COMPLYING WITH:

Payment Card Industry (PCI)

Data Security Standards

Using SEA Solutions

iSecurity

absCompress

absMessage

Legal Notice: This document reflects the understanding of Software Engineering of America, Inc. of System i security and auditing compliance related to the Payment Card Industry Data Security Standards set by the Payment Card Industry Security Standards Council. SEA is not in a position to guarantee and assumes no responsibility that the implementation of the recommendations in this whitepaper ensures a complete and full compliance with all aspects of the Payment Card Industry standards. The information is provided as an informational piece. SEA advises users to undertake their own research and advice to satisfy their required level of compliance with the standards.

Introduction

The Payment Card Industry (PCI) Security Standards Council was formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International to provide a single data security standard (DSS) for companies who process, store or transmit credit, debit, prepaid, ATM and POS card information. The PCI Standards Council created the Data Security Standard in 2004 to protect cardmembers from fraud, and to increase controls over sensitive data.

According to the PCI Standards Council, the PCI DSS "is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures".

Requirements

The official site for the PCI Data Security Standard is http://www.pcisecuritystandards.org.
The current version of the standard is v2.0 which was released in October 2010. The DSS centers on these 12 requirements:

PCI DSS Core Requirements

Build and Maintain a Secure Network	
Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	
Requirement 5	Use and regularly update anti-virus software
Requirement 6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
Requirement 7	Restrict access to cardholder data by business need to know
Requirement 8	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes
Maintain an Information Security Policy	
Requirement 12	Maintain a policy that addresses information security

Source: PCI Security Standards Council

Compliance

It is the credit card companies who enforce compliance. The credit card companies will hold you responsible for stolen credit card data. A merchant failing to comply with any part of the regulation may be fined and penalized by the individual credit card companies, by up to $500,000 per incident. Penalties also include a temporary or even permanent restriction from service provider lists, which means that your business may not accept credit cards for a specified period of time.

In 46 of 50 states in America, a business is legally responsible for reporting security breaches to the public. This means that, for any company whose security is breached, the reporting of the breach will alert credit card companies on any compromise to credit card data security.

What's involved in meeting credit card company security requirements?
The size of your business determines the level of security requirements you must meet. To ensure compliance, the PCI Security Standards Council requires annual security assessments, which must be completed by a qualified security assessor (QSA). Smaller businesses who do not meet certain volume transactions must annually complete a self-assessment questionnaire.

Compliance is not a one-time event, but a continual process, and the PCI Council treats it as such. In the Requirements, the Council specifies ongoing actions and periodic maintenance which must be taken to be in compliance. In addition, the PCI Council releases new data security enhancements and changes in response to issues in the marketplace. It is up to the merchant to be apprised of these updates to the requirements and respond accordingly.

Many merchants use technology to automate the process of maintaining compliance with the PCI DSS. They look to firms like SEA to provide solutions that will provide ongoing, automated compliance.

IBM i

This whitepaper focuses on PCI Compliance on the IBM i Series. IBM's iSeries does a great job of storing and protecting credit card information. But the native IBM i is missing a layer of security and is vulnerable in networked environments and, without additional security software, can be hacked.

Software Engineering of America strongly recommends that IBM i owners at the very least should seriously consider our Firewall product to make their IBM i more secure. As you will see in the following information, iSecurity Audit, Compliance Evaluator, Authority on Demand and AP Journal provide a complete solution to addressing PCI Compliance.

PCI Requirements

Build and Maintain a Secure Network

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

"Firewalls are computer devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted 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 untrusted networks, whether entering the system via the Internet as e-commerce, employee internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network."

"Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1."

An effective and properly configured firewall will ensure that unauthorized users are blocked from intruding into a system. In summary, the standards require specific firewall configurations that only allow certain users access based on need. See Sections 1.1-1.5.

Relevant Summary

- [1.1] You must identify all connections, including wireless access to cardholder data
- [1.1.3] Requires that you control access by IP addresses
- [1.2] You should deny traffic from non-trusted hosts/networks, except for necessary protocols
- [1.2] Direct access between the Internet and cardholder data environment is prohibited
- [1.4] A firewall should be installed on any computer that accesses the organization's network

SEA Solution: iSecurity Firewall and Audit

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

"Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information."

Internal and external attacks often result from utilizing default vendor passwords.
Changing these passwords and security settings will make your system less vulnerable. See Sections 2.1-2.4.

