

Astaro OrangePaper

How to comply with the Payment Card Industry Standard

Author: Angelo Comazzetto

*Astaro Product
Evangelist*



Date: 2008-05-02

Content

Page

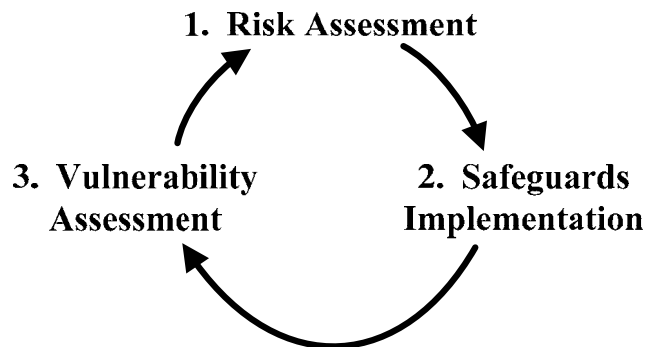
Overview	2
The PCI Standard.....	3
PCI History	3
Risk Assessment: The Starting Point	4
Strategies for Implementing Safeguards.....	4
The PCI Guidelines and the Astaro UTM Solution.....	5
Compliance Ease-of-Use	12

Overview

The Payment Card Industry Data Security Standard (PCI DSS) requires minimum standards of security from any organization that handles payment cards or credit cards. The details of the security requirements vary with the size of the organization, but in each case, three steps are required.

1. Risk Assessment
2. Safeguards Implementation based on the Risk Assessment
3. Vulnerability Assessment to measure the effectiveness of the Safeguards Implementation

This “Circle of Compliance” approach is shown below



The automated Astaro Compliance Reporter provides a “formal risk assessment” as required by the DSS. Following the risk assessment, Astaro products and partners can then assist users to implement the safeguards recommended by the Astaro Compliance Report.

The PCI Security Standards Council manages global training and certification programs for qualified security assessors (QSAs) and approved scanning vendors (ASVs). Vulnerability Assessment measures the effectiveness of the Safeguards Implementation. The results of the Vulnerability Assessment, usually required quarterly, are used to update and revise the Risk Assessment and turn the Circle of Compliance.

The PCI Standard

The Payment Card Industry Data Security Standard applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit/debit card data. This new set of guidelines and operational requirements went into effect June 30th, 2007. Failure to comply with the Payment Card Industry security standards may result in heavy fines, restrictions or permanent expulsion from card acceptance programs.

Certification has been troublesome for card handlers. In July 2007, Visa stated that 40 percent of Level 1 retailers were compliant with the DSS. In May 2006, the compliance rate for that group was 18 percent. Despite making considerable progress in the last year, the industry continues to have significant compliance problems.

PCI History

The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to protect customer information, safeguard transactions, and provide risk assessment by identifying vulnerabilities or exploits that could be used to compromise systems and interfere with the integrity of the process.

On December 15th 2004, Visa, MasterCard, American Express, and Discover combined resources to create a single PCI Data Security Standard (DSS), which would allow them to meet the needs of their existing individual programs under a standardized process. PCI effectively combines requirements of the following programs:

Visa - CISP (Cardholder Information Security Program)

MasterCard - SDP (Site Data Protection)

American Express - DSS (Data Security)

Discover - DISC - (Data Security Guidelines)

Astaro services and partners can be used by participating financial institutions and merchant locations to assist them in meeting the requirements set forth by the PCI standard.

Risk Assessment: The Starting Point

Risk assessment as a technical discipline was greatly advanced in the 1970s and 1980s during the expansion of the environmental industry. Huge problems such as PCB contamination and dioxin removal were addressed by developing a systematic procedure to determine a very basic yet difficult question: how much protection is enough?

In the United States, the question of “how much is enough?” was addressed for information security by the National Institute of Standards and Technology (NIST) by order of the US Congress. The Clinger-Cohen Act of 1996 directed the Secretary of Commerce to set minimum standards for the security of “sensitive but non-classified” information. These standards are binding on US agencies and recommended for regulated industries. The NIST protocols also meet the PCI DSS requirement for a “formal risk assessment” and are compatible with the ISO 27001 framework.

Starting as a single document, the NIST standards quickly expanded to cover all aspects of information security. A single printed copy of the applicable standards as of March 2007 required more than a meter of shelf space. Automation of the NIST risk assessment process was commercialized in 2006 and initially applied to the banking industry. The Astaro Compliance Reporter for PCI rolled out in late 2007.

