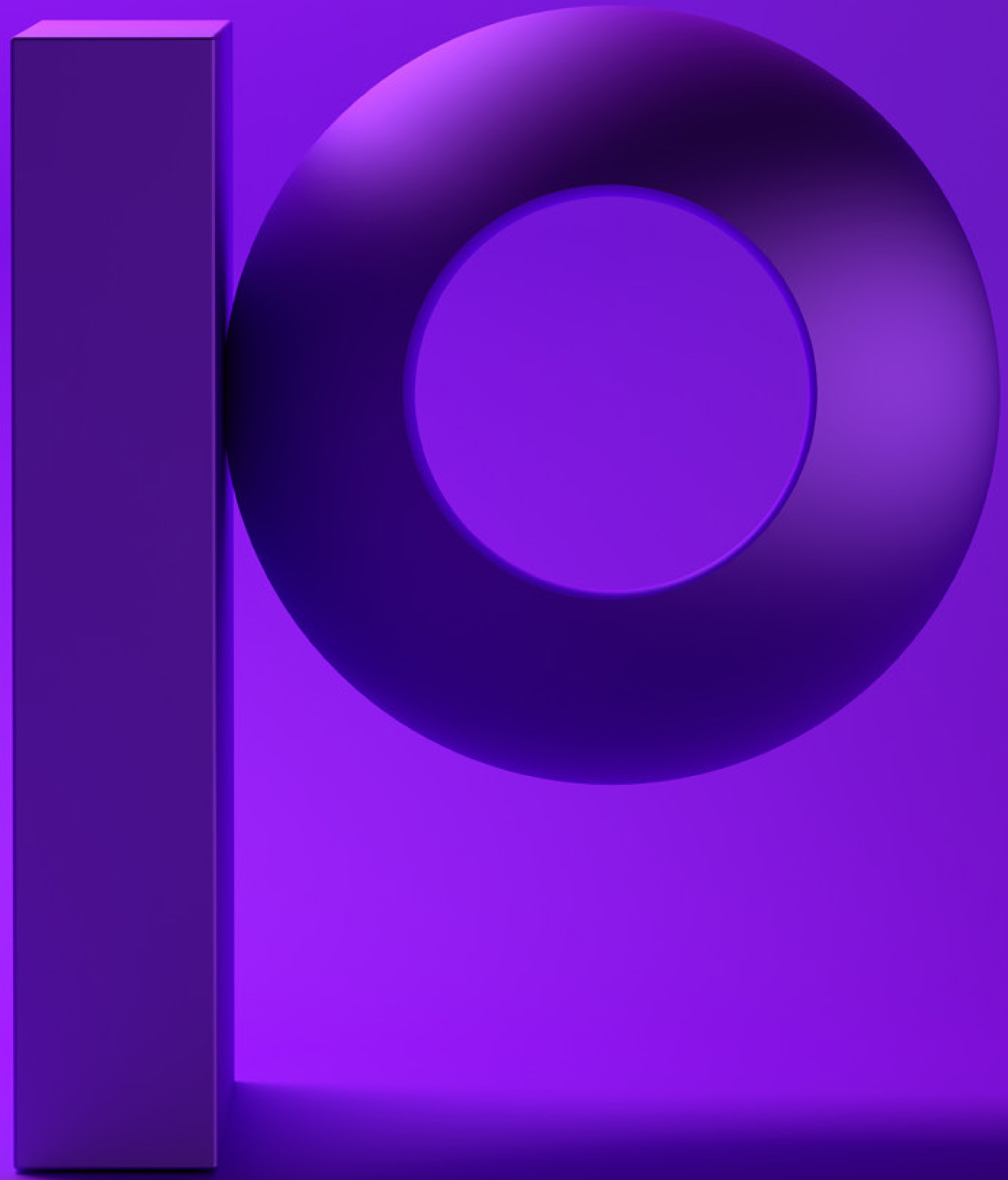
precisely

An Introduction to IBM i Security Risk Assessment



Introduction

A deep level of understanding is required to assess compliance and implement security controls across your enterprise given today's expanding landscape of regulations that require protection of financial data, personally identifiable information and other sensitive corporate data. Continuous assessment of security risks is necessary to understand not only your initial or current security posture, but to ensure that security controls continue to be set in a way that protects the sensitive data stored on your servers.

A common misconception that can leave IBM i systems open to data breaches is that addressing physical and network security is enough to keep systems and data safe. Though controlling physical access and ensuring network security is important, the most common vulnerabilities in IBM i environments come from improper security configurations.

