









PowerTech Flash Audit Report Company ABC (SYSTEMXYZ)

8/28/2006

INTRODUCTION

The majority of iSeries machines today are open to vulnerabilities unique to the iSeries Architecture and the applications which reside on the system. This PowerTech Flash Audit reviews security vulnerabilities in **eight** major security areas and, if necessary, recommends specific steps for remediation.

Based on the results of this Flash Audit, this system will need remediation in several areas which currently pose risks in controlling system activity. Given the current assessment of this server, the risk of a security breach on this system is **HIGH**. The recommended remediation will position this system to conform to industry wide best practices as defined by the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT). The following pages will describe the nature of the vulnerabilities in 7 key areas:

SYSTEMXYZ - Questions Answered	Areas	Rating
1. Is your iSeries data safe within its network?	Network Security	
2. Are your assets protected by data security?	User Default Rights (Public Authority)	
3. What are common object authority trends?	System Survey	
4. Are your user profiles secured from attack?	User Security	
5. Are you following IBM security guidelines?	System Security	
6. How well can you detect security related events?	System Auditing	
7. Are powerful user permissions kept in check?	Administrative Rights (Special Authority)	
8. How powerful are your group profiles?	Group Profiles	

Rating Scale

High Risk	Medium Risk	Low Risk
		

Even the most experienced IT security personnel need quality software tools to help them monitor, detect and block security breaches. An enormous number of business transactions occur on your system everyday, and any one of them may be important to your security officer. On average, an iSeries user can generate between 50 and 300 security related audit events each day.

Your system has **564** user ID's, which translates into **28200 to 169200** transactions per day. As the sophistication of end users grows, the volume of security events makes it increasingly difficult to detect security breaches.

DETAILED REPORT

1. NETWORK SECURITY (Is your iSeries safe within your network?)

The iSeries is shipped with a wide variety of network services pre-configured and ready to communicate with other nearby computers. All iSeries systems should have network services secured by installing programs on IBM network servers to monitor and control network access.

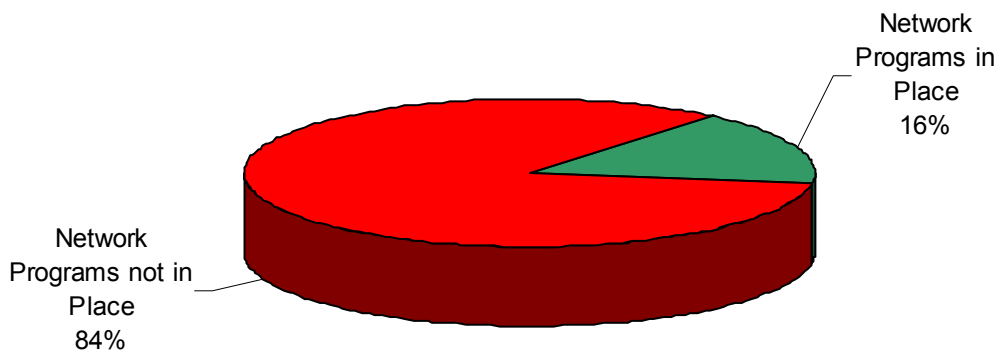
On this server, network traffic is not being monitored and access is not being controlled on 26 of the network points. **Five of the thirty-one areas** of vulnerability (exit points) are being monitored. Therefore, both authorized *and* unauthorized users can upload data, download data, or run commands without detection. Company ABC is susceptible to risks, including theft of intellectual property, without forensic evidence to assist in an investigation. That is, someone could commit fraud and cover their tracks. Several COBIT objectives apply to this section.

COBIT DS5.2 – Identification, Authentication, and Access –“The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules.”

COBIT DS5.10 Violation and Security Activity Reports –“ IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify, and resolve incidents involving unauthorized activity.” Action is required to be able to comply with this objective because currently you cannot log or control important network activity.

There are three ways to access data on an AS/400 system – through a menu and an application, from a system command line, or across a network. Most applications do a sufficient job of securing access through the menu and through command lines. The greatest risk of abuse remains both internal and external network access using data transfer capable tools.

