Security Risk Assessment
for IBM i, using Enforcive SRA

The urgency for cyber risk assessment is growing at a rapid pace, with a risk assessment is becoming an essential component of many regulatory compliance demands. That being said, the Enforcive Security Risk Assessment is considered an essential tool to ensure corporate sustainability. The Security Risk Assessment is a fast, reliable and cost effective way to verify the tools and infrastructure used to secure your IBM i.

Enforcive Security Risk Assessment checks your system definitions, explains what they mean and recommends changes if necessary. It is sufficiently detailed to give guidance to the technical staff responsible for system security while providing a management overview for non-technical administrators and managers.

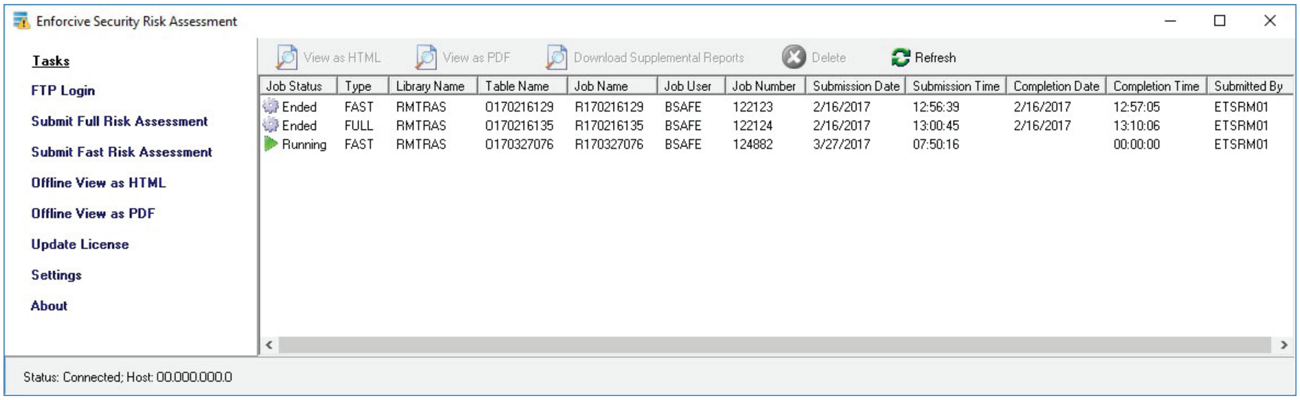
Security auditors often have difficulty understanding the special security features of IBM i. Even administrators of IBM i, when asked to conduct a security assessment, may not know where to start. With the Enforcive Security Risk Assessment, you don’t need to bring in external consultants or tie up your valuable in-house security experts to conduct manual checks. Over a dozen categories of security values are checked automatically and analyzed. The findings are published with recommendations.

Key Features

- Checks dozens of security definitions on your IBM i
- Compares actual values against recommended best practice
- Intuitive icon tagging with three simple severities
  - “OK”
  - “Warning”
  - “High Risk”
- Explanations of meaning and significance of system definitions
- Contains management summary which gives a high-level picture of the security risk resulting from your system definitions
- Easy guidance to reducing cyber security risks
- Report can be distributed by email
- Stand-alone product

Detailed Sections Include:

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


Enforcive Security Risk Assessment
Tasks
FTP Login
Submit Full Risk Assessment
Submit Fast Risk Assessment
Offline View as HTML
Offline View as PDF
Update License
Settings
About
View as HTML
View as PDF
Download Supplemental Reports
Delete
Refresh

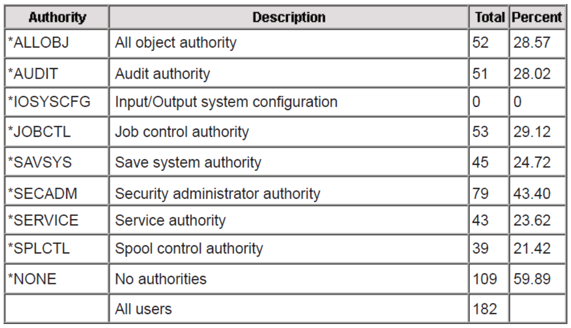
Job Status	Type	Library Name	Table Name	Job Name	Job User	Job Number	Submission Date	Submission Time	Completion Date	Completion Time	Submitted By
Ended	FAST	RMTRAS	0170216129	R170216129	BSAFE	122123	2/16/2017	12:56:39	2/16/2017	12:57:05	ETSRM01
Ended	FULL	RMTRAS	0170216135	R170216135	BSAFE	122124	2/16/2017	13:00:45	2/16/2017	13:10:06	ETSRM01
Running	FAST	RMTRAS	0170327076	R170327076	BSAFE	124882	3/27/2017	07:50:16		00:00:00	ETSRM01

Figure 1: Enforcive Security Risk Assessment

The Enforcive Security Risk Assessment provides a useful and informative picture of your IBM i security to IT risk and compliance auditors and can be rerun at any time without imposing on IT staff. As such, it helps organizations fulfill requirements for an annual risk assessment as required under PCI DSS and HIPAA.