Strategies for Implementing Safeguards

Following a risk assessment, it is the responsibility of card handlers to deal with their risks by implementing appropriate safeguards. Safeguards identified by the risk assessment process will include hardware, software and administrative components. While implementing administrative safeguards should be straight-forward, the integration of the hardware and software components can be done using two different and incompatible strategies:

1. Specialized “point products” that address individual safeguards, such as independent and separate firewalls, anti-virus software, denial of service devices, etc.
2. Integrated multi-purpose “Unified Thread Management” (UTM) products that address a range of safeguards in a single system.

A review of life-cycle costs for information security systems will rapidly show that the major cost of such programs is in the configuration, updating, maintenance and management of the various safeguards. Every new or upgraded device is a potential point source failure and requires configuration, administration and integration with all other portions of the system. This reality points to the minimum cost strategy for effective information security.

Keep the system as simple as possible

Use as few key components as possible

Make the key components as robust and effective as possible

This minimum cost/maximum effectiveness strategy is readily fulfilled using the Astaro line of UTM products. A recent Gartner report points to UTM devices largely replacing single point protection systems throughout the industry over the next decade. The Astaro family of UTM's is acknowledged to be the industry leader in performance.

Using the Astaro system, all areas of the product can be administered with a single WebAdmin interface. This avoids the need for training staff to deal with tedious command line syntaxes or convoluted GUI's. For sensitive high-uptime installations, it is possible to combine up to ten Astaro Security Gateway appliances in a load-sharing, failover-capable cluster to deliver all the benefits of a Unified Threat Management approach and eliminate the "single point of failure" argument against such a deployment.

The simpler the system, the more likely it is to be effectively managed. Complexity has many hidden costs and risks. The Astaro UTM family can do a great deal to manage and control these risks.

The PCI Guidelines and the Astaro UTM Solution

The PCI Standard is a list of 12 requirements located in 6 control-groups, all of which must be addressed by any merchant or institution that wishes to do business using payment cards from the major credit card companies. The following pages will educate on the PCI Standard and how Astaro's award-winning Unified Threat Management Security Gateways can be used to assist this process with a minimal amount of time, effort, and training.

Build and Maintain a Secure Network

1) Install and maintain a firewall configuration to protect cardholder data.

A firewall's primary purpose is to separate the trusted internal side (or LAN) of a network from an un-trusted public side, such as the Internet. Astaro utilizes a powerful firewall component that allows for extremely granular controls as to what can pass through the device in both incoming and outgoing directions. In addition, Astaro Security Gateway products ship from the factory in a state that denies all traffic flows, meaning that an administrator must specifically "punch holes" for the traffic he wishes to allow through the device. This approach ensures that there are no hidden allowances on the device that might cause unapproved traffic flows and compromise the security of the network without the administrator's knowledge. By shipping as a default-deny policy, administrators can easily verify the controls they have put in place and are not left wondering what else they must research and do to "lock down" the installation.

2) Do not use vendor-supplied defaults for system passwords and other security parameters

Astaro knows that many hackers and those that wish to exploit systems often start with a known list of commonly used or default access passwords for a certain systems, in the hopes of finding a location where the administrators have either forgotten (or simply not bothered) to change the default security passwords and access methods put in place during installation or at the factory.

All [Astaro Security Gateway](#) models require that the administrator enter new password information for the WebAdmin upon first login, and, by default, the SSH (command line) access to the Astaro environment is disabled. Should the administrator of the Astaro Security Gateway need command line access, he must first enable that function from within WebAdmin and then set the necessary passwords himself. This means there is no default set of logins that could be exploited to gain access to the system, and only passwords and procedures specifically implemented by an administrator can be used.

Protect Cardholder Data

3) Protect stored cardholder data.

The best protection for your data is to deny intruders the ability to access it at all. By deploying an Astaro solution at your gateway, you can limit access to the internal network from the outside world, and also restrict the sessions that are allowed in to those using approved mediums, such as SSH or SSL. Rather than set global access permissions allowing any address or location to flow through the device, Astaro allows accesses by individual IP's or hostnames, providing a finer degree of access and allowing you to know specifically where visitors will be accessing data from.

4) Encrypt transmission of cardholder data across open, public networks.

