PCI DSS Compliance with IBM Power i

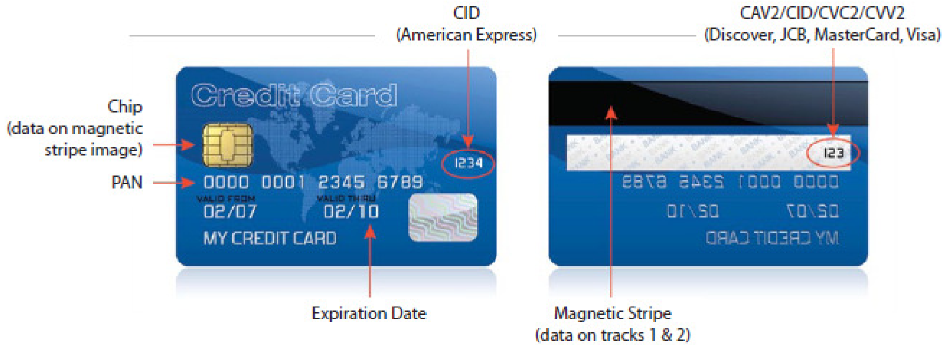
iSecurity

White Paper

Introduction

During recent years, merchants have been a target for financial fraud: For example, over 234 million records holding sensitive financial information were breached between 2005-2008 from payment card transactions and processing systems [PCI DSS Quick Guide, Page 4]. As most businesses store credit card information (numbers, expiration dates, verification codes and personal data) online, this information is in many cases easily accessible and could be used for malicious purposes. Weak points are everywhere – point-of-sale devices, web-applications, data transmissions, personal computers and more. Merchants who constitute a center of payment card transactions must use security procedures to prevent theft of data.

Types of Data on a Payment Card



(Source: PCI Quick Reference Guide, Page 11)

Need to have, Need to know: PCI DSS (Payment Card Industry Data Security Standard) is a common security standard (https://www.pcisecuritystandards.org) applicable to credit card transactions (including VISA, American Express, and MasterCard), intended to help organizations prevent credit card fraud. Any organization that stores, processes or transmits cardholder data is required to comply with the PCI DSS standard. A merchant (in all instances) failing to comply with any part of the regulation might be severely fined by the PCI Security Standard Council, by up to $500,000 per incident. At the end of the day, the company is responsible for how it manages its data, and, regardless of the size of the organization, its compliance must be assessed on a regular basis.

Credit Card information and Power i: IBM Power i (System iAS/400) presents a unique set of challenges when it comes to PCI compliance. Power i hosts credit card processing applications such as home grown ERP and Web applications that accept and process credit cards. Although Power i systems are perceived as secure, this is not wholly accurate - system exit points are wide open and comprehensive application data trails are not provided by the operating system, allowing exposure of data and creating a new security need.

Complying with PCI

PCI-DSS consists of 12 requirements within six categories [source: PCI Quick Guide, Page 8] which cover best security practices. Below is a summary of these requirements, focusing on the relevant items to Power i security. Each requirement is followed by a guideline specifying how to actually implement the requirement.

Note: Numerous items which appear in formal PCI documentation are not discussed in this document, as they are irrelevant for choosing security software. For example, item number 9.3: ‘Ensure visitors are authorized before entering areas where cardholder data is maintained’ is not mentioned. Therefore, we recommend a careful review of formal PCI documentation before defining and implementing site-security procedures.

Build and Maintain a Secure Network

Requirement 1: Configure a Firewall

Relevant Summary

- [1.1] All connections to cardholder data (including wireless) must be identified
- [1.2] Traffic from non-trusted hosts/networks should be denied, except for necessary protocols
- [1.2] Direct access between the Internet and cardholder data environment must be prohibited
- [1.4] Firewall should be installed on any computer that accesses the organization’s network

Guidelines: The objective is preventing criminals from virtually accessing payment system networks and stealing cardholder data. Remote access to Power i can be accomplished via FTP, remote commands, SQL and ODBC protocols. The company's firewall solution must ensure that unauthorized users are blocked from penetrating corporate systems, by covering all 53 Power i communication protocols (FTP, ODBC, Telnet, SQL, etc). Each network access point should be logged and any breach attempt should be immediately reported.