Relevant Summary

- [2.1] Easy-to-guess and default passwords and settings supplied by a vendor must never be used
- [2.2.2] You must disable all insecure services
- [2.3] Web-based management tools for non-console administrator access should be encrypted

SEA Solution: iSecurity Firewall, Audit, Antivirus, Authority On Demand

PCI Requirements (continued)

Protect Cardholder Data

3. Protect Stored Cardholder Data

Protection methods such as encryption, truncation, masking and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as email and instant messaging.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.

Encrypt cardholder data to ensure classified information remains secure.
See sections 3.1- 3.6.

Relevant Summary

- [3.1] Keep a minimal amount of cardholder information
- [3.3] Most PAN digits must be masked
- [3.4] PAN should be encrypted when stored
- [3.5] Protect encryption keys

SEA Solution: Authority On Demand, absCompress

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

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Since public networks are vulnerable and common targets for hackers, it is important to encrypt transmitted data.
See sections 4.1 – 4.2.

Relevant Summary

- [4.1] Encrypt transmitted data over public networks (Internet, wireless, GSM, GPRS, etc)
  Use strong security protocols i.e., SSL, IPSEC for data transmission.

SEA Solution: absCompress, iSecurity Audit and Firewall

PCI Requirements (continued)

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs.

Malicious software, commonly referred to as —malware—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Utilizing anti-virus software is important on a system because viruses are easily entered into a system discreetly and unknowingly. Additionally, it is important to constantly check for updates since viruses are developed constantly.
See sections 5.1 – 5.2.

Relevant Summary

- [5.1] Use and deploy Anti-Virus software on all System i's that can host or be affected by malware
- [5.2] Ensure that the Anti-Virus is current, running and can generate audit logs

SEA Solution: Antivirus

6. Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

All software and applications should be updated with security patches provided by the vendor to ensure that vulnerabilities are reduced. See sections 6.1-6.6.

Relevant Summary

- [6.2] Establish a process to identify newly-discovered security vulnerabilities, such as subscribing to alert services, automatic updates

SEA Solution: iSecurity Firewall, Audit, Antivirus and Compliance Evaluator.

PCI Requirements (continued)

Implement Strong Access Control Measures

7. Implement Strong Access Control Measures

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Makes sure that only authorized users are accessing confidential information. See Sections 7.1 – 7.2.

Relevant Summary

- [7.1] Restrict access to information to only those personnel whose job requires it
- [7. 2] Default access should be set to "deny all" unless specifically allowed

SEA Solution: iSecurity Firewall, Audit, Journal, Capture, Authority On Demand and Compliance Evaluator

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

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

By assigning a unique ID to each user, an administrator will be able to track who specifically accessed certain files, made notifications, deletions etc. See Sections 8.1 – 8.5

Relevant Summary

- [8.1] Every user must have a unique ID, allowing the business to trace each action to a specific user
- [8.2] Ensure proper user authentication and password management for administrator and nonconsumer users
- [8.3] Implement a two-factor authentication for remote access
- [8. 4] All passwords should be encrypted both in storage and during transmission
- [8.5.1] Calls for ensuring proper user authentication and password management

SEA Solution: iSecurity Firewall, Audit, Capture, Authority On Demand, Compliance Evaluator

PCI Requirements (continued)

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, —onsite personnel refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A visitor refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. Media refers to all paper and electronic media containing cardholder data.

Only allow authorized users to obtain physical access to cardholder information.
See sections 9.1 – 9.10.

Relevant Summary

- [9.1] Limit and monitor physical access to systems in the cardholder data environment

Implement Strong Access Control Measures

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Tracking and logging user activity is important to ensure that an administrator is able to analyze when users' access unauthorized data or if something goes wrong. Logs will allow administrators to backtrack to find the proper source.
See sections 10.1– 10.7.

Relevant Summary

- [10.1] Allow thorough analysis to determine the cause of a security compromise
- [10.2] Implement automatic audit trails for all system components, for the following events (at the very least): Access to cardholder data or audit trails, actions taken by users with admin privileges, failed login attempts, etc
- [10.5] Requires the recording of certain audit trail entries: user ID, event type, date/time, success/failure indication, origination of event, affected data/resource
- [10.3] Secure audit trails so they cannot be altered
- [10.7] Retain audit trails for at least a year or in accordance with legal/industry requirements

SEA Solution: iSecurity Firewall, Antivirus, Audit, Journal, Capture, Authority On Demand and absMessage

PCI Requirements (continued)

11. Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Check frequently for software updates to ensure that the latest security threats are blocked by your system.
See sections 11.1 – 11.5.