The Internet is not a secure medium. Traffic that travels from one location to another is susceptible to interception at any point in between, which could be as few as one, or as many as hundreds. Any of these points could be malicious in nature and decide to sniff or examine the traffic as it passes through and, in so doing, compromise your data. The solution is to provide secure tunnels between these points that data can travel through encrypted, and Astaro provides a myriad of options and configuration schemes designed to allow these tunnels (VPNs) to be placed between Astaro and most other capable devices. By securing the traffic by means of DES or AES encryption at strengths up to 256 bits, transactions can be securely sent across a normal Internet connection without the need to purchase expensive, managed proprietary links (WANs) and dedicated VPN appliances. Not only can Astaro devices make these tunnels using hundreds of possible configuration variables to ensure communication to thousands of devices and endpoints, but the administrator requires only a small amount of knowledge and can build tunnels of enterprise-level strength and complexity with less than a dozen clicks on the Astaro Security Gateway menus.

Tunnel security provides secure point-point data transfer, but Astaro can also simplify the process of implementing and using company-wide e-mail encryption. By offloading the tedious task of educating employees on SMIME or OpenPGP encryption procedures, the Astaro Gateway can do the necessary encryption and decryption between compatible sources with no client programs necessary. This industry-leading technology allows a full company adoption of secure encrypted e-mail with no special learning curve for the employees. The administrators even have the option to pre-load Astaro with necessary

certificates or key rings for the companies and individuals that require secure e-mail transactions, or just allow Astaro to watch active e-mail activity and adopt key information as it flows through the box. This allows all future communications to and from that outside user to be encrypted automatically, with no extra administrative steps. By offering unparalleled simplicity with industry standard encryption methods, supporting secure e-mail is now possible for all companies, regardless of budget and user-experience.

Maintain a Vulnerability Management Program

5) Use and regularly update anti-virus software.

Modern networks can be a mix of desktops, laptops, servers and appliances, running various operating systems and platforms. Administrators face a large task in trying to standardize on an anti-virus solution that will accommodate their entire network, update itself regularly, and provide company-wide reports on virus activity, effectiveness, and current threats. However, by deploying up to three gateway Anti-virus systems on an Astaro solution, companies can use the gateway to remove virus threats at a single chokepoint. Combined with a desktop defense plan, gateway scanning from Astaro can make protecting against virus threats a much less tedious task, as you scan all incoming and outgoing traffic at the gateway. This approach allows viruses to be caught and discarded before they even enter the network and get the chance to cause damage, and the Astaro system updates automatically every 15 minutes with new patterns downloaded as needed and with no user input required or loss of operations during the update. In addition, should a virus be brought into the network by an outside source, it will not be allowed to pass through the Astaro outgoing and infect your customers and business associates as a result.

6) Develop and maintain secure systems and applications.

By providing several application proxies, Astaro can do much more than simply pass your traffic. Astaro systems can examine traffic and apply detailed filtering options to further secure the network and the transmissions. Our HTTP filtering allows companies to fully monitor what sites their users are visiting, for how long, and using how much bandwidth. In addition to the logging, Astaro can deploy URL and Spyware filtering, Phishing attack prevention, and anti-virus scanning for downloaded files and objects. The approaches here can range from allowing everything and simply monitoring the activity, to fully

restricting web-surfing to only a handful of approved sites. The configuration choices are there, and the implementation takes just minutes.

Astaro Mail filtering allows malicious and unwanted “dirty” mail to be deflected or stored on the gateway for review and/or retrieval by administrators or users, depending on the desired functionality and company policy. This allows for clean mail to travel easily to the server and inboxes, while unwanted mail can be dealt with using a variety of checks and options. With only a few clicks, you can fully filter both incoming and outgoing e-mail for Spam and Viruses, and even customize the system to ensure that mail from high priority sources is allowed immediate access. Further adding to Astaro’s capabilities is our exciting new Encryption functionality, which allows companies to deploy full PGP or SMIME abilities to their entire company’s e-mail without the need for any desktop software or user training, making this a first on a Unified Threat Management product.

Implement Strong Access Control Measures

7) Restrict access to cardholder data by business need-to-know.

Astaro environments make possible extensive levels of granularity in many configuration areas. A common approach in a firewall is to make permissions allowing an internal network to access the Internet on a certain port/service. With Astaro, it is possible to set permissions and access controls down to single users or IP addresses, even within an already denied group. This allows you to avoid having to create extensive and complex additional security policies that single users are placed under, since you can simply target a user for additional permissions in tandem with his or her already-allowed actions under a broader group. Further, Astaro makes it possible to filter by source IP or hostname, so you can even make a port available from the outside to only a certain source and then re-use that same port for a different source, to a different destination internally. This provides thousands of configuration possibilities designed to make certain that the proper people are accessing resources with no unneeded overlap of security permissions.

