

Detailed Analysis – Achieving PCI Compliance with SkyView Partners' Products

The Payment Card Industry has a published set of Data Security Standards to which organization's accepting and storing credit card information must comply. Since these Data Security Standards are written in generic terms, one must do some interpretation to determine how the requirements apply to IBM i or i5/OS.

Using the requirements directly from the Payment Card Industry's Data Security Standards document, requirements are translated into IBM i and i5/OS terms and a description of how the SkyView products assist is provided.

SkyView product descriptions:

Risk Assessor for IBM i and i5/OS is an IBM i and i5/OS security diagnostic tool that compares your security configuration against security best practices. Risk Assessor examines more than IBM i and i5/OS 100 "risk points" including system values, user profile settings, object level authorities, TCP/IP configuration, and more. Risk Assessor provides easy-to-read reports that allow you to easily determine where your systems' security configuration deviates from security best practices. In addition, Risk Assessor provides a comprehensive analysis guide which includes an explanation of the best practices settings and recommendations for IBM i and calls attention to specific PCI DSS considerations/requirements.

Policy Minder for IBM i and i5/OS is an IBM i and i5/OS security compliance tool that compares your systems' current settings against your organization's security policy requirements. Your policy implementation is documented and non-compliant items are identified. Using the FixIt function, non-compliant items can be set back to match policy settings. Policy Minder automates the process of keeping your IBM i and i5/OS security configuration in compliance with your security policy.

PCI Requirements – Section 2.2 and 2.2.2:

- Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (2.2)
- Configure system security parameters to prevent misuse. (2.2.2)

Solution: Use Risk Assessor to determine how your systems' security configuration compares to security best-practices as well as specific PCI requirements.

PCI Requirement – Section 2.2.3:

- Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).

Solution: Use **Policy Minder** to compare the current auto-start and time-out values of the TCP/IP servers against policy requirements. If this value is changed, the next compliance check will identify the server as non-compliant. In addition, **Risk Assessor** provides a report of all open ports and all port restrictions in place at the time Risk Assessor was run.

PCI Requirements – Section 2.1 and 6.3.6:

- Always change vendor-supplied defaults before installing a system on the network (2.1)
- Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers. (6.3.6)

Solution: Use **Policy Minder** to check user profile configuration settings to ensure no vendor profiles have a password and are set to status of disabled. Policy Minder can also be used to ensure no IBM-supplied profiles have default passwords and system value settings are not changed away from your policy requirements during the installation of a vendor package.

PCI Requirements – Section 7.1, 7.1.1 and 7.1.2:

- Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: (7.1)
 - Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities (7.1.1)
 - Assignment of privileges is based on individual personnel's job classification and function (7.1.2)

Solution: **Policy Minder** provides an automated method for the discovery of new profiles with elevated (*ALLOBJ) privileges or profiles that have been made a member of the QSECOFR group. In addition, the user profile category in Policy Minder allows you to define the attributes of each role. Compliance checks identify the profile and its attributes that are out of compliance with the role definition. Policy Minder's FixIt function allows administrators to change the user profile attributes to be in compliance with the role definition and provides a documented record of the change.

PCI Requirements – Section 7.2, 7.2.1, 7.2.2 and 7.2.3:

- Establish an access control system for systems components with multiple users that restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: (7.2)
 - Coverage of all system components (7.2.1)
 - Assignment of privileges to individuals based on job classification and function (7.2.2)
 - Default "deny-all" setting (7.2.3)

Solution: Use the library and directory categories in **Policy Minder** to maintain compliance for the privileges each role is to be given to individual files or applications. Compliance checks will identify the each item out of compliance along with the configuration issues causing the non-compliance status. Policy Minder's FixIt function can be used by administrators to change the settings to match the roles' requirements and provides a documented record of the change. Finally, use the system value, library and directory categories in Policy Minder to ensure the system settings remain configured as "deny-all."

PCI Requirement – Section 8.5.1:

- Control addition, deletion and modification of user IDs, credentials and other identifier objects.

