









# Security Scan

## Executive Summary

The majority of IBM i (AS/400; iSeries; System i) machines today are open to vulnerabilities unique to the IBM i architecture and the applications on the system. This Security Scan reviews vulnerabilities in six major categories and maps them to corresponding COBIT controls. Currently, the risk of a security breach on this system is **High**.

COBIT is a control framework for Information Technology best practices that many auditing firms use as a guide to assess compliance with Sarbanes Oxley (SOX) and other regulations.

Category	Controls Tested (COBIT)	Report
User Access to Data	DS 5.3 - Identity Management DS 5.5 - Security Testing, Surveillance, and Monitoring	
Public Authority to Libraries	DS 5.4 - User Account Management	
User Security	DS 5.3 - Identity Management DS 5.4 - User Account Management	
System Security	DS 5.9 - Malicious Software Prevention	
System Auditing	DS 5.5 - Security Testing, Surveillance, and Monitoring	
Administrator Rights (Special Authority)	AI - 3.2 - Infrastructure Resource Protection DS 5.3 - Identity Management	

Even experienced IT security personnel need quality software tools to monitor, detect, and block security breaches. An enormous number of business transactions occur on your system daily and any of them may be important to your security. A typical IBM i user generates between 50 and 300 security-related audit events each day.

Your system has 68 user IDs, which translates into 3,400 to 20,400 transactions per day. As end users become more sophisticated, the number of security events increases, making it more difficult to detect security breaches.

## User Access to Data

The IBM i is shipped with a variety of network services that are factory-configured and ready to communicate with other computers. All IBM i servers should have network services secured by installing exit programs on IBM network servers to monitor and control network access. Security of user access across the network is **poor** on this system. Some of the most visible network services are:

**FTP:** The FTP server can upload data from a PC to the IBM i and download data to a PC. Any user with a PC can perform the common FTP commands like list directories, change directories, put (upload) files, get (download) files, and delete files.

**Exposure!** On SAMPLE, FTP activity is not being monitored by exit programs and there are no access control rules in place to prevent users from transferring critical data over FTP.

**Database:** ODBC database connections can manipulate information in database files on the IBM i using common SQL commands like UPDATE, SELECT, and DELETE. Most PCs have ODBC drivers installed that allow users to access data directly on IBM i servers. Often, it's as easy as selecting a drop-down menu in Microsoft Excel.

**Exposure!** On SAMPLE, the database server is not being monitored by exit programs and there are no access control rules in place to prevent users from manipulating critical data via ODBC connections.

**Remote Command:** Any user on a PC with IBM's Client Access can issue commands remotely to a IBM i server that they connect to through the network. The limit capability setting on their user profile does not affect their ability to run remote commands.

**Exposure!** On SAMPLE, Remote Command activity is not being monitored by exit programs and there are no access control rules in place to prevent users from entering critical system commands from a PC.

Overall, on SAMPLE, network traffic is not being monitored and access is not being controlled on 27 of the network exit points. 0 of the 27 areas of vulnerability (exit points) are being monitored.

### Relevant COBIT objectives:

#### *COBIT DS5.5: Identity Management*

Ensure that all users (internal, external, and temporary) and their activity on IT systems (business application, system operation, development, and maintenance) are uniquely identifiable.

#### *COBIT DS5.5: Security Testing, Surveillance and Monitoring*

Test and monitor the IT security implementation in a proactive way. IT security should be re-accredited in a timely manner to ensure the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

The following table outlines the exit points for network access servers that were checked on this system.