Distribution of Powerful Users

By User Authorities



Authority	Description	Total	Percent
*ALLOBJ	All object authority	52	28.57
*AUDIT	Audit authority	51	28.02
*IOSYSCFG	Input/Output system configuration	0	0
*JOBCTL	Job control authority	53	29.12
*SAVSYS	Save system authority	45	24.72
*SECADM	Security administrator authority	79	43.40
*SERVICE	Service authority	43	23.62
*SPLCTL	Spool control authority	39	21.42
*NONE	No authorities	109	59.89
	All users	182	

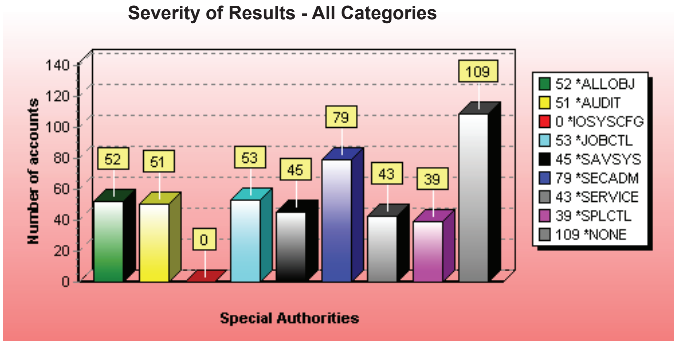
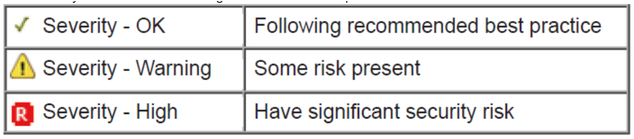


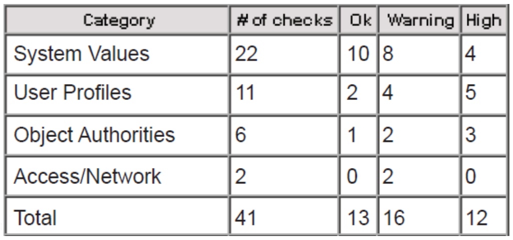
Figure 2: Statistics Accompanying Certain Checks

The conclusions are divided to three different 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
System Values	22	10	8	4
User Profiles	11	2	4	5
Object Authorities	6	1	2	3
Access/Network	2	0	2	0
Total	41	13	16	12

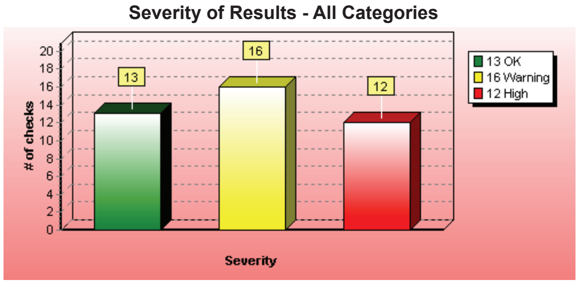


Figure 3: Summary Tables and Graphs

How It Works

1. **Install** the software on the target IBM i system, then install the GUI on the PC.

2. **Initiate** execution from the GUI. The Enforcive security assessment runs as a native job on the target computer. When the job has completed the assessment will be available.

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

Assessment Details

System Values
System Value: QPWDEXPITV - Password Expiration Interval
Current Value: 30

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, even if you are not displaying sign-on information.

Analysis and Recommendations

It is therefore set correctly according to our recommendations of 30-90 days and some industry standards. However, other industry standards differ. We recommend using the System Value QPWDEXPITV on your User Profiles to control their password expiration interval. This ensures 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 of *NOMAX means that the password does not expire, which allows intruders an indefinite period of time to obtain or guess the password.

VISION®
SOLUTIONS

For more information: visionsolutions.com
1-800-683-4667 (Toll-free U.S. and Canada) or 1-949-253-6500