Requirement 2: Default Passwords and Parameters

Relevant Summary

- [2.1] Easy-to-guess and default (vendor-supplied) passwords and settings must never be used
- [2.3] Non-console administrator access such as web-based management tools should be encrypted

Guidelines: Internal and external attacks often result from utilizing default or easy-to-guess administrator passwords. Specifically on Power i, default profiles beginning with the letter “Q” (i.e. QSECOFR, QSYS) need to be carefully monitored. Companies should employ tools that provide full password management capabilities, including enforcement of site-defined password policies. In addition, the selected security solution should produce detailed daily reports of unsecured passwords.

Protect Cardholder Data

Requirement 3: Protect Stored Data

Relevant Summary

- [3.3] Most PAN digits must be masked
- [3.4] PAN should be encrypted when stored
- [3.5] Protect encryption keys

Guidelines: The objective is very simple – protecting stored payment card data to prevent its unauthorized use. Data encryption is a very effective way to prevent intruders from using stolen information even when they succeed in obtaining it. Naturally, encryption keys must be strong and should be managed securely. In addition, the ideal security system should allow display control of classified data on the user's screen, by restricting access of unauthorized users to specific database records and fields.

Requirement 4: Encrypt Transmission

Relevant Summary

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

Guidelines: Sensitive cardholder data should be encrypted before transferring it between Power i & other platforms. More advanced solutions, such as tokenization, provide additional safeguards. Such solutions actually reduce the scope of the PCI footprint which needs to be protected to a central data vault only, lower the cost and shorten the process of attaining PCI compliance.

Maintain a Vulnerability Management Program

Requirement 5: Anti-Virus

Relevant Summary

- [5.1] Use and deploy Anti-Virus software on all systems that can be affected by malware
- [5.2] Ensure that the Anti-Virus mechanism is current, running and can generate audit logs

Guidelines: Power i hardware and software architecture enforce the validation of every stored object (program or data) through a Licensed Internal Codes authority component. Therefore, no currently-known virus can attack Power i. However, the Power i can serve as a host for PC-based viruses, stored on IFS and then redistributed to other PC machines, infecting files and/or mapped network drives. Companies should employ an Anti-Virus solution that provides full protection against Windows-compatible viruses and programs used or stored on System i server. The selected anti-virus tool should also support definition of automatic, pre-scheduled periodic scans.

Requirement 6: Secure Systems and Applications

Relevant Summary

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

Guidelines: Security mechanisms should be defined to audit and capture user activities in real-time and automatically respond to any security event – by sending messages/alerts to various destinations, initiating external programs, etc. Changes in business-critical data should also be monitored, and configured to alert relevant personnel when user-defined thresholds are crossed.

Implement Strong Access Control Measures

Requirement 7: Restrict Access

Relevant Summary

- [7.1] Access must be granted on a need-to-know basis and in accordance with job responsibilities
- [7.2] Default access should be set to “deny all” unless specifically allowed

Guidelines: User authorizations should be defined in strict accordance with their specific responsibilities. Personnel having access to production/system libraries should be restricted and continuously monitored. The security system should dynamically allow for receiving additional authorizations, according to pre-defined dates/times, IP addresses, etc. When higher rights are provided, the system should then log the activity and send an audit report and real-time alerts.

Requirement 8: Assign Unique ID

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 non-consumer users
- [8.3] Implement a two-factor authentication for remote access
- [8.4] All passwords should be encrypted both in storage and during transmission

Guidelines: The objective is to ensure that any action on sensitive cardholder data can be performed only by authorized users. To achieve this, full password management capabilities must be employed, including enforcement of site-defined password policies (i.e. password expiration time). In addition, all user activities must be monitored by the system (see Requirement 10 – Monitor Access).

Requirement 9: Restrict Physical Access

Relevant Summary

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

Guidelines: Companies should consider automatically protecting unattended workstations to assure full network security server control.

Regularly Monitor and Test Networks

Requirement 10: Monitor Access

<u>Relevant Summary</u>

- [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
- [10.3] Keep all user activity information: user ID, event type, date/time, success/failure indication, origination of event, affected data/resource
- [10.5] 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

Guidelines: To effectively manage and protect sensitive data, it is critical to track and log user activities. If something goes wrong, this log would allow the necessary analysis to determine the cause and the people responsible for it. Employ a system that monitors any Operating System activity, keeps all relevant information and generates full detailed reports in various formats. Responses should be initiated in real-time to potential threats and security violations.