Exit Point Server	Description	Exit Program	Importance
*REXEC_SO	Remote Command Sign-On (Logon)	No	High
*TFRFCL	Client File Transfer Server	No	High
*RMTRSV	Remote Command Server	No	High
*SQLSRV 2	ODBC & JDBC Server	No	High
*SQLSRV 1	ODBC & JDBC Server	No	High
*FILESRV	Remote File Server (Used when drivers are mapped to IFS)	No	High
*RTVOBJINF	ODBC & JDBC Retrieve Object Info	No	High
*SQL	ODBC & JDBC Sign-On (Logon)	No	High
*NDB	ODBC & JDBC Native Database	No	High
*FTPREXEC	Remote Command through FTP	No	High
*FTPSERVER	File Transfer Protocol (FTP) server on the IBM i	No	High
*FTPCLIENT	File Transfer Protocol (FTP) client on the IBM i	No	Medium
*TELNET	TCO/IP Terminal Emulation	No	Medium
*DQSRV	Client Data Queue Server	No	Medium
*TFTP	Trivial FTP	No	Medium
*DATAQSRV	Remote Data Queue Server	No	Medium
*VPRT	Client Virtual Print Server	No	Low
*FTPSIGNON 1	Allow/Prevent Anonymous FTP	No	Low
*RQSRV	Client Remote SQL Server	No	Low
*QNPSERVER	Virtual Print Server : (Spool File)	No	Low
*QNPSERVER	Virtual Print Server : (Entry)	No	Low
*LMSRV	Client License Server	No	Low
*MSGFCL	Client Message Server	No	Low
*CNTRLSRV	Client Access License Server : (License Mgt)	No	Low
*CNTRLSRV	Client Access License Server : (Conversion Map)	No	Low
*CNTRLSRV	Client Access License Server : (Client Mgt)	No	Low
*SIGNON	OS/400 Sign-On Server	No	Low

Distribution Data Management (DDM) is an IBM protocol that provides users or applications remote access to database files. DDM access to this system is not secured.

#### Command Line Access

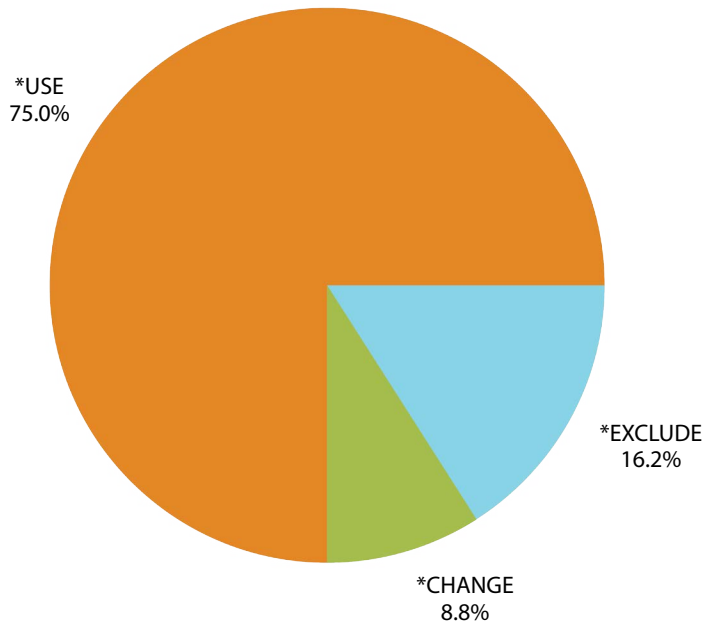
If a user has command line authority (LMTCPB \*NO or \* PARTIAL), they can run virtually any of the more than 2,000 commands that are shipped with the operating system. Some of these commands, such as DSPJOB and DSPLIB, are not of great concern. Others, such as ENDJOB, ENDSBS, and DLTJOB, are of greater concern, especially if the underlying objects are not properly secured. If a user has access to a command line, the number of things they can do is limitless. You can use the LMTCPB attribute of a user profile to limit the command line access of users.

There are 62 user profiles on this system with command line access, 59 of which are enabled.

## Public Authority

IBM i servers are shipped with a default set of users rights assigned to the general public.

The chart below shows that all users (\*PUBLIC) have the rights to read or change 84% of the libraries on the system. All users can delete data or applications from more than 6 (9%) of the libraries.