AS400 Exit Programs in Place



Exit Point Server	Description	Exit Program Present	Level of Exposure
*DDM	Alternate ODBC Server	No	High
*DQSRV	Client Data Queue Server	No	High
*FILESRV	Remote File Server	No	High
*FTPCLIENT	TCP/IP Outbound File Transfer	No	High
*FTPSERVER	TCP/IP Inbound File Transfer	No	High
*NDB	ODBC & JDBC Native Database	Yes	High
*RMTSRV	Remote Command Server	No	High
*RTVOBJINF	ODBC & JDBC Retrieve Object Info	Yes	High
*SQL	ODBC & JDBC Signon	Yes	High
*SQLSRV 1	ODBC & JDBC Server	Yes	High
*SQLSRV 2	ODBC & JDBC Server	Yes	High
*TELNET	TCP/IP Terminal Emulation	No	High
*DATAQSRV	Remote Data Queue Server	No	Medium
*FTPREXEC	TCP/IP Remote command thru FTP	No	Medium
*REXEC_SO	Remote Command-Signon	No	Medium
*TFRFCL	Client File Transfer Server	No	Medium
*TFTP	Trivial FTP	No	Medium
*CLI	CLI Connection 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
*FTPSIGNON 1	Allow/Prevent Anonymous FTP	No	Low
*LMSRV	Client License Server	No	Low
*MSGFCL	Client Message Server	No	Low
*RQSRV	Client Remote SQL Server	No	Low
*SIGNON	OS/400 Signon Server	No	Low
*VPRT	Client Virtual Print Server	No	Low
*WSG	5250 screens to a browser	No	Low
QNPSEVR	Virtual Print Server : (Entry)	No	Low
QNPSEVR	(Spool File)	No	Low

Command Line Access:

There are **153** user profiles on this system with Command Line authority, **82** of which are enabled

If a user has Command Line authority (LMTCPB(*NO or *PARTIAL)) on OS/400, they have the ability to run virtually any of the 2000+ command that are shipped with the OS/400 operating system (V5R3). Some of these commands, such as DSPJOB and DSPLIB, may not be of great concern. Other commands 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 that they can do is often limitless.

How commands are entered.

A user can enter commands from a variety of interfaces. Some of the better known command entry points are;

1. The User's Initial Menu
2. Subsequent menu options that such as WRKJOB, WRKOUTQ or WRKJOBQ, or other IBM screens
3. Hidden Function Keys (F17) in business applications
4. FTP prompts
5. Clients Access' Remote Command facility
6. DDM's Remote Command facility
7. REXEC.

As a general rule, end users should not be given direct access to OS/400 commands. Preventing users from typing commands at any given interface requires a two step process. First, change the user profile to LMTCPB(*YES). This tells the operating system that thus user is not allowed to enter command at an OS/400 command line, or through the FTP prompt. Second, implement an exit program on both the DDM and the REXEC exit points that will block remote commands submitted by most or all users.

2. USER DEFAULT RIGHTS - Public Authority (What type of access do your users have?)

iSeries servers are delivered from IBM with a default set of user rights assigned to the general public. The default set of rights for this server **are too permissive** for most computing environments.

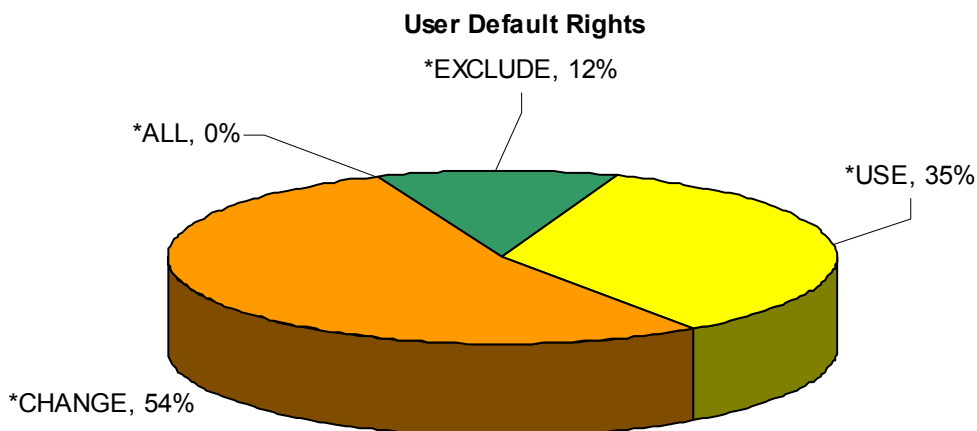
The chart below shows all users have the rights to read or change 88% of the libraries on this system. All users can delete data or applications from more than 107 of the libraries. (53 %)

