WHITE PAPER

Managing IBM i Privileged Users for Regulatory Compliance

This white paper discusses best practices in managing, limiting, and auditing privileged or powerful user accounts on your Power Systems™ servers running IBM i (System i, AS/400). What are the security exposures from powerful user accounts and special authorities such as *ALLOBJ? What are your auditors looking for? How do Information Technology frameworks such as COBIT and ISO 27002 affect your business, and how can you configure your system to comply with them? You'll learn the answers to these questions and explore some best practices for reducing your security exposures from powerful users on your system.

The past few years have seen an increased emphasis on the security and control of critical corporate Information Technology (IT) assets in companies, both large and small. This new emphasis is driven largely by U.S. legislation such as the Sarbanes-Oxley Act (SOX), the California Privacy Act (SB1386), the Health Insurance Portability and Accountability Act (HIPAA), and the federal Gramm-Leach-Bliley Act (GLBA). Many other countries and jurisdictions also are emphasizing the need for IT organizations to monitor and protect valuable data assets. In response, companies are scrambling to implement IT security plans against which they can demonstrate their adherence to best practices and thus their compliance with regulations. One of the top concerns of auditors on the Power Systems and other platforms is the proliferation of unregulated and unmonitored users with powerful privileges. On IBM i servers, we define powerful accounts as any account with special authorities, or simply those with direct rights to production data.

This white paper looks at some of the most common exposures that result from such powerful profiles. We then relate these vulnerabilities to the relevant COBIT and ISO 27002 controls, and suggest best practices for managing and reducing the number of powerful profiles. We also recommend techniques for dealing with programming staff who need to have emergency access to production data.

The Risks and Exposures of Special Authorities in IBM i

Let's start by reviewing some of the potential exposure on an IBM i server. Special authorities are rights granted to a user that specifically exempt that user from the restrictions normally enforced by traditional IBM i security. The reason special authorities exist is to provide a select number of highly trusted users with the ability to circumvent security controls when business conditions require it. These "security bypass" rights are very powerful and should be reserved only for trusted and knowledgeable IT professionals. And because of their power, security frameworks such as COBIT and ISO 27002 require that the use of these special authorities should be subject to monitoring and management review.

In IBM i, when you create or change a user profile, you implicitly or explicitly assign special authorities to the user profile. When you assign a user class (for example, *SECOFR, *SYSOPR, *USER, *PGMR) to a user profile, you also assign a set of default special authorities to the user. The following table shows the default special authorities that are assigned to each user class:

User Class	Default Special Authorities
*SECOFR	All special authorities
*SECADM	*SECADM
*PGMR	None
*SYSOPR	*JOBCTL and *SAVSYS
*USER	None

There are eight types of special authority in IBM i. It is vitally important to monitor and manage the distribution and use of these rights.

1) Total Access (*ALLOBJ)

*ALLOBJ authority is the most powerful authority on any Power Systems server. This authority, which is roughly equivalent to root on a UNIX system, grants the user complete access to all libraries, data, and programs on the system. A user with All Object authority cannot be controlled. An employee with access to this special authority, and who is either careless or has malicious intent, would have very little difficulty in exploiting his or her authority to steal critical data, damage production systems, or otherwise wreak havoc on a system. Access to *ALLOBJ special authority implicitly provides the user with access to the other seven special authorities.

2) Authority to Create New Users (*SECADM)

Security Administrator (*SECADM) grants the authority to create, change, and delete user IDs. The ability to create and change IDs implies the ability to extend access to other individuals and thus requires careful monitoring. This authority should be reserved for essential administration personnel only.

3) Ability to Configure Communication Routes (*IOSYSCFG)

System Communication Configuration authority (*IOSYSCFG) provides the ability to configure and change communication configurations (lines, controllers, devices, and so on), including the system's TCP/IP and Internet connection information. In knowledgeable hands, System Communication Configuration authority also can be used to set up nearly invisible access from the outside as a security officer—without needing a password.

4) System Auditing (*AUDIT)

Audit authority (*AUDIT) puts a user in control of the system auditing functions, allowing access to sensitive security logs that could expose system weaknesses. Users with *AUDIT also can manipulate the system values that control auditing, including user and object auditing. In addition, these users could turn off auditing for sensitive objects to obscure certain actions.

5) Complete Authority Over All Reports and Jobs (*SPLCTL)

Spool Control authority (*SPLCTL) gives the user rights to read and modify all spooled objects (for example, reports, job queue entries) on your system. The user can hold, release, and clear job and output queues, even if they're not authorized to those queues. For example, a user with spool control authority could read and modify critical payroll data once it's been sent to a printer. It's not possible to hide the data in reports from a user with *SPLCTL special authority.

