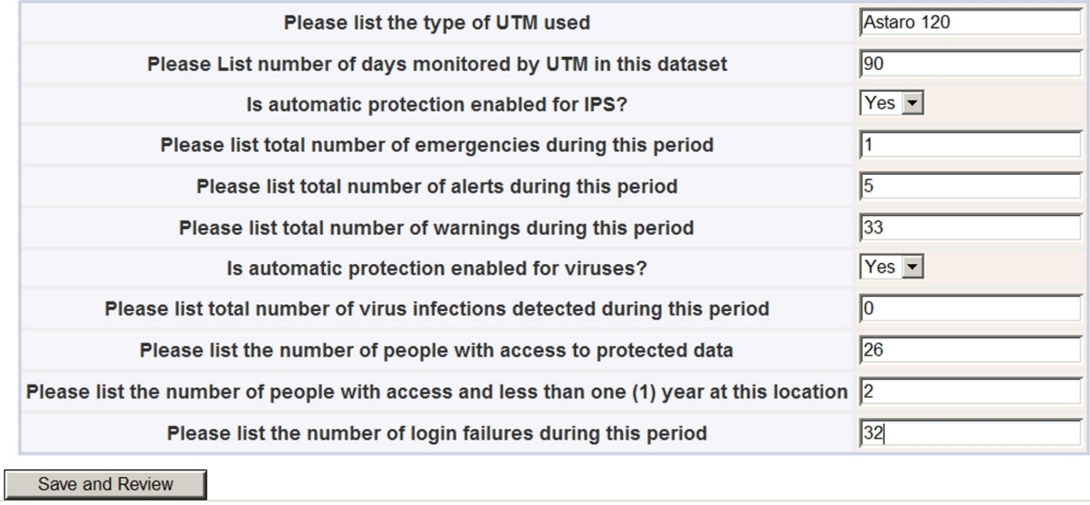
Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company’s network, as well as traffic into more sensitive areas within a company’s internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees? Internet-based access through desktop browsers, or employees? e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.



Question	Description	Answer
PCI_R1-12	**PCI_R1-1.2** *Build a firewall configuration that denies all traffic from 'untrusted' networks and hosts, except for protocols necessary for the cardholder data environment.*	Yes

Analog data is input using the form shown below;