Public receives ***CHANGE (or *ALL)** on newly created objects in 192 libraries (96%)

With these settings and the lack of network security, Company ABC is susceptible to unintentional, experimental, or malicious acts that could result in data loss, theft, or fraud.

To mitigate the risk of unauthorized access, auditors recommend that ***PUBLIC** is ***EXCLUDE** on every significant production database and source code and that individuals or groups of individuals are specifically given the necessary authority as required. Some iSeries applications will not work properly if you designate ***PUBLIC** is ***EXCLUDE**. We will review effective ways to meet this requirement without having to designate ***PUBLIC** to ***EXCLUDE** in all cases. Generally, your system allows individuals access to data far beyond their demonstrated need. This will need to be changed to adhere to the following best practices as defined in CoBIT:

COBIT DS5.3 – Security of Online Access to Data - ...IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change, or delete data.



3. SYSTEM SURVEY (What are common object authority trends?)

PowerTech collected sample data from the system on object authority or ownership. The following results were found...

Surveyed Application: JDE

Library Owner = JDE *Public Authority = *ALL

Object Owner: JDE *Public Authority = *ALL

PowerTech confirmed with the client that most of the sensitive objects in the Authorization application have the same Library and Object level authority as the surveyed objects therefore PowerTech's assessment will be based on this information...

Library/Object Owner = JDE

PowerTech found that all JDE data is owned by JDE group profile. Having object ownership means that the data can be viewed, copied, changed, or deleted. **82** users belong to JDE Group profile and assume the same authority. These users on the system have the authority to view, copy, change and delete all JDE data as well as delete the JDE library. With working knowledge of TCP/IP connectivity, valid AS/400 profile, any PC user can utilize common tools such as Microsoft Excel, Access, DOS or even IBM Client Access to access data undetected and exercise this heightened authority. All of this activity, ODBC, FTP, DDM, etc., is transparent to the system and cannot be controlled through the menu.

***Public = *ALL**

PowerTech found that all JDE data files grant *Public ALL authority. Any object that grants *Public ALL rights means that all system users have authority to **view, copy, change, or delete** those objects. With working knowledge of TCP/IP connectivity, valid AS/400 profile, any PC user can utilize common tools such as Microsoft Excel, Access, DOS or even IBM Client Access to access data undetected and exercise this heightened authority. All of this activity, ODBC, FTP, DDM, etc., is transparent to the system and cannot be controlled through the menu.

▶ **Exposure:** All PC users, with a valid profile and sign-on, can access data through TCP/IP services (i.e. Remote Command, FTP, DRDA, etc.) and (at minimum)...

- View, Copy, Change, or delete all JDE data.

- All users can delete the JDE Library and all data that is contained within.

*Note: IBM native OS does not provide any means of tracking or auditing PC transactions via FTP, ODBC, Telnet, etc.

Sarbanes-Oxley Act: Requires CEOs/CFOs to implement financial and IT controls to prevent and detect any attempted financial manipulation. CEOs/CFOs must certify on a quarterly basis that financial and IT controls are in place, and are effective. The new controls must be able to identify any personnel that attempt to alter established accounting methods or any existing financial records in an effort to enhance their company's financial performance reports.

*All users can manipulate financial data on the system. Also since the IBM native operating system does not audit nor provide any means to detect this activity, it is our opinion that this system is **not Sarbanes-Oxley compliant**.

