

How SkyView Products Assist with PCI Compliance

The Payment Card Industry has a published set of Data Security Standards which any organization that accepts credit card information must adhere to. Since these Data Security Standards apply to all systems, one must do some interpretation to determine how the requirements apply to the System i (AS/400 or iSeries.) While some specifications are clearly spelled out, such as the password requirements, others are defined by their intent. The Data Security Standard's intent is that the integrity of the data can be assured, that access to the data is restricted and that the system's security scheme is configured to support this intent. This is where the interpretation comes in. SkyView Risk Assessor compares your system's security configuration against security best practices for over 100 risk points – these include various i5/OS configuration items such as system values, user profile settings, TCP/IP configuration, guest user profiles and more. Risk Assessor provides an explanation of the issue to allow you to determine whether the issue requires remediation. If remediation is required, Risk Assessor provides suggestions on how to start the remediation process.

Beyond Risk Assessor's helping you ensure the system's configuration supports the intent of the Data Security Standard on i5/OS, here are some ways SkyView products address specific Data Security Standards requirements:

- Detection of default passwords. Risk Assessor lists any i5/OS user profiles that have a default password and along with the capabilities currently assigned to these profiles. SkyView Policy Minder can check user profile configuration to ensure no profiles have default passwords.
- Data Security Standards requires "strong access controls." In i5/OS terms this means that database files containing cardholder data be set to public authority *EXCLUDE. Policy Minder can help you change this setting as well as perform regular compliance checks to ensure the files remain secured appropriately. If users are specifically allowed access, this can also be included in the check.
- Policy Minder templates can be used to regularly monitor user profile configuration
 - to check the configuration of user profiles, ensuring profiles are created with the correct special authorities, group assignments, initial programs, auditing settings, etc.
 - to flag new profiles have been created, changed or restored that now have *ALLOBJ (security officer) authority. to identify profiles that are no longer active and should be removed from the system
 - to ensure all users' passwords are changed every 90 days
- Using the Policy Minder system value category you can check to ensure that
 - the system's password composition rules (minimum length 7, requirement to contain a digit, be changed every 90 days, only be reused after 4 other passwords have been used, and locking the user out after 6 invalid password attempts) are being enforced.
 - i5/OS auditing remains active and is configured properly
- Risk Assessor specifically addresses the requirement for i5/OS for "an annual process that identifies threats and vulnerabilities, resulting in a risk assessment."
- Policy Minder documents the i5/OS implementation of the organization's security policy.
- To provide proof to auditors that you are regularly monitoring your security configuration, Policy Minder generates compliance check reports. If the item being checked is in compliance, meaning that it meets the requirements of your policy), a one-page summary report is generated stating that the item(s) are in compliance with the policy requirements. If the item is out of compliance, the report contains a detailed description of the discrepancy.

Carol Woodbury is President and co-founder of [SkyView Partners, Inc.](http://www.skyviewpartners.com) She is the designer and architect of the SkyView products and has over 17 years in the security industry, 10 of those working the AS/400 Security Architect and Chief Engineering Manager of Security Technology. Carol's second book, *Experts' Guide to OS/400 and i5/OS Security*, is available at www.amazon.com.