Relevant Summary

- [11.2] Limit and monitor physical access to systems in the cardholder data environment
- [11.4] Use network detection/prevention systems to monitor traffic in the cardholder data environment
- [11.5] Deploy file integrity monitoring software to alert on unauthorized modification of critical files

SEA Solution: Firewall, Audit, Antivirus, Journal, Capture, View, Compliance Evaluator, absMessage

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, personnel refers to full-time and part-time employees, temporary employees, contractors and consultants who are —resident on the entity's site or otherwise have access to the cardholder data environment.

Educating personnel is crucial to establishing firm security procedures and handling suspicious situations.
See sections 12.1-12.10

Relevant Summary

- [12.5.2] Calls for monitoring and analyzing security alerts

SEA Solution: Firewall, Audit, Journal, Capture, View, Compliance Evaluator, Authority on Demand, absMessage

SEA's IBM i Solutions Suites – PCI Compliance

PCI Requirements	iSecurity Suite							abs Suite	
	Firewall	Audit	AntiVirus	Journal	Capture	Authority on Demand	Compliance Evaluator	absCompress	absMessage
Build and Maintain a Secure Network									
1. Install and Maintain a Firewall Configuration to Protect Cardholder Data	✓	✓							
2. Do Not Use Vendor Supplied Defaults for System Passwords and Other Security Parameters	✓	✓	✓			✓			
Protect Cardholder Data									
3. Protect Stored Cardholder Data						✓		✓	
4. Encrypt transmission of cardholder data across open, public network	✓	✓						✓	
Maintain a Vulnerability Management Program									
5. Use and regularly update anti-virus software or programs			✓						
6. Develop and maintain secure systems and applications	✓	✓	✓				✓		
Implement Strong Access Control Measures									
7. Restrict access to cardholder data by business need-to-know	✓	✓		✓	✓	✓	✓		
8. Assign a unique ID to each person with computer access	✓	✓			✓	✓	✓		
9. Restrict physical access to cardholder data									

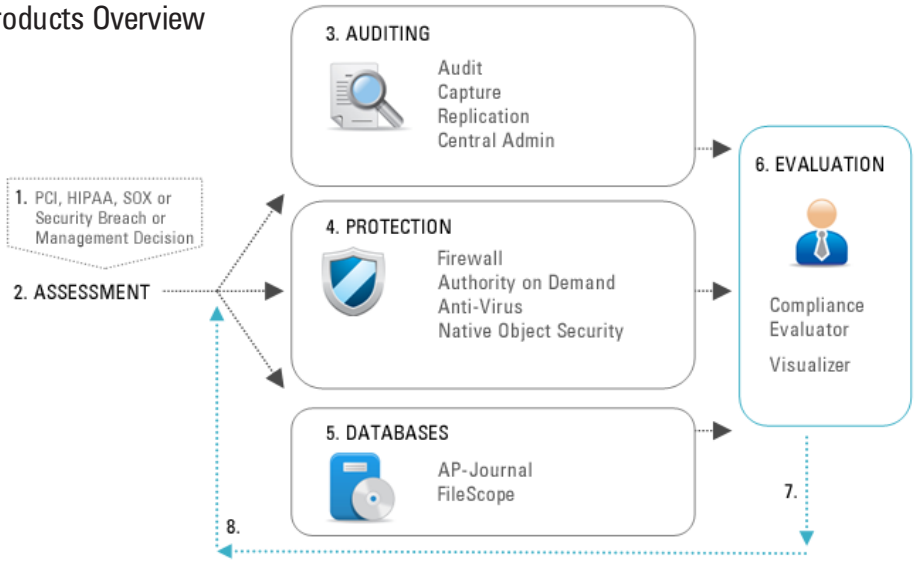
PCI Requirements	iSecurity Suite							abs Suite	
	Firewall	Audit	AntiVirus	Journal	Capture	Authority on Demand	Compliance Evaluator	absCompress	absMessage
Regularly Monitor and Test Networks									
10. Track and monitor all access to network resources and cardholder data	✓	✓	✓	✓	✓	✓			✓
11. Regularly test security systems and processes	✓	✓	✓	✓	✓	✓	✓		✓
Maintain an Information Security Policy									
12. Maintain a policy that addresses information security for employees and contractors	✓	✓	✓	✓	✓	✓	✓		✓

SEA Solutions

iSecurity Suite

The iSecurity product suite offered by SEA consists of modular solutions to meet today's security requirements. These solutions can be customized to meet your specific needs without interfering with day-to-day business operations. Implementing this user-friendly security solution will keep your data safe and comply with today's strict industry standards, such as PCI.

iSecurity Products Overview



iSecurity is one of the leading solution providers for the IBM i environment. This solution provides security at all levels of the System i prior to protecting the credit card data itself. In other words, access to the data via users, programs, terminals etc. is protected as well. This is important because it ensures all aspects of the System i environment are safe from potential threats. The flexibility and comprehensiveness of this data security solution is integrated into a single security and compliance package to prevent data loss and unauthorized accesses. The following are the iSecurity modules with information on how they securely protect your IBM i.