4. USER AND PASSWORD SECURITY (Can user IDs be compromised?)

User and Password Security are critical because they are the most obvious, and the most exploited, method of compromising a system. The following charts are an overview of your User and Password Security. On this system the risk of attacks on users and passwords is **MEDIUM**.

One of the most difficult aspects of user and password security is that the elements can change from day to day. For instance, today there may be no invalid sign on attempts, but tomorrow there could be over 100, indicating an attempted hack. We recommend putting solutions and processes in place to constantly monitor these areas.

User Security

On this system **all 5 areas are a high degree of concern**. See the actual numbers below:

Category	Standard	System XYZ
Inactive User IDs	0	249 (175 Enabled)
Number of Users with Invalid Sign on Attempts	5	21
Largest number of Invalid Sign on Attempts on 1 profile	< 3 per profile	11
Unsecured User Profiles	0	1
Users with Default Passwords	0	25 (7 Enabled)

Password Security Chart

The Password Rules chart shows that password rules are **good** on this system. On the iSeries a standard password rule set is made up of these four elements. This system complies with all 4 password recommendations.

Password Setting	Standard	System XYZ
Passwords should expire in less than:	90 days	60 days
Minimum Length	6 characters	6 characters
Are Digits Required?	Yes	Yes
Password must be different from previous:	10 passwords	32 passwords

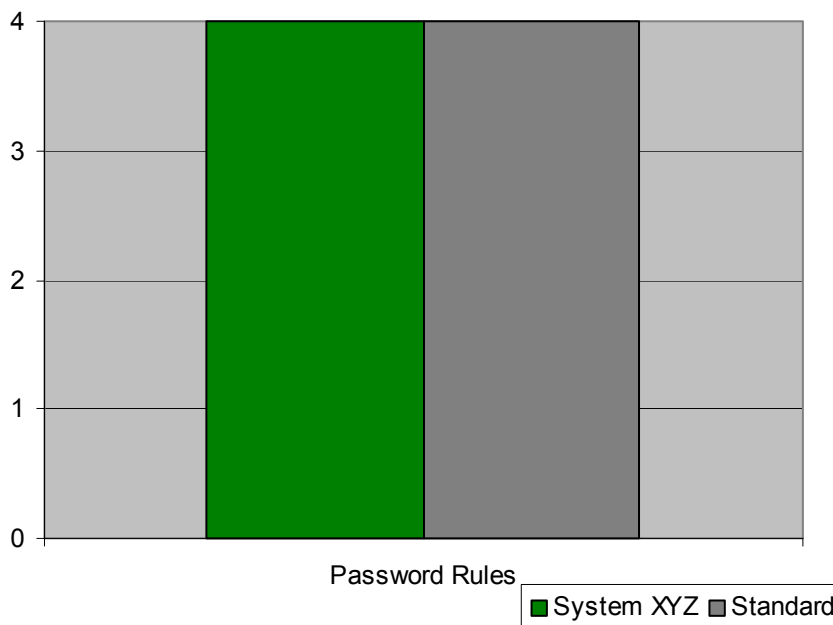
Our recommendations for password policy are based on sections 9.3.1 and 9.5 of the ISO 17799 standard, which provide detailed guidance on setting strong password policies and managing user accounts. CobiT points out the need for effective management of user accounts:

COBIT DS5.4 – User Account Management

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts.

COBIT DS5.6 - User Control of User Accounts

Users should systematically control the activity of their proper account(s)...



5. SYSTEM SECURITY (Are you following IBM's minimum security recommendation?)

OS/400 provides a variety of methods of securing both the operating system itself, and the workstations that are connected to it. In order for the operating system to stay intact, you must carefully monitor programs (typically from third party vendors) that attempt to modify operating system objects. Additionally, when a user logs on to your system, each terminal session represents a security exposure anytime a user walks away and leaves the terminal session unattended. In this section we examine the system values that protect your Operating system and your workstations.

	Protecting the Operating System
Weak	There are no restrictions on the types of programs that can be loaded on this system. A knowledgeable external programmer (such as a vendor or a contractor) could load programs that bypass your security without being detected. (QALWOBBJRST)
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. (QVFYOBJRST)
Moderate	Any user of this system could create programs that adopt another user's authority. (QUSEADPAUT)
Good	Your system is running at level 40 (QSECURITY). This is the IBM minimum recommended setting.

