



## SkyView Risk Assessor for OS/400 & i5/OS

"To determine whether or not you are "safe and secure" you need to start with a comprehensive assessment. I designed SkyView Risk Assessor to fill that need with reports that cover over 100 security risk points on your System I (iSeries) systems."

**Carol Woodbury,**  
System i Security Expert, noted  
author, award winning presenter and  
President of SkyView Partners Inc.

A comprehensive diagnosis is often overlooked when it comes to the security configuration of OS/400. Most system administrators only have the time to manage passwords and monitor a few, selected system values. But when it comes to security, the task extends beyond passwords and system values.

Risk Assessor automates the process to gather security information from these 100+ "risk points" across OS/400.

With **Risk Assessor** (a product designed and coded to Carol Woodbury's specifications) you get a tool that leverages Carol's expertise to produce a comprehensive report that includes:

- \* Details about the security issues discovered;
- \* Explanations of the business risks presented, and
- \* Steps to start addressing the issues found.

The column to the right is the **Table of Contents** for the Main Security Assessment Document generated with Risk Assessor. From this you can see the comprehensive nature of this product.

Findings will be unique for **each** system analyzed.

NOTE: the items in **Blue** indicate unique data gathering and processing performed by Risk Assessor. The analysis consists of one or more queries and/or combining sets of data and/or writing to APIs.

### 100+ "Risk Points" covered by Risk Assessor

#### Users on the System (19 risk points covered)

##### Users with Default Passwords

##### Inactive Users

Powerful Users

##### Powerful Groups

##### Groups that Own Objects

##### Groups whose Passwords are not \*NONE

Altered IBM Profiles

##### IBM Profiles with a Password

##### IBM Profiles that are Group Profiles

##### Profiles that are "Not" \*EXCLUDE

##### \*USE Authority to IBM-Supplied Profiles

##### Password Expiration Interval

##### Limited Capability Users

##### Commands for Limited Users

##### Controlling Users' Green Screen Environment

##### User Profiles with Programs that Adopt Authority Controlling

##### Users' PC Desktop

DST Users and Passwords

Validation Lists Users

#### Object Level Authority (9 risk points covered)

##### \*PUBLIC Authority of Libraries

Users Authorized to Create Libraries

Create Authority

##### \*PUBLIC Authority of Directories

Users Authorized to Create Directories

Getting Started with Object Authorities

Authorization Lists

##### File Shares

##### Application Administration

#### System Values (40 risk points covered)

##### 22 Security System Values \*

##### 11 Password System Values \*

##### 6 Auditing System Values \*

##### 1 Library System Value (public authority settings) \*

#### Exit Points (9 risk areas covered)

##### Network Access Points

Trigger Programs

Open Database File Exit

##### Commands

##### Command Exits

##### Validity Checker & Prompt Override Programs

##### User Profile Exits

##### Viruses in the IFS

Network Attributes

#### Final Considerations (17 areas covered)

##### Auto-Start Values

##### Time-Out Values

Users with Authority to STRTCPSVR Command

##### Users with Authority to the \*QATM Config Files

##### Users with Authority to WebSphere Configurations

##### Open Ports & Port Restrictions

##### Server Authentication Entries

##### NetServer Guest Profile

Adopted Authority

##### Output Queues

##### Job Descriptions

##### Subsystem Descriptions

##### User Objects in QSYS

##### Management Central

Unused Products or Libraries

Check Object Integrity (CHKOBJITG)

QSYSMSG Message Queue

#### Other Considerations (8 areas covered)