To understand security risks on your IBM i, it is essential to review security settings and configurations throughout the system. However, performing a risk assessment on an IBM i server requires significant knowledge of dozens of IBM i capabilities and their related configurations. Reviewing an IBM i security configuration also requires in-depth knowledge of the implementation of each specific system capability. If you are considering performing your own assessment, it is crucial to be aware of the critical aspects of your IBM i system's configurations that you should inspect. This eBook overviews just some of these important areas and shares how Precisely can help with your assessment needs.

Operating System Security Settings

There are dozens of security-related system values and network attributes that must be assessed to ensure your IBM i system is configured with secure settings. Reviewing these higher-level security settings is an essential step in evaluating your security configuration. To view the security-related system values on IBM i, you can use the WRKSYSVAL(*SEC) CL command.

Security Level

System value QSECURITY controls the security level of your IBM i Server.

This system value must be set to 40 or 50 to ensure a secure IBM i runtime environment

Password Settings

System values exist to control both password composition and expiration intervals. The configuration of these QPWDxxx system values must be examined to ensure they enforce strong password policies on your IBM i.

Audit Level

The QAUDxxx system values control audit support on your IBM i server. These values must be evaluated as part of your security risk assessment to ensure that auditing is active on your system and that the appropriate level of audit data for your enterprise is being captured in the QAUDJRN audit journal.

Network Security

Open Ports

Open ports allow remote access to your IBM i server, and they can act as gateways to other systems. As part of a risk assessment, you must understand which ports are in listening mode on your IBM i and what service is listening at each port. This should be reviewed regularly to ensure that unwanted applications are not running on your system.

Network Servers

There are over 30 network servers that can be started with the Start TCP Server CL command. Additional network servers are started via other interfaces such as the Start Host Servers CL command, available through the Portable Application Solutions Environment (PASE), or older supported technology still in use like the Systems Network

Architecture (SNA).

Configuration of these network servers must be analyzed as part of your risk assessment to ensure appropriate security settings and to validate that only those needed are being started.

Exit Points

Network-related exit programs are a great way to provide additional protection and monitoring for the network servers. However, unauthorized exit programs may cause system degradation or provide sensitive information to unwanted sources. You should check all exit points with exit programs, not only the network exit points, to ensure you know who created the exit programs and why they are in place.

Web and Application Servers

IBM i supports several web servers that are used to host client-server applications running on IBM i. Each of these web server configurations must be analyzed to ensure appropriate security settings have been configured. These settings include the ability to establish an encrypted flow of data between client and server and the authentication requirements when a client connects to IBM i.

User Profiles

Distribution of Powerful Users

It is important to look at the number powerful users on your IBM i system as part of your assessment. Having too many users with a high level of privilege puts your system at risk of a user abusing a powerful profile.

User profiles with special authorities are targets for misuse by either legitimate users or attackers. Special authorities should only be granted to a user or application expected to perform a certain function that requires that authority. As part of your assessment, validate that all profiles with special authorities (*ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE or *SPLCTL) require those authorities to do their jobs.

User Class

User class defines the role granted to a user. As with special authorities, it is essential to ensure that the number of users assigned to powerful user classes is kept to a minimum. Your assessment should include validating that users have a valid reason to be assigned to *SECOFR, *SECADM, *SYSOPR or *PGMR classes.

Limit Capabilities

Limit capabilities should also be assessed to ensure users only have the ability to work from the command line or change the initial menu, initial command line, current library, or attention key program if that is appropriate for their role. You will want to assess whether the users on your system have limited capabilities, partially limited capabilities or capabilities that are not limited.

Disabled and Inactive Users

Disabled profiles present a vulnerability because they can be enabled either by mistake or with malicious intent. Likewise, inactive user accounts, either for employees who have left the company or created for testing purposes, can be a security vulnerability.

Disabled and inactive user profiles should be reviewed as part of your assessment. You will want to determine a reasonable period that profiles can be inactive or disabled before they are flagged as an issue in your assessment.

Data Security

While many of the areas previously discussed can be assessed by examining configurations in the operating system, the security of data must be examined by different means.

Within IBM i, there are two very different database implementations. Db2 is the best understood because it's been around for more than 30 years.The IFS file system, introduced in a later release of IBM i, is also now heavily used by applications to store IBM i data within directories and stream files.

As part of a security risk assessment, each database file and stream file must be investigated to determine if the file contains sensitive data. If so, additional analysis must be performed.

Data at Rest

Once a list of Db2 files and stream files containing sensitive data is created, a more in-depth look is required at object authorities and the use of encryption or Row and Column Access Control technologies.

Object Authority

A comprehensive assessment must ensure that only the appropriate user and group profiles have access to the data and that the public authority of the file is set to *EXCLUDE.

- **Public Authority Setting on Sensitive Objects**
  The ideal public authority setting for any object containing sensitive data is AUT(*EXCLUDE). By default, this prevents an end user who does not have *ALLOBJ special authority from accessing the object in any way. For end users who need access to the sensitive object, authority can be specifically granted. In addition, the public authority setting of the library or directory should also be evaluated to ensure the value set for *PUBLIC is the value you expect.