	<u>Workstation Security</u> - Users logged onto interactive sessions present a security risk if those workstations can be used by other users or otherwise compromised
Good	Interactive jobs on this system time out for lack of use after 45 minutes (QINACTITV)
Moderate	There is no limit to which workstations a security officer can sign on to. (QLMTSECOFR)
Good	Jobs that experience a communications failure are automatically ended (QDEVRCYACN).
Moderate	There is no limit to the number of concurrent sessions a user can start (QLMTDEVSSN).
Good	After 3 invalid sign-on attempts, user profiles are disabled

6. SYSTEM AUDITING (How well are you watching?)

System auditing is comprised of two functions: logging and reporting. *Logging* simply means events are recorded in a secure log. *Reporting* is where *relevant* security events are brought to the attention of system administrators and site management. Logs are an important information source for intrusion detection/prevention and vulnerability assessments.

Security events **are** logged at Company ABC. However it is unclear whether those logs are being monitored for discrepancies. It should be noted that an average user typically creates between 50 and 300 security events each day, and the use of automated monitoring tools is suggested for effective system management.

It is important to collect the data, in order to effectively manage default user rights, network security, user and password settings, system security, and administrative rights. But it is more important to have a monitoring discipline in place that continually tracks these areas for changes. Often times, this is best done with automated monitoring tools.

Network Events: The operating system provides multiple exit points that enable the monitoring of network traffic over popular services such as FTP, ODBC, and DDM. This system does not provide any means to track or audit network transactions from PC's or other nearby computers. This inability to monitor should be addressed immediately to comply with regulatory standards such as Sarbanes-Oxley.

The CobiT objectives are clear on the need for security auditing and monitoring.

COBIT DS 13.6 - Operations Logs

“Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing ...”

COBIT DS 5.7 - Security Surveillance

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

System Name	Logging Data	Audit Tools
System XYZ	Yes	No
Rating	Strong	Weak

SYSTEM AUDITING (Continued)

Audit Values on the system are your assurance that actions can be traced to their original users. This system comes standard with a full range of auditing capabilities to assure compliance with industry and government standards.

Audit control features have been turned on at the system level

The Default value for auditing of new objects is to not audit objects.

1 of the sixteen possible system wide auditing values have been enabled. The Status of these audit values are as follows:

Audit Value	Description	System Value	Importance
*AUTFAIL	Log Authority failures	YES	High
*DELETE	Log deletion of objects	YES	High
*OBJMGT	Log object management changes	YES	High
*SYSMGT	Log changes to certain system management areas	NO	High
*SAVRST	Log restore actions to security sensitive objects	YES	High
*SECURITY	Log security related changes	YES	High
*SERVICE	Log usage of the system and hardware service tools	YES	High
*PGMFAIL	Log Program failures caused by security violations	YES	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
*OFCSRVR	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

For a complete discussion on recommended audit settings, refer to the article “Common Sense Security Auditing” on the PowerTech website at http://www.powertechgroup.com/pt-solutions_auditwhitepapers.html

SYSTEM AUDITING (Continued)

Network Events (Exit Point): IBM native OS supplies 31 exit point or backend TCP/IP ports, the system does not provide any means to track or audit PC transactions such as FTP, ODBC, DDM, etc. The following Table depicts exit point servers that can be audited and associated exposure levels. Level of exposure is based on average amount of server use and ease of exploitation.