Authority	Libraries	Percentage
USE	51	75.0
CHANGE	6	8.8
ALL	0	0.0
AUTL	0	0.0
USER DEF	0	0.0
Read and open	0	0.0
EXCLUDE	11	16.2

\*USE = Users have read access only. Users can delete objects from the library (assuming the user has authority to the object).

\*PUBLIC receives \*CHANGE on newly created objects in 30 libraries (44%)

\*PUBLIC access to libraries is a measurement that indicates how accessible the system is to the average end user. As defined by the operating system, \*PUBLIC represents any user that can log in. You can learn more about how to monitor and audit library authority settings, in the [PowerTech Compliance Monitor](#).

## User Security

User and password security are critical because they are the easiest way to compromise a system. On this system the security controls for users and passwords appear to be **moderate**. The following tables overview your user and password security:

### User Security:

On this system 2 areas are a high degree of concern in regard to user security. See the actual numbers below:

User Security Category	Recommendations	SAMPLE
Inactive User ID	0	3 (3 Enabled)
Number of Users with Invalid Sign-On Attempts on 1 Profile	Less than 5	0
Largest Number of Invalid Sign-On Attempts on 1 Profile	Less than 3	0
Unsecured User Profiles	0	0
Users with Default Passwords	0	7 (6 Enabled)

### Password Settings:

The Password Settings table shows that password rules are **weak** on this system.

Password Settings	Standard	SAMPLE
Expiration	90 Days	None
Minimum Length	6 Characters	4 Characters
Digits Required	Yes	No
Different from Previous	10 Passwords	0 Passwords
Block Password Change	24 Hours	*None
Password Rules	Per Corporate Policy	*PWDSYSVAL

Our recommendations for password policy are based on IBM recommendations and the ISO 27002 (formerly known as ISO 17799) standard, which provides detailed guidance for setting strong password policies and managing user accounts. COBIT points out the need for effective management of user accounts.

### Relevant COBIT objectives:

#### COBIT DS5.3 - Identity Management

Ensure that all users (internal, external, and temporary) and their activity on IT systems (business application, system operation, development, and maintenance) are uniquely identifiable.

#### COBIT DS5.4 - User Account Management

Address requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges.

## System Security

The operating system provides a number of methods of securing itself and the workstations connected to it. In this section we examine the system values that protect your operating system and your workstations. The security of the System Values settings is **medium** on this system.

System Value	Value	Ratings	Comments
QSECURITY	40	Good	Your system is running at level 40 (QSECURITY), the minimum setting recommended by IBM.
QALWOBJRST	*ALL	Weak	There are no restrictions on the types of programs that can be loaded on this system. A knowledgeable programmer (including a vendor or contractor) could load programs that bypass your security without being detected.
QVFYOBJRST	1	Weak	Programs are not checked for valid signatures when loaded on this system. The source and authenticity of operating system programs cannot be validated by this system.
QUSEADPAUT	*NONE	Weak	Any system user could create programs that adopt another user's authority.
QDEVRCYACN	*DSCMSG	Good	Jobs that experience communications failure are ended automatically.
QINACTITV	*NONE	Weak	Interactive jobs on this system never time out for lack of use.
QLMTDEVSSN	0	Moderate	There is no limit to the number of concurrent sessions a user can start.
QLMTSECOFR	0	Moderate	There is no limit to which workstations a security officer can sign on to.
QMAXSIGN	5	Moderate	Users are permitted 5 attempts to sign on before an action is taken.
QMAXSGNACN	1	Moderate	Workstation is disabled.
QSCANFS	*ROOTOPNUD	Good	Stream files in the root(/), QOpenSys, and user-defined files systems will be scanned for virus threats.
QSCANFSCTL	*NONE	Moderate	All accesses will be scanned which may degrade system or application performance.

### Scan-Related Exit Points

You have no virus scanning enabled when a file is opened - **Weak**

You have no virus scanning enabled when a file is closed - **Moderate**

Correct settings for the system values in the save and restore category help ensure that no inappropriate or malicious software is installed on the system.

