syncsort

PRODUCT SHEET

Assure Security Risk Assessment

Given the increasing frequency of cyber attacks, it is essential to regularly conduct security risk assessments as part of a comprehensive IT security program. In fact, many compliance regulations, such as PCI DSS and HIPAA, require annual IT risk assessments. Unfortunately, not all security auditors understand the special security features of IBM i, and not all IBM i administrators have the knowledge or the time to conduct regular, thorough security assessments.

Assure Security Risk Assessment, a core component of Assure Security, is an essential tool for any organization that wants to proactively understand its IBM i security risks without overloading IT managers or hiring external consultants. It checks over a dozen categories of security values, reports on findings and makes recommendations. Sufficient detail is provided to guide technical staff on remediation, while managers receive a higher-level summary of risk level.

Key Features

- Runs as a native job on the IBM i
- Checks dozens of security definitions on your IBM i
- Compares actual values against recommended best practice
- Tags results with three simple severities – OK, Warning, or High Risk
- Explains the meaning and significance of system definitions
- Delivers easy guidance on reducing cyber security risks
- Provides a high-level management summary of security risks resulting from your system definitions
- Produces reports in HTML and PDF formats

Detailed Sections Include:

- Management Summary
- System Values
- Default Passwords
- Disabled Users
- Inactive Users
- Distribution of Powerful Users
- Library Authorities
- Open Ports
- Exit Programs

How It Works

Assure Security Risk Assessment provides a useful and informative picture of your IBM i security. Reports can be given to IT risk and compliance auditors help fulfill requirements for an annual risk assessment required under regulations such as PCI DSS and HIPAA. The tool can be re-run at any time without burdening IT staff.

1.) **Install** the software on the target IBM i system. Then install the GUI on the PC.

2.) **Initiate** execution from the GUI. The security assessment runs as a native job on the target IBM i partition. When the job has completed, the assessment results will be available.

3.) **Review** the results in the GUI and save in HTML or PDF format.

Distribution of Powerful Users

By User Authorities

Authority	Description	Total	Percent
*ALLOBJ	All object authority	51	48.11
*AUDIT	Audit authority	38	35.84
*IOSYSCFG	Input/Output system configuration	43	40.56
*JOBCTL	Job control authority	58	54.71
*SAVSYS	Save system authority	42	39.62
*SECADM	Security administrator authority	40	37.73
*SERVICE	Service authority	40	37.73
*SPLCTL	Spool control authority	49	46.22
*NONE	No authorities	47	44.33

Conclusions Are Divided into Three Severities

✓ Severity - OK	Following recommended best practice
⚠ Severity - Warning	Some risk present
R Severity - High	Have significant security risk

Summary of Severities for each Category

Category	# of checks	OK	Warning	High Risk
System Values	23	7	10	6
User Profiles	20	3	8	9
Object Authorities	13	1	6	6
Access through Network	2	0	2	0
Total	58	11	26	21

Sample Assessment Details

System Values

System Value: QPWDEXPITV - Password Expiration Interval

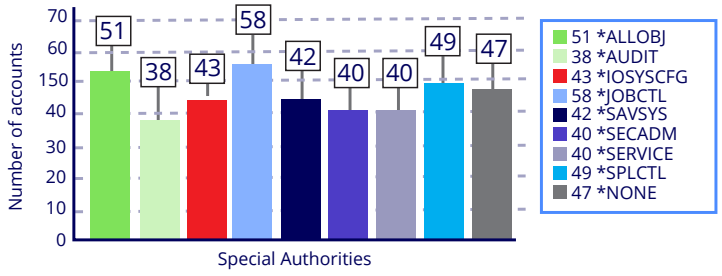
Current Value: ***NOMAX**

Specifies the number of days for which passwords are valid. This provides password security by requiring users to change their passwords after a specified number of days. If the password is not changed within the specified number of days, the user cannot sign-on until the password is changed. Seven days before the password ends, you are warned at sign-on time, even if you are not displaying sign-on information (the system value QDSPSGNINF). The password expiration interval for your system is defined in system value QPWDEXPITV, which is currently set to *NOMAX .

Analysis and Recommendations

A password expiration interval value of *NOMAX allows users to never change their passwords. This gives hackers unlimited time to try and discover passwords. We recommend using the System Value QPWDEXPITV on your User Profiles to control their password expiration interval. This insures that passwords for User Profiles are changed on a regular basis determined centrally by your company policy. Without this, each user could have a different interval which could include longer periods of time beyond the company policy or more troubling a value of *NOMAX. A value *NOMAX means that the password does not expire which allows intruders an indefinite period of time to obtain or guess the password.

Summary of Special Authorities



syncsort