Requirement 11: Test Security

<u>Relevant Summary</u>

- [11.2] Run internal/external network vulnerability scans periodically and after network changes
- [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

Guidelines: The objective is to frequently test system components, processes and software in order to ensure that security is maintained in the long term, and specifically during new software deployment or system configuration changes. The system should provide comprehensive analysis of your security system – the result would be used to analyze strengths and weaknesses, check all system security aspects and evaluate the compliance of the system with industry and corporate policies.

Maintain an Information Security Policy

Requirement 12: Maintain a Policy

<u>Relevant Summary</u>

- [12] Inform all employees of their expected duties related to security and awareness of cardholder data sensitivity.

Guideline: Companies should provide all employees with security education in order to establish firm security procedures.

Summary

Choosing the right security solution for corporate Power i environments is a challenging and important task, intended to minimize the risk of security breaches and keep customer information secure. When assessing the current security status, one must first gather all necessary security information: policies, change controls, network diagrams, cardholder data flow, location of repositories, etc. It is highly recommended to assign a project manager and key people from IT, security, Human Relations and legal departments to ensure that all aspects are considered in security-related choices.

There are a number of software products on the market that help evaluate a company's compliance level. The selected system should be non-disruptive to production systems and business critical application data, and should present PCI and other compliance rankings in summarized form per individual systems, as well as an overall score the entire enterprise.

Finally, the evaluating software should be flexible enough to allow each site to locally define- and schedule- its compliance and reporting requirements.

iSecurity – A Complete System i Security Solution

Raz-Lee's iSecurity™ is a comprehensive user-friendly security solution for the System i environment. iSecurity addresses insider threat, external security risks, and the need to protect business-critical application data, as well as providing for effortless compliance with mandatory security regulation.

Taken together, these capabilities make iSecurity the solution of choice for System i Managers, Auditors, System Administrators and Application Managers.

With over 25 years of experience gained in thousands of System i installations, iSecurity offers an end-to-end security solution for companies' System i infrastructure and business-critical databases. iSecurity ensures successful security audits and effortless compliance with regulations such as SOX, HIPAA and PCI. Moreover, it dramatically reduces the resources needed to monitor activity even as it increases the power of its security capabilities.

iSecurity Features

- End-to-end solution for achieving compliance and preventing security breaches
- Modular design comprising numerous stand-alone solutions that integrate into custom packages
- Advanced network access and auditing solutions
- Highly flexible and easily scalable, including network access simulation mode
- Built-in reports, report generator, and scheduler for total reporting support
- Best-Fit algorithm proven especially efficient in large environments
- Choice of GUI and green-screen interfaces
- Advanced user profile management reporting including allocating specific authorities as needed
- Multi-system reporting capabilities including e-mailing reports in PDF, HTML, and CSV formats
- Single-screen management and administration of multiple servers and partitions
- Single-view compliance scorecard report for all servers and partitions
- Real-time network access, QAUDJRN and application data alerts sent to e-mail, SMS, SYSLOG and more

iSecurity Products

Prevention Pack

- **Firewall** - secures every type of network access to and from the System i.
- **Visualizer for Firewall** - provides at-a-glance graphic views of log data collected by Firewall.
- **Password** - integrates all OS/400 password management capabilities, blocking non-secure passwords.
- **Screen** - protects unattended terminal screens.
- **Assessment** - analyzes security definitions and values, and suggests corrections and solutions.

Compliance Pack

- **Audit** - reports on user activities and object access in real-time, including multi-system environments.
- **Visualizer for Audit** - provides at-a-glance graphic views of log data from the system audit journal.
- **Action** - invokes corrective and reporting procedures for detected security breaches in other iSecurity modules, and sends emails, SMS and SYSLOG messages.
- **System Control** - controls and monitors system resources, jobs, and message queues.
- **Assessment** - analyzes security definitions and values, and suggests corrections and solutions.