### Relevant COBIT Objectives

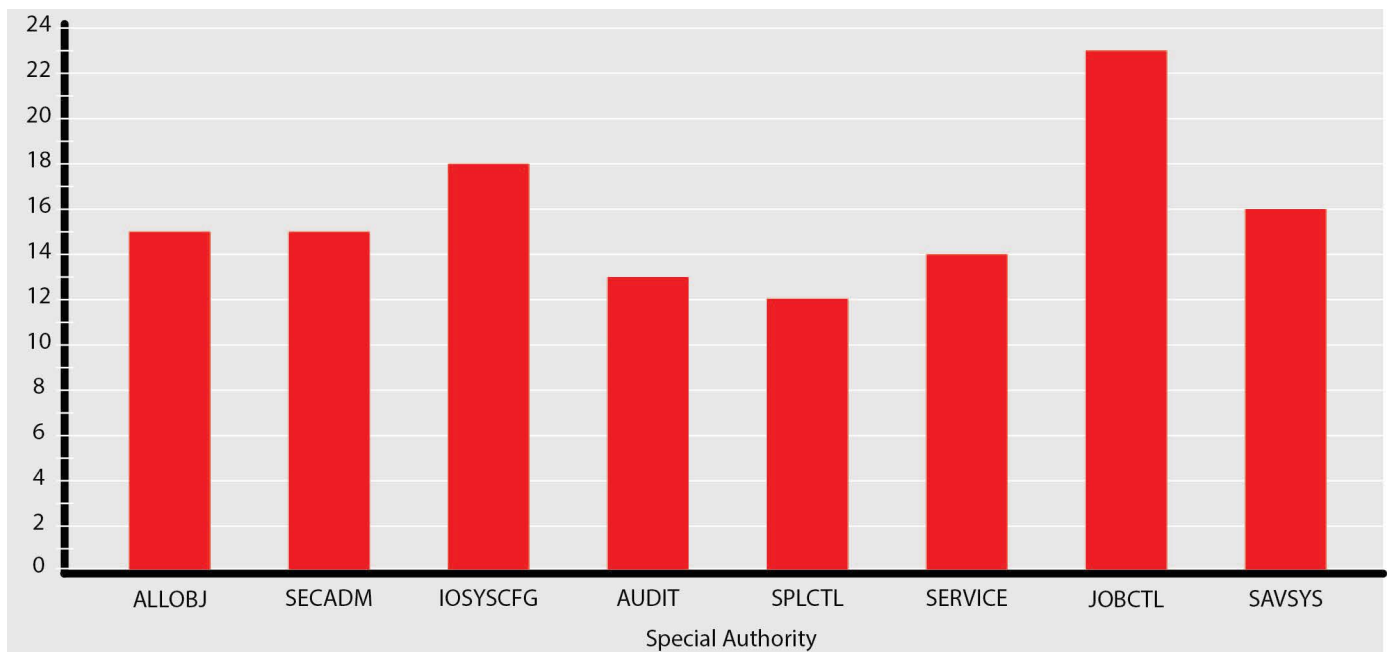
#### COBIT DS5.9 - Malicious Software Prevention, Detention, and Correction

Put preventative, detective, and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

## Administrative Rights

Administrative Rights (root-level privileges) are called special authorities. These rights are very powerful and should be for trusted and knowledgeable IT professionals only. Users with these special authorities should have their activities audited. The risk level due to the number of special authorities on this system is **Moderate**.

The following chart shows that 8 of the 8 special authorities are above our recommended threshold of 10 users with each special authority.



A developer, programmer, or database administrator with \*ALLOBJ special authority on a production system has full access to make changes to sensitive information in databases. Segregation of duties cannot be enforced if the IT staff have special privileges in their everyday business profiles.

### Relevant COBIT objectives:

*COBIT DS5.3 - Identity Management*

*COBIT DS5.4 - User Account Management*

*COBIT AI3.2 - Infrastructure Resource Protection and Availability*

Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated. IBM i servers typically run mission-critical applications, and special authorities grant users special privileges for these components.