Firewall

Firewall protects and secures all types of access to and from the IBM i, keeping your company safe from intruders. Not only is Firewall an easy-to-use filter for incoming and outgoing TCP/IP activity and intrusion prevention, it will also manage user profile status, password restrictions, sign-on time control, object access control, rules exceptions, and logging of all activity. Scripts can be created in real-time to automatically respond to monitored activity with system commands and programs to alert you via an email, AS/400 message, and/or by phone. Users can utilize the Java-based GUI in addition to the traditional green-screen interface to effectively monitor and analyze activity for any type of IBM i environment.

Audit

Audit provides real-time monitoring and logging of system and user activities. Audit also takes action against these threats by triggering proactive alerts. Monitored activity can be viewed, printed or obtained via an automatic report scheduler that can be sent to an administrator, senior manager and auditors. Scripts can be created in real-time to automatically respond to monitored activity with system commands or programs, alert you via email AS/400 message and/or by phone.

Antivirus

Antivirus will scan compressed files and protect against viruses found on your System i server. This application runs natively on your System i and scans your IFS and mail for viruses and will eliminate the requirement to download these files to your PC or server for scanning. This prevents unnecessary network traffic from tying up your LAN. In addition, Antivirus removes infected files from the system, scans emails through the Mail Alert Scan feature and utilizes a user-friendly GUI interface. On-access, On-Demand scanning and automatic updates are other key features of Antivirus that will keep your system safe.

AP - Journal

The AP - Journal solution will allow you to monitor data modifications, providing you with before and after images of your data. Enterprises can see who made changes, what modifications were made, and when these changes took place. For example, data retrieval is simple and allows security administrators to have control over information flowing within their organization.

Capture

Capture secretly obtains and documents users' screens for ultimate security without affecting system performance. The solution works silently and invisibly in the background while users will not notice it is running. This solution allows administrators to see what users are doing and what they are doing with specific information. Capture can automatically trigger screen capturing according to a variety of pre-defined rules. Administrators can retrieve archived screenshots for definitive and accurate forensics whilst keeping your system in compliance.

Authority On Demand

iSecurity Authority on Demand provides an advanced solution for emergency access to critical application data and processes, which is one of the most common security slips in System i (AS/400) audits. Furthermore, current manual approaches to such situations are not only error-prone, but do not comply with regulations and auditors' often stringent security requirements. Authority on Demand enforces segregation of duties and enables relevant personnel to obtain access to approved information when needed. Its real-time audit of access rights protects sensitive corporate assets and significantly reduces the number of profiles with powerful special authorities.

Compliance Evaluator

iSecurity Compliance Evaluator enables managers to quickly check the compliance of their systems with industry and corporate policies based on customizable, user-friendly reports. It provides concise one-page reports featuring an overall compliance score, as well as specific ratings for any security-related component of System i, such as system values, network attributes and user profiles. The information provided includes status checking for items such as System Values, Network Attributes, User Profile Attributes and Object Authorities.

abs Suite

The abs Suite offered by SEA consists of absCompress and absMessage. These System isolutions provide data compression and encryption as well as message and resource management. Integrating these solutions into your System i environment will ensure that you are aware of system activity in real-time as well as provide protection for your critical files and data.

absCompress

absCompress compresses objects over 80% at high speeds to save space and reduce file transfer time. absCompress provides government-approved AES encryption up to 256 bit. Users can enter a string as a password for strong security measures. In addition, the history console can track the details of all compression or decompression it performs.

absMessage

absMessage allows administrators to sort messages through a centralized platform and take action immediately. Users have the flexibility of viewing these messages through a Java GUI, web console, PDA, or green screen. In addition, users can make appropriate and automated response notifications to these alerts. Users can reply to these messages and create filters for a highly organized message management system. Monitor system resources or be notified of important alerts whilst setting automatic responses to these escalations.