Stand-Alone Modules

- **Compliance Evaluator** – quickly performs single-view network-wide compliance checks for any or all partitions and systems
- **Authority on Demand** - monitors access rights for critical data and processes.
- **AP-Journal BizAlerts & Business Analysis** – initiates real-time alerts upon critical changes in application data and produces cross-application timeline reports
- **AP-Journal Regulation Compliance** – reports on field-level "before" and "after" values in application databases.
- **Native Object Security** - enables system administrators to easily define target security levels per object and object type, and to check for inconsistencies.
- **User Profile & System Value Replication** – enables effective reproduction of user profiles, passwords and parameters, and revival of deleted users.
- **Capture** - real-time green screen tracking solution for compliance audit trails.
- **View** - provides air-tight field- and record-level security, hiding sensitive information as required.
- **Anti-Virus** - scans files and e-mail attachments for viruses, Trojan horses, and malicious code.
- **Central Administration** - manages multiple systems from a single control point

.

iSecurity

iSecurity Product Series - Compliance with PCI Requirements

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	√	√	√	√	√			√	√					√		
2.1	Always change vendor-supplied defaults before installing a system on the network. This includes wireless devices that are connected to cardholder data environment or are used to transmit cardholder data.	√	√	√	√	√			√	√					√		
2.3	Encrypt all non-console administrative access such as browser/Web-based management tools.										√						
3.3	Mask PAN when displayed; the first six and last four digits are the maximum number of digits you may display. Not applicable for authorized people with a legitimate business need to see the full PAN. Does not supersede stricter requirements for displays of cardholder data such as on a point-of-sale receipt.										√						

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
3.4	Render PAN, at minimum, unreadable anywhere it is stored – including on portable digital media, backup media, logs, and data received from or stored by wireless networks.										√						
3.5	Protect cryptographic keys used for encryption of cardholder data from disclosure and misuse.	√	√	√	√	√			√	√	√				√		
5.1	Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).						√										
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.						√										
6.3	Develop software applications in accordance with PCI DSS based on industry best practices and incorporate information security throughout the software development life cycle.							√	√	√							
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	√	√	√	√	√			√	√					√	√	√
7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need-to-know, and is set to "deny all" unless specifically allowed.	√	√	√	√	√			√	√					√	√	√

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
8.1	Assign all users a unique user name before allowing them to access system components or cardholder data.		√	√	√	√			√	√							
8.2	Employ at least one of these to authenticate all users: password or passphrase; or two-factor authentication (e.g., token devices, smart cards, biometrics, and public keys).		√	√	√	√			√	√				√			
8.3	Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service or terminal access controller access control system with tokens; or virtual private network with individual certificates.		√	√	√	√			√	√							
8.4	Render all passwords unreadable for all system components both in storage and during transmission using strong cryptography based on approved standards.		√	√	√	√			√	√							
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.		√	√	√	√			√	√				√			

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment											√					
10.1	Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.		√	√	√	√				√			√			√	
10.2	Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects.		√	√	√	√				√			√			√	
10.3	Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.		√	√	√	√				√			√			√	

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
10.5	Secure audit trails so they cannot be altered.		√	√	√	√				√			√			√	
10.6	Review logs for all system components related to security functions at least daily.	√	√	√	√	√			√	√			√			√	
10.7	Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.	√	√	√	√	√			√	√			√			√	
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. ASVs are not required to perform internal scans.	√		√	√	√			√								
11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification, including network- and application-layer penetration tests.	√		√	√	√			√								
11.4	Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. IDS/IPS engines must be kept up to date.	√		√	√	√			√								

PCI Article	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Administration	Anti-Virus	AP-Journal	Action	Capture	View	Screen	Authority on Demand	Password	Assessment	Native Object Security	Replication
11.5	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.		√	√	√	√				√							
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.	√	√	√	√	√		√	√	√			√				
Notes	All products run in **both GUI and green screen** except: Visualizer (GUI), AP-Journal (GS), AOD (GS), Assessment (PC)																
	Reports produced by all products can be automated via the report scheduler and output can be printed and e-mailed as PDF, HTML or CSV attachments.																

For More Information

For a free valuation of the iSecurity product please contact us on 6103 9885 4877 or email info@ahtech.com.au
You can also visit us at www.ahtech.com.au

AH Technology

AH Technology Pty Ltd
PO Box 205 Malvern Victoria 3144

Tel: +613 9885 4877 Fax: +613 8678-0665
Email: info@ahtech.com.au www.ahtechnology.com.au