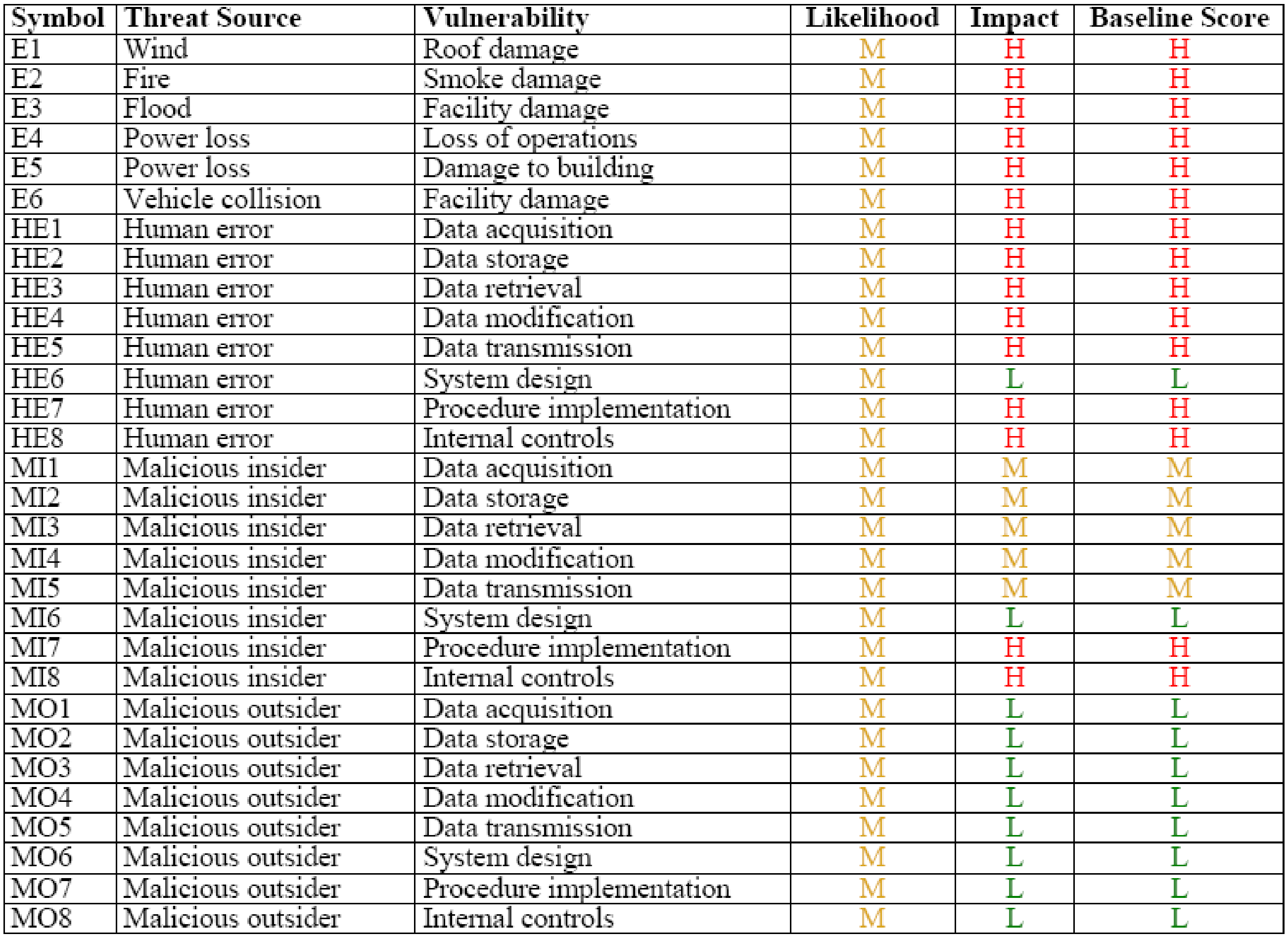


Please list the type of UTM used	Astaro 120
Please List number of days monitored by UTM in this dataset	90
Is automatic protection enabled for IPS?	Yes
Please list total number of emergencies during this period	1
Please list total number of alerts during this period	5
Please list total number of warnings during this period	33
Is automatic protection enabled for viruses?	Yes
Please list total number of virus infections detected during this period	0
Please list the number of people with access to protected data	26
Please list the number of people with access and less than one (1) year at this location	2
Please list the number of login failures during this period	32

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.

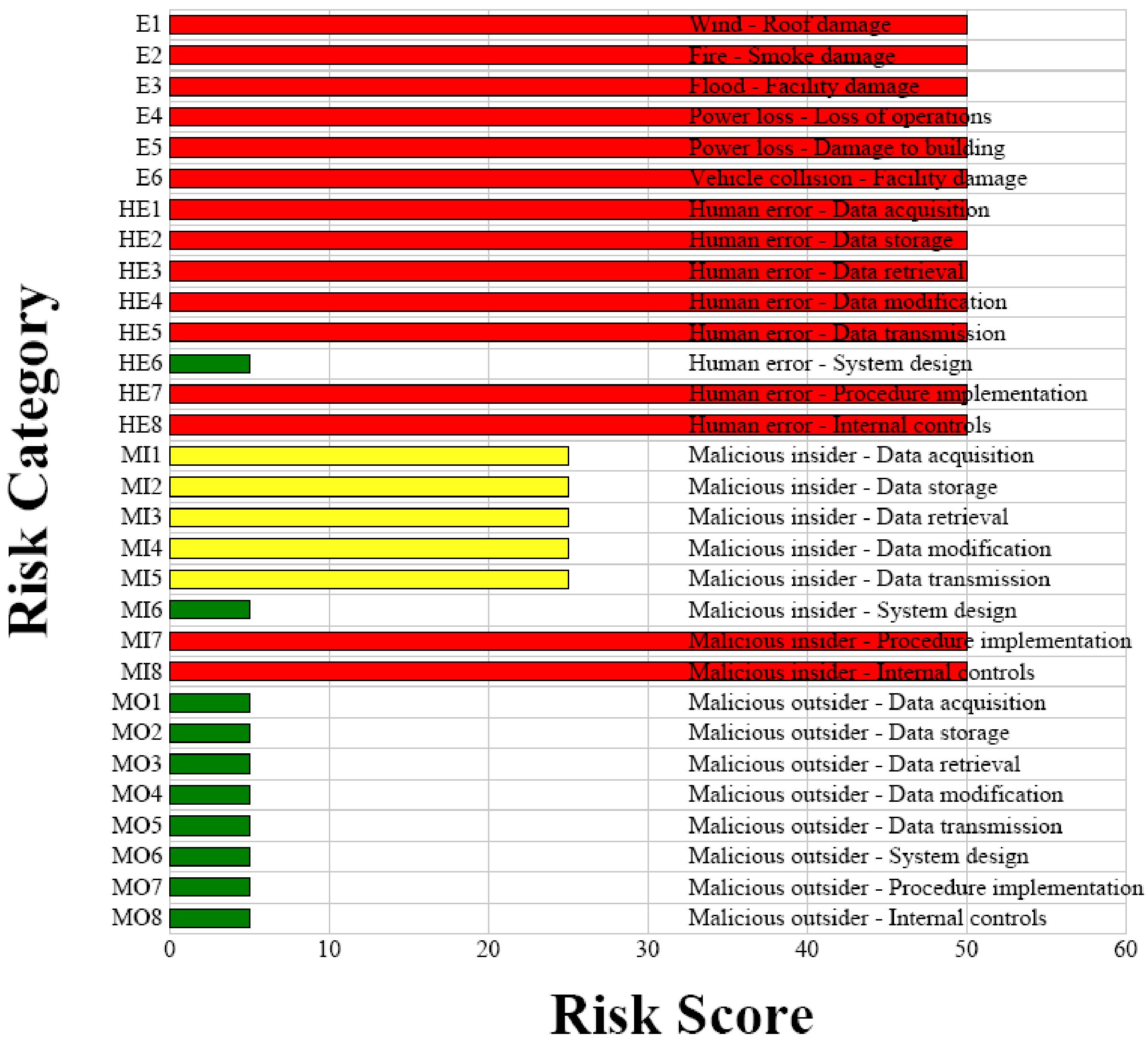
The output of the risk assessment includes a tabulated list of risk scores, a graphic showing the same data, and a Gap Report showing the missing safeguards.