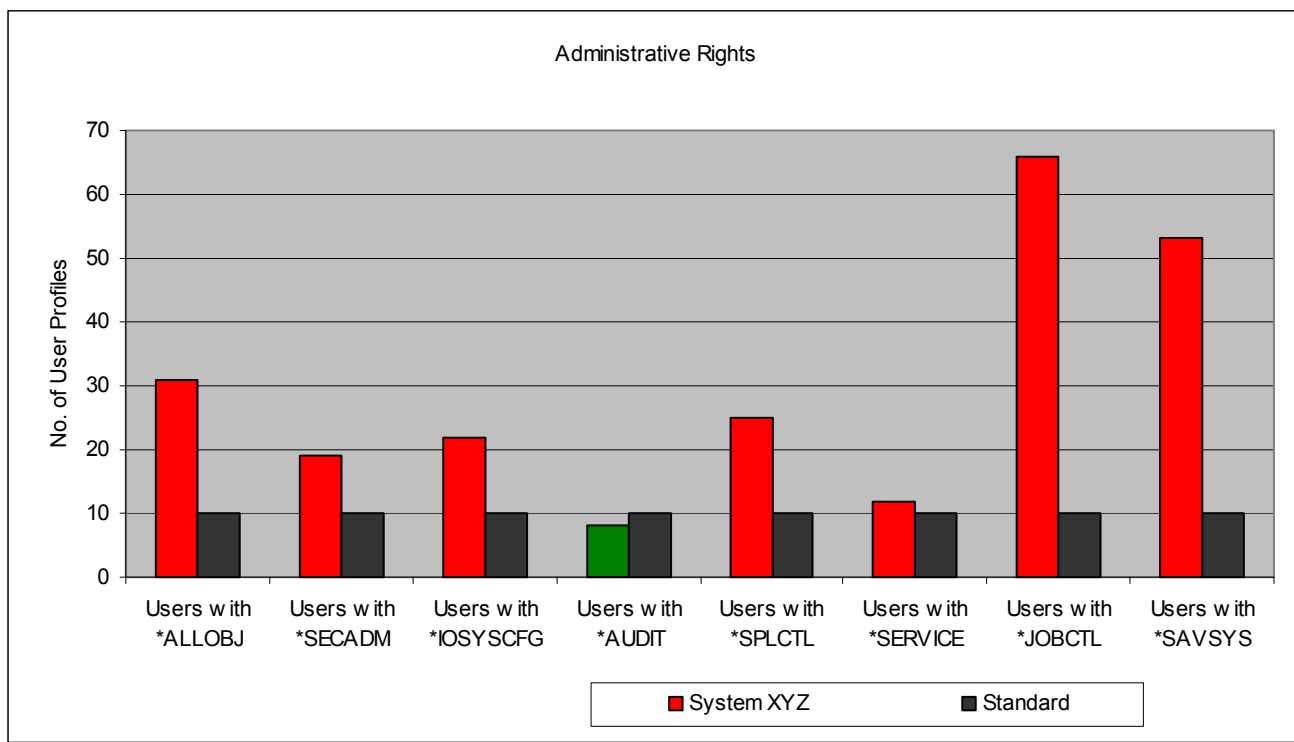
Exit Point Server:	Description	Exit Program Present	Level of Exposure
*DDM	Alternate ODBC Server	No	High
*DQSRV	Client Data Queue Server	No	High
*FILESRV	Remote File Server	No	High
*FTPCIENT	TCP/IP Outbound File Transfer	No	High
*FTPSEVER	TCP/IP Inbound File Transfer	No	High
*NDB	ODBC & JDBC Native Database	Yes	High
*RMTSRV	Remote Command Server	No	High
*RTVOBJINF	ODBC & JDBC Retrieve Object Info	Yes	High
*SQL	ODBC & JDBC Signon	Yes	High
*SQLSRV 1	ODBC & JDBC Server	Yes	High
*SQLSRV 2	ODBC & JDBC Server	Yes	High
*TELNET	TCP/IP Terminal Emulation	No	High
*DATAQSRV	Remote Data Queue Server	No	Medium
*FTPREXEC	TCP/IP Remote command thru FTP	No	Medium
*REXEC_SO	Remote Command-Signon	No	Medium
*TFRFCL	Client File Transfer Server	No	Medium
*TFTP	Trivial FTP	No	Medium
*CLI	CLI Connection Server	No	Low
*CNTRLRV	Client Access License Server): (License Mgt)	No	Low
*CNTRLRV	Client Access License Server): (Conversion Map)	No	Low
*CNTRLRV	Client Access License Server): (Client Mgt)	No	Low
*FTPSIGNON 1	Allow/Prevent Anonymous FTP	No	Low
*LMSRV	Client License Server	No	Low
*MSGFCL	Client Message Server	No	Low
*RQSRV	Client Remote SQL Server	No	Low
*SIGNON	OS/400 Signon Server	No	Low
*VPRT	Client Virtual Print Server	No	Low
*WSG	5250 screens to a browser	No	Low
QNPSERVR	Virtual Print Server : (Entry)	No	Low
QNPSERVR	(Spool File)	No	Low