Solution: Use the user profile category of **Policy Minder** to maintain the configuration of all user profiles on the system. Compliance checks identify changes to user profiles and attributes which do not match role configuration requirements. In addition, FixIt can be used to change the profile back to its original settings or to fix the non-compliant attributes.

PCI Requirement – Section 8.5.4:

- Immediately revoke access for any terminated users.

Solution: **Policy Minder's** FixIt function can be used to delete user profiles from the system. FixIt produces a report which can be used as proof to your auditor that terminated users' profiles are being removed from the system on a timely basis. If large numbers of profiles need to be removed, this can be easily accommodated through the user profile upload function which uploads a list of profiles into Policy Minder from a spreadsheet.

PCI Requirement – Section 8.5.5:

- Remove/disable inactive user accounts at least every 90 days.

Solution: **Policy Minder** can simplify the discovery and automate the removal of inactive profiles. You can use Policy Minder to find and take action on inactive profiles. Actions include the ability to set the status to *DISABLED, remove the profile's password and more. You can also delete the profiles using Policy Minder, providing proof that your process is being followed. To simplify the processing of these profiles, you can omit profiles that are an exception – that is, should never have action take on them. This way, the list of profiles only contains those on which action should be taken. When printing this policy, profiles omitted are documented.)

PCI Requirement – Section 8.5.6:

- Enable accounts used by vendors for remote maintenance only during the time period needed.

Solution: The user profile category of **Policy Minder** can be configured to examine the status of all vendor profiles. The FixIt function can be scheduled to run nightly to set any vendor profile back to *DISABLED status if the profile's status is discovered to be *ENABLED.

PCI Requirement – Section 8.5.8:

- Do not use group, shared, or generic accounts and passwords.

Solution: A **Risk Assessor** report identifies all groups along with which group profiles have passwords. Once this issue has been remediated, the user profile category of Policy Minder can be configured to ensure these group profiles are not assigned a password.

PCI Requirements – Section 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, and 8.5.15:

- Change user passwords at least every 90 days (8.5.9)
- Require a minimum password length of at least seven characters (8.5.10)
- Use passwords containing both numeric and alphabetic characters (8.5.11)
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. (8.5.12)
- Limit repeated access attempts by locking out the user ID after not more than six attempts. (8.5.13)
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. (8.5.15)

Solution: The system value category of **Policy Minder** can check the password and session time-out system values to ensure they meet these requirements. In addition, the user profile category of Policy Minder can be configured to examine user profile settings to ensure these values (in particular, the password expiration interval) has not been overridden in the user profiles with a less restrictive settings.

PCI Requirements – Section 12.1, 12.1.1, 12.1.2, 12.1.3:

- Establish, publish, maintain, and disseminate a security policy that accomplishes the following: (12.1)
 - Addresses all PCI DSS requirements. (12.1.1)
 - Includes an annual process that identifies threats and vulnerabilities and results in a formal risk assessment. (12.1.2)
 - Includes a review at least once a year and updates when the environment changes (12.1.3)

Solutions: Use **Policy Minder** to document the IBM i or i5/OS implementation of your security policy requirements. Risk acceptance statements can be added to the policy definitions as well as cross-references to specific sections of your organization's security policy. All of these can be printed in PDF format and given to your auditor as documentation of your policy implementation. In addition, you can run **Risk Assessor** to fulfill the requirements for your annual (or more often if needed) IBM i and i5/OS risk assessment.

PCI Requirement – Section 12.2:

- Develop daily operational security procedures that are consistent with requirements in this specification (12.2)

Solution: Both **Policy Minder** and **Risk Assessor** can be run as often as is required to meet your compliance requirements.

These are just some of the ways SkyView Partners' products can reduce the cost and complexities of maintaining your compliance requirements. For more information, please visit the SkyView Partners website at www.skyviewpartners.com.

Who is SkyView Partners? SkyView Partners Inc. is a firm specializing in policy-based security compliance management and assessment software as well as security services for IBM i (AS/400 and iSeries) customers.