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.



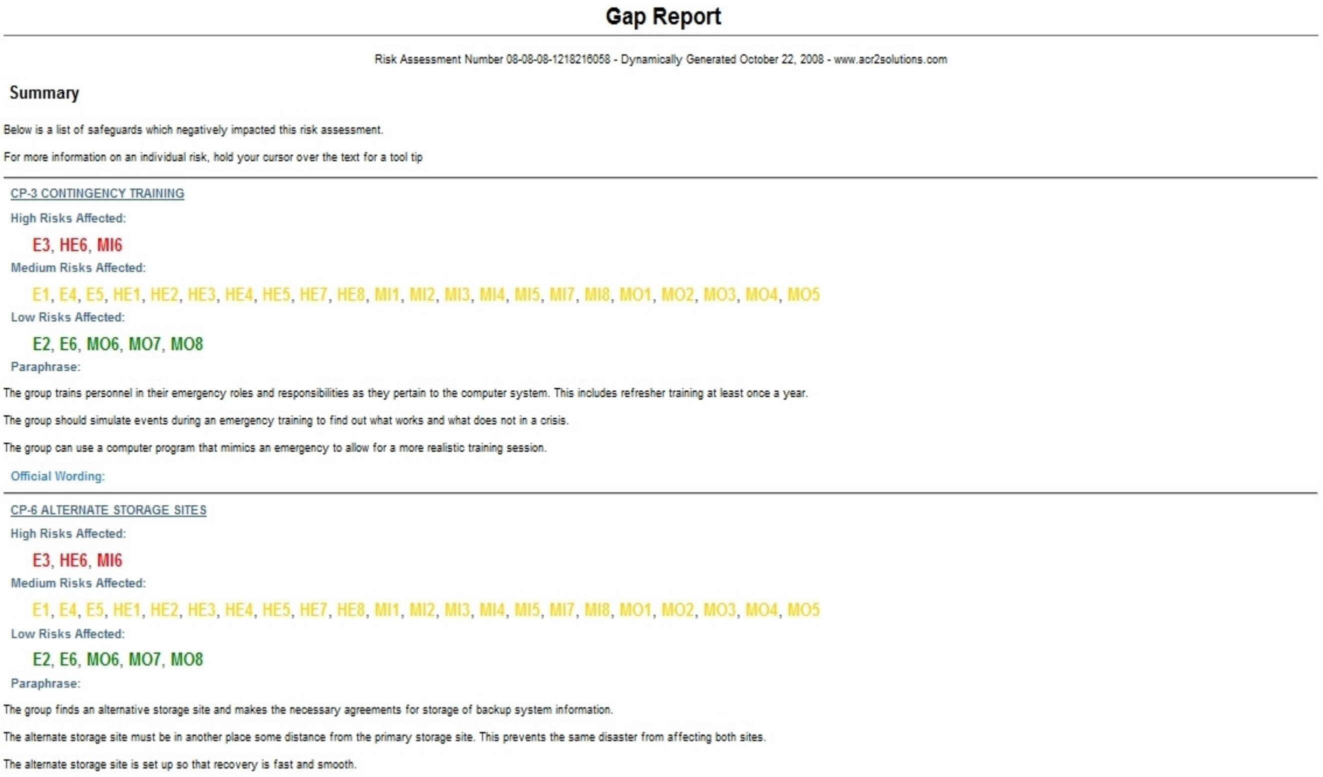
Symbol	Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
E1	Wind	Roof damage	M	H	H
E2	Fire	Smoke damage	M	H	H
E3	Flood	Facility damage	M	H	H
E4	Power loss	Loss of operations	M	H	H
E5	Power loss	Damage to building	M	H	H
E6	Vehicle collision	Facility damage	M	H	H
HE1	Human error	Data acquisition	M	H	H
HE2	Human error	Data storage	M	H	H
HE3	Human error	Data retrieval	M	H	H
HE4	Human error	Data modification	M	H	H
HE5	Human error	Data transmission	M	H	H
HE6	Human error	System design	M	L	L
HE7	Human error	Procedure implementation	M	H	H
HE8	Human error	Internal controls	M	H	H
MI1	Malicious insider	Data acquisition	M	M	M
MI2	Malicious insider	Data storage	M	M	M
MI3	Malicious insider	Data retrieval	M	M	M
MI4	Malicious insider	Data modification	M	M	M
MI5	Malicious insider	Data transmission	M	M	M
MI6	Malicious insider	System design	M	L	L
MI7	Malicious insider	Procedure implementation	M	H	H
MI8	Malicious insider	Internal controls	M	H	H
MO1	Malicious outsider	Data acquisition	M	L	L
MO2	Malicious outsider	Data storage	M	L	L
MO3	Malicious outsider	Data retrieval	M	L	L
MO4	Malicious outsider	Data modification	M	L	L
MO5	Malicious outsider	Data transmission	M	L	L
MO6	Malicious outsider	System design	M	L	L
MO7	Malicious outsider	Procedure implementation	M	L	L
MO8	Malicious outsider	Internal controls	M	L	L