7. ADMINISTRATIVE RIGHTS - Special Authority (What kind of power do your users have?)

Administrative Rights, called Special Authorities in AS/400 jargon, are rights that are granted to allow a specific security sensitive function to be performed by specific users for a specific reason. These rights are very powerful and should be reserved only for trusted and knowledgeable IT professionals. In addition, users with these special authorities should have their activities subject to independent review.

There are eight types of administrative rights delivered by IBM, and it is important to monitor and manage the dissemination and use of these rights. Auditors are increasingly concerned about how an organization manages these powerful profiles, given known damage caused by disgruntled current and former employees.

The following chart shows that **7 of the 8 special authorities** are well above the recommended thresholds. For most organizations there should be less than 10 profiles with any of these special authorities. This is an area of concern for Company ABC because special authorities appear to be excessive. **Work to remove the administrative rights from most users, and continuously monitor that these rights are not redistributed.**



(See Special Authorities page in Appendix A for definitions of these authorities)

This iSeries system has too many profiles that are too powerful. In the hands of careless or disgruntled employees, this could result in data loss, theft, or damage. CoBIT objectives point out the need for management to check the recorded accountability of user accounts on a regular basis:

COBIT DS5.5 – Management Review of User Accounts

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

8. GROUP ADMINISTRATIVE RIGHTS (What special authorities do groups do you have?)

Group profiles are an efficient method of managing security for large numbers of employees who perform similar job functions. Historically, iSeries applications have used group profiles to provide end users with access to an application, and, in unchecked cases, have provided end users ownership of all application objects. During the execution of an application, a member of a Group Profile inherits all of the group's regular authority as well as the group's Special Authority. In applications where the group profile also owns the application, the effect is to extend ownership rights to every member of the group. For this reason it is important that Group authority be tightly scoped and judiciously distributed.

Group Special Authorities –

There are 2 group profiles on this system that have some level of Special Authority. These two group profiles have a combined membership of 22 users.

Group Name	Total Members	Special Authorities						
Group1	20			*IOSYSCFG			*JOBCTL	*SAVSYS
Group2	2			*IOSYSCFG			*JOBCTL	*SAVSYS
Total	22			22			22	22

Group Object Ownership –

In addition to the problem of widely dispersed group special authorities, group profile object ownership presents a significant security risk on this system. If group profile QPGMR were to shed it's *ALLOBJ special authority a serious risk to overall system security would only be slightly reduced, because the 961 members of this group profile will still have complete access to, and control over, 256,941 production application objects owned by the QPGMR group.

Group Name	Total Members	Total Objects Owned
Group1	20	100
Group2	2	200
Total	22	

Recommendations for System: SYSTEMXYZ

These recommendations are based on Flash Audits performed for Company ABC on the SYSTEMXYZ system. Using the information from that analysis, a recommendation for remediation has been created in priority order. The priority is based on three factors: security risk, time to complete and estimated cost.