- **Object Authority and Authorization Lists**
  As part of your risk assessment, you must also analyze the list of users authorized to your sensitive data objects. The Display Object Authority (DSPOBJAUT) and Display Authority (DSPAUT) CL commands will show you both the list of users authorized to an object as well as the public authority of the object. Verify that the list of users authorized to the data object is correct. Authorization lists are used to define a list of users and the authority each user has to any object that is being secured. If your sensitive objects are secured by an authorization list, you must evaluate the users on the list via the Display Authorization List (DSPAUTL) CL command to ensure they should have access to the object.

- **Group User Profiles**
  Group User Profiles are used to share authorities (special authorities as well as authority to objects). When assessing the list of users authorized to an object, you must consider any group profiles with authority to the sensitive object. If a group profile is authorized to the object, then all members of the group profile also have authority. To see the list of users who are a member of a group profile, you can use the Display User Profile (DSPUSRPRF) CL command and the TYPE(*GRPMBR) parameter.

Encryption and Tokenization

On IBM i, encryption is often used to secure data by taking the clear text data and turning it into an unreadable string called ciphertext. Temporarily or permanently replacing data with token values is also acceptable to satisfy certain regulatory requirements or business needs. Your list of sensitive data must be examined to ensure that it is protected by an appropriate method.

If encryption is used, analysis of the encryption key management is also required to ensure the encryption keys are adequately protected and properly managed.

Row and Column Access Control

IBM i also provides Row and Column Access Control, or RCAC, to allow or prevent access to rows of a Db2 table (records of a Db2 file) and to mask data in a particular column (field). For example, you may want a user to see only rows of the table that contain a specific value within a column, such as DEPT = 123. Or, to mask out all but the last four digits in a column, such as ***-**-1234.

As part of a security risk assessment, Db2 files with sensitive records should be inspected to ensure that access to and views of sensitive rows are protected by RCAC.

Data in Motion

Many applications will send data from your IBM i server over a network to a target system for processing or storage. When confidential data is sent over a network, it is essential that the data is encrypted, so an intruder cannot capture it while it is in transit. A risk assessment should analyze all applications that send data over internal and external networks to ensure that the appropriate level of encryption is being used.

To fully protect data while in transit, an assessment should also validate the use of an appropriate network protocol (TLS 1.2 or higher) as well as with the use of an encryption algorithm approved by the National Institute of Standards (NIST).

Determining which network protocol and encryption algorithm (cipher suite) is a difficult task and may require services to evaluate the application. A network application such as WireShark is often necessary to assess the network connection security settings.

Application Security

Determining if your applications are secure poses a significant challenge when performing a security risk assessment. A higher-level examination of the application objects can be performed. For example, what public authority is granted to the application objects? Do the application programs adopt the authority of the program owner? Is the application data encrypted or protected via RCAC?

To completely understand the security posture of an application, penetration testing may be required to try to “break” the application. Penetration testing is a very specialized skill that often requires a service provider to perform the test adequately.

How Precisely Can Help

Performing a detailed security risk assessment is a time-consuming and challenging task. However, in today's high-risk environment, it is required. Seeking help from a trained security professional or using a third-party assessment tool can significantly reduce the time needed to perform an accurate risk assessment, and it provides you with an objective view of your security posture.

Precisely's Assure Security Risk Assessment tool is essential for any organization that wants to understand its IBM i security risks. It checks over a dozen categories of security values, compares them to recommended best practice, reports on findings, and makes recommendations. A high-level summary of risk level is provided for management, while detailed reports provided technical staff with guidance on remediation.

For those who want support from security specialists that can analyze risk assessment results and provide consultation on threat remediation, Precisely also offers risk assessment services. Knowledgeable security professionals can also be engaged to optimally tune your environment and delve deeper into data protection requirements.

If the results of your assessment show vulnerabilities, Precisely's Assure Security can be implemented to add layers of security around your IBM i system and its data. Its capabilities include:

- Assure Multi-Factor Authentication to strengthen IBM i logon security
- Assure Elevated Authority Manager to automate management of authorities
- Assure System Access Manager to control system and data access through exit points
- Assure Encryption to encrypt and tokenize IBM i data at rest
- Assure Secure File Transfer to encrypt data in motion across networks
- Assure Db2 Data Monitor to monitor and block access to sensitive records
- Assure Monitoring and Reporting to extract insights from IBM i journal data and optionally forward those insights to a SIEM

To learn more about Precisely's Assure Security and Assure Security Risk Assessment, visit https://www.precisely.com/product/precisely-assure/assure-security precisely