This information can also be shown graphically, as in the following example from a different risk assessment. The risk assessment graph provides an 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.



Gap Report

Risk Assessment Number 08-08-08-1218216058 - Dynamically Generated October 22, 2008 - www.acr2solutions.com

Summary

Below is a list of safeguards which negatively impacted this risk assessment.

For more information on an individual risk, hold your cursor over the text for a tool tip

CP-3 CONTINGENCY TRAINING

High Risks Affected:

E3, HE6, MI6

Medium Risks Affected:

E1, E4, E5, HE1, HE2, HE3, HE4, HE5, HE7, HE8, MI1, MI2, MI3, MI4, MI5, MI7, MI8, MO1, MO2, MO3, MO4, MO5

Low Risks Affected:

E2, E6, MO6, MO7, MO8

Paraphrase:

The group trains personnel in their emergency roles and responsibilities as they pertain to the computer system. This includes refresher training at least once a year.

The group should simulate events during an emergency training to find out what works and what does not in a crisis.

The group can use a computer program that mimics an emergency to allow for a more realistic training session.

Official Wording:

CP-6 ALTERNATE STORAGE SITES

High Risks Affected:

E3, HE6, MI6

Medium Risks Affected:

E1, E4, E5, HE1, HE2, HE3, HE4, HE5, HE7, HE8, MI1, MI2, MI3, MI4, MI5, MI7, MI8, MO1, MO2, MO3, MO4, MO5

Low Risks Affected:

E2, E6, MO6, MO7, MO8

Paraphrase:

The group finds an alternative storage site and makes the necessary agreements for storage of backup system information.

The alternate storage site must be in another place some distance from the primary storage site. This prevents the same disaster from affecting both sites.

The alternate storage site is set up so that recovery is fast and smooth.

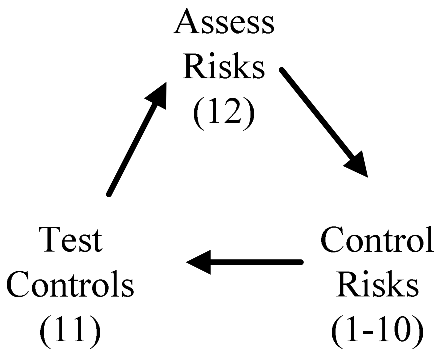
Following vendor negotiations and safeguards installation, it is usually good to have a period of weeks of "normal operations" before testing the upgraded system.

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.


Assess Risks (12)
Control Risks (1-10)
Test Controls (11)