## System Auditing

A major feature of the operating system is its ability to log important, security-related events in a secure audit journal. System SAMPLE is using the auditing features on this system **Weak**.

The security log (QAUDJRN) does not exist on SAMPLE.

Audit Value	Description	Value	Importance
*AUTFAIL	Log authority failures	No	High
*DELETE	Log deletion of objects	No	High
*OBJMGT	Log object management changes	No	High
*SYSMGT	Log changes to certain system management areas	No	High
*SAVRST	Log restore actions to security sensitive objects	No	High
*SECURITY	Log security related changes	No	High
*SERVICE	Log usage of the system and hardware service tools	No	High
*PGMFAIL	Log program failures caused by security violations	No	High
*CREATE	Log creation of new objects	No	Medium
*JOBDTA	Log job events such as start and stop	No	Medium
*PGMADP	Log usage of programs that adopt authority	No	Medium
*NETCMN	Log APPN firewall events	No	Low
*OFCSRV	Log Office Vision/400 security changes	No	Low
*OPTICAL	Log usage of optical storage devices	No	Low
*PRTDTA	Log printing functions	No	Low
*SPLFDTA	Log usage of spooled files (reports)	No	Low

The default value for auditing of new objects is to not audit objects. (QCRTOBJAUD)



Auditing Network Events: The operating system provides multiple exit points that enable the monitoring of network traffic due to popular services such as FTP, ODBC, and DOM.

You can review which exit points are monitored on the User Access Section.

### Relevant COBIT objectives are:

#### COBIT DS5.5 - Security Testing, Surveillance, and Monitoring

Test and monitor the IT security implementation in a proactive way. IT security should be re-accredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection of unusual and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

## Recommendations

These recommendations come from compliance checks performed on the system. Using that information, the recommendations were created in priority order, based on three factors: security risk, time to complete, and estimated cost.

### *User Access Recommendations*

Secure and Monitor Network Transactions Immediately - This IBM i server is open to any PC on your network-enabled services. PC-to-IBM i transactions are untraceable and uncontrollable on these servers. This type of network access is the greatest weakness in your current system implementation. We strongly recommend that you control and monitor network activity to and from you IBM i servers. Currently, any user with a PC and valid user ID can access all of the data on the system through network services and bypass your menu security.

[PowerTech Network Security](#) is a leading access control solution for the IBM i that lets you monitor and control network access through edit points.

### *System Auditing Recommendations*

Set Security Event Trigger Points - This system could log thousands of security events daily, but there is no way to sort and filter the important events and notify the right people. Also, the operating system does not provide a way to track TCP/IP traffic, such as ODBS or FTP, to the system. Implement an IBM i security/auditing solution that tells you: who has authority to what? What events are security exposures? What new exposures are being created daily?

[PowerTech Compliance Monitor](#) allows you to automatically generate customized audit reports on a regular basis for each customer.

### *User Security Recommendations*

Implement Standards or User Security - This server does not have consistent standards. We made recommendations based on industry experience and standards. In some cases, you may need to deviate from the industry standard. In those cases, we recommend documenting each deviation.

### *User Security*

Inactive Profiles - Monitor for inactive user IDs and remove them from the system. Eliminate the 3 inactive profiles (3 are enabled) on this system.

Profiles with Default Passwords - 7 profiles have default passwords (6 are enabled). Reduce this number to zero and monitor for new ones.

### *Administrative Rights Recommendations*

Administrative Rights - Special Authority - All of these special authorities should be reviewed and the number of profiles for each should be reduced to the minimum. The rationale for granting these special authorities should be documented. Once the standards are set, start regular monitoring so that any new special authorities are highlighted.

[PowerTech Authority Broker](#) enables companies to cut down on the number of user profiles with special authorities. Users swap to increased privilege levels based on when it is necessary and their actions are audited.