8) Assign a unique ID to each person with computer access.

In protecting your network, Astaro fully supports seamless integration to your Windows Active Directory and Novell E-Directory environments, with other options available as well (such as RADIUS, SAM etc.). By tying in your Astaro to your user directory structure, Astaro can track usages and monitor activity

with full username support, so that time consuming lists which reference what user was using an IP become unnecessary. With each user being tracked and logged under their username, regardless of the workstation they are using, the reporting and forensic abilities of the company and administrators increase dramatically. This provides the powerful ability to quickly deploy multiple security profiles with various access permissions to the entire company based on user group, and ensure the proper employees have the access they require. By having Astaro integrate with your user directory, you make anyone using the company network fully accountable.

9) Restrict physical access to cardholder data.

All Astaro appliances are rack-mountable, allowing them to be placed in the secure storage or network rooms at your company. In addition, the Astaro requires passwords be entered for any physical access, further keeping your network secured. By properly securing your crucial network components physically, potential malicious individuals cannot compromise the infrastructure of the site via console hacking or physically damaging or disabling equipment.

Regularly Monitor and Test Networks

10) Track and monitor access to network resources and cardholder data.

A strong feature of Astaro Security Gateway is logging system. Astaro logs every packet that passes through the device, and places it into a dedicated log file depending on the process that handled it and the nature of the traffic. With over 40 separate log file sections, the information you need is always available for forensic analysis, reporting, or general viewing. In addition, the logging system automatically archives and compresses the data each day, archives it, and opens new logs, putting the data you need just a few clicks away. For added redundancy, Astaro offers multiple configuration options where log files can be streamed to a syslog server or bundled and sent nightly to an FTP server, secure network file share, or copied over SSH.

Adding to the built-in reporting capabilities of the Astaro Security Gateway, is the [Astaro Report Manager](#). This dedicated application runs on a separate server, where log-crunching CPU power can be given more freely to reporting operations without sacrificing the performance of the gateway device. This allows creation of hundreds of reports in thousands of different detail layouts, all fully searchable and customizable. Administrators can even maintain

detailed mailing lists that send various reports to different company resources at configurable times, and they can monitor a live dashboard that is continually updated to show threats, monitoring triggers and user-configured action items.

11) Regularly test security systems and processes.

Astaro is also equipped with a detailed and fully configurable, built-in self-monitoring system. This system monitors all the processes and daemons that run on device and will trigger alerts and notifications for over 200 events that might require administrator action. By keeping administrators informed as to what is happening on their Astaros and their networks, regular policing of the unit is not necessary. The WebAdmin interface also provides any logged-in administrator with a full systems overview, showing current bandwidth usage, hardware status of CPU, RAM, and other factors. Also provided are numerous top-10 lists providing information on the amount of e-mail and web pages surfed, top network users for the day, VPN activity and more. These in-line reports are generated new each day, which allow administrators to quickly identify spikes or anomalies in network activity so they can adapt and deal with issues as needed.

Maintain an Information Security Policy

12) Maintain a policy that addresses information security.

Other solutions require complex certifications and lengthy training programs to deploy in a secure manner. Astaro's WebAdmin GUI has been specifically designed to provide unsurpassed ease-of-use, so the focus can be on securing the network, not learning a new system for months on end. Overly complex solutions also open the door for misconfiguration and subsequent security holes. Astaro's 7th generation WebAdmin allows users to create and configure enterprise level security policies and access controls with just a few clicks, which are then passed to Astaro's own configuration daemon that does all the necessary steps in the security system. As a result, it has never been easier to deploy intricate and effective security configuration in a shorter amount of time. The added benefit is that a company can bring new administrators online with minimal training, and the entire company policy can be reviewed, evaluated, adjusted and re-deployed on the fly at any time. We put the information you need at the front so that configuration is never a mystery and digging through countless sub screens or command line files is not needed.

Compliance Ease-of-Use

As the deadline for the PCI Standard looms, it is more important than ever for institutions to ensure compliance before penalties are assessed against them. By deploying a single, Unified Threat Management solution from Astaro, your PCI compliance can be all but addressed with minimal training and deployment planning, while enjoying an enterprise class of security tools in a single solution all designed to make your network security experience more effective than ever before.

Contact



Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

www.astaro.com

The Americas

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2008 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.