1. **Secure and monitor network transactions Immediately – This iSeries server is open to any PC on your network through a variety of network enabled services. PC to iSeries transactions are untraceable and uncontrollable on these servers.** This type of network access is the greatest weakness in your current system control implementation. We strongly recommend that you control and monitor network activity to and from your iSeries servers. Currently, any user with a PC and valid AS/400 ID can access all data on the system through network services, bypassing your traditional menu security.
2. **Set Security Event Trigger Points** – This system could log potentially thousands of security events each day, but there is no tool to sort and filter the most important events and bring those to the attention of the proper individual. Also the native OS does not provide means to track any TCP/IP traffic, such as ODBC, FTP, etc., to the system. Consider implementing an iSeries security/auditing solution that tells you: - Who has authority to what? What events represent security exposures? What new exposures are being created on a daily basis?
3. **Implement Standards for User Security and Administrative Rights** – This server does not appear to have consistent standards. We have made recommendations based on industry experience and standards. In some cases the industry standard may need to be deviated from, but in those cases we would recommend clear documentation for this deviation.
 - o **User Security -**
 - Profiles with Default Passwords – 25 profiles have default passwords (7 are enabled). Reduce this number to zero and monitor for new instances.
 - Inactive Profiles – Monitor for inactive User ID's and remove them from the system promptly. Eliminate the 249 inactive profiles (175 of which are enabled) on this system.
 - Unsecured Profiles – Eliminate unsecured profiles. Identify the profiles that the public could hijack and secure those profiles.
 - a. **Administrative Rights – Special Authority** - All of these Special Authorities should be reviewed and the number of profiles for each should be reduced to the bare minimum. In all cases the rationale for granting these special authorities should be documented. Once the standards have been set, regular monitoring should be instituted so that any new special authorities are immediately brought to light.

Special Authority	Number of Users	Special Authority	Number of Users
*ALLOBJ	31	*AUDIT	6
*IOSYSCFG	20	*JOBCTL	32
*SAVSYS	22	*SECADM	32
*SERVICE	6	*SPLCTL	21

Appendix A: Special Authorities Definitions (Administrative Rights)

1) All-Object Authority (*ALLOBJ)

This is the most powerful authority on any AS400 system. This authority grants the user complete access to everything on the system. A user with All-Object Authority cannot be controlled.

Risk: Extremely High **Difficulty to Exploit:** No difficulty

2) Service Authority (*SERVICE)

Service Authority provides the user with the ability to change system hardware and disk configurations, to sniff network traffic and to put programs into debug mode (troubleshooting mode) and see their internal workings. The system services tools include the ability to trace systems functions and to patch and alter user made and IBM delivered programs on disk manipulate data on disk.

Risk: Extremely High **Difficulty to Exploit:** Moderately difficult

3) Save and Restore Authority (*SAVSYS)

This authority allows the user to backup and restore objects. The user need not have authority to those objects. The risk with SAVSYS Authority is that a user with this authority can save all objects (including the most sensitive files) to disk (save file), delete any object (with the Free Storage option), restore the file to an alternate library, and then view and alter the information. Should the user alter the information, they would have the ability to replace the production object with their saved version.

Risk: High **Difficulty to Exploit:** Low difficulty

4) System Configuration Authority (*IOSYSCFG)

System communication configuration authority can also be used to set up nearly invisible access from the outside as a security officer -- without needing a password. System Configuration Authority provides the ability to configure and change communication configurations (e.g. lines, controllers, devices), including the system's TCP/IP and Internet connection information.

Risk: Extremely High **Difficulty to Exploit:** Moderately difficult

5) Spool Control Authority (*SPLCTL)

Spool Control authority gives the user read and modify all spooled objects (reports, job queue entries, etc.) on your system. The user may hold, release and clear job and output queues, even if they are not authorized to those queues.

Risk: High **Difficulty to Exploit:** No difficulty

6) Security Administrator Authority (*SECADM)

Security Administrator grants the authority to create, change and delete user ID's. This authority should be reserved to essential administration personnel only.

Risk: High **Difficulty to Exploit:** No difficulty

7) Job Control Authority (*JOBCTL)

Job Control Authority can be used to power down the system or to terminate subsystems or individual jobs at any time, even during critical operational periods. Job Control Authority provides the capability to control *other user's* jobs as well as their spooled files and printers.

Risk: Moderate **Difficulty to Exploit:** Low difficulty

8) Audit Authority (*AUDIT)

Audit Authority puts a user in control of the system auditing functions. Such a user can manipulate the system values that control auditing and control user and object auditing. These users could also turn off auditing for sensitive objects in an effort to obscure certain actions

Risk: Moderate **Difficulty to Exploit:** Low difficulty