6) Hardware Service Access (*SERVICE)

Service authority (*SERVICE) gives the user the ability to change system hardware and disk configurations, to "sniff" network traffic, to put programs into debug mode (troubleshooting), and to see their internal workings. The system services tools include the ability to trace system functions and to patch and alter user-written and IBM-delivered programs on disk. It also allows users to turn RAID parity on and off and to remove disk drives from the system. The number of users with this powerful authority should be tightly limited.

7) Regulated Authority Over All Reports and Jobs (*JOBCTL)

Job Control authority (*JOBCTL) 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 users' jobs as well as their spooled files and printers. *JOBCTL differs from *SPLCTL in that it can be regulated and restricted, though our experience shows us that it often is not.

8) System Save Capability (*SAVSYS)

The risk with *SAVSYS authority is that users with this authority can save all objects (including the most sensitive files) to disk (as a save file), restore the file to an alternate library, and then view and alter the information. After they alter the information, they may even have the ability to replace the production object with their saved version. These same users can delete any object (using the Free Storage option on SAV* commands) on the system regardless of their regular authority to that object.

You can find basic-level information about the number of profiles on your system that have special authorities by entering the following command on a command line:

```
PRTUSRPRF TYPE (*AUTINFO) SELECT (*SCPAUT)
```

Or, if you have auditing software installed, it may be easier to use a report that shows the list of users with special authorities (for example, the User Authority Control report in PowerTech's Compliance Monitor).

You also should pay special attention to group profiles with special authorities. Be aware that while some profiles might not have special authorities themselves, they may inherit those special authorities through membership in one or more groups.

Power Through Too Much Authority

A user profile does not require special authorities to be powerful—the power can come from the fact that the profile may own or have access to important production data. By default, the owner of an object has complete authority to the object. This includes the ability to see the contents of the object, change any attribute or data element in the object, and move, rename, specify security for, and/or delete the object. Having end users, development staff, or third-party vendors own production objects is not a good idea. Nor is it a good idea for end users, operators, or other IT staff to have *CHANGE or *ALL rights to sensitive production data.

Again, it's important to pay special attention to the group profiles that own data. Object ownership in IBM i gives powerful rights to the owning profile, and if the owner of an object is a group profile, to any member of that group.

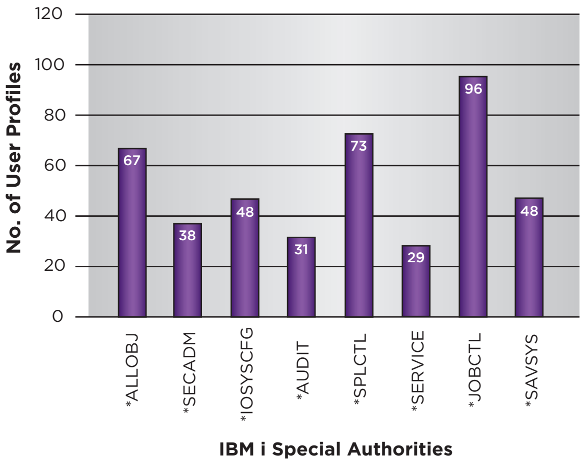
The State of IBM i Profiles Today

Over the past several years, PowerTech has published an annual State of IBM i Security study,[1] based on a series of high-level audits conducted the previous year. The 2010 study contained data from 202 Power Systems servers from a diverse mix of 125 companies audited during 2009. In the category for IBM i special authorities, the results were remarkable:

- The average system had 67 profiles with *ALLOBJ special authority.
- Only 5 percent of the systems reviewed in the study had fewer than 10 users with *ALLOBJ authority.

These statistics demonstrate a glaring vulnerability in the vast majority of systems today. With *ALLOBJ authority, IT staff can bypass any change management software that is in place and make changes directly to production data. Figure 1 shows the average number of user profiles with each special authority on these systems.

FIGURE 1: POWERFUL USERS (SPECIAL AUTHORITIES)



While it's difficult to create a hard and fast rule for all environments, we recommend that the number of users with each special authority be kept to the barest minimum. As a rule of thumb, when the number of users with powerful authorities approaches 10, closer scrutiny is warranted. Section 11.2.2 of the ISO 27002 standard says that such special privileges should be "restricted" and "controlled through a formal authorization process."

The study indicates that there are far too many powerful profiles on our Power Systems servers. Auditors take exceptions to programmers or other IT staff with *ALLOBJ authority, yet in many cases, users have this most powerful authority because they occasionally need it for emergency access to, and repair of, production applications.

What Are Auditors Looking For?

As part of any standard audit of a Power Systems server, auditors check for the abuse of special authorities. Even auditors who are not familiar with IBM i are aware of this issue from their work on other platforms. In a presentation at the 2004 Gartner IT Security Summit, Ernst & Young[2] noted the following as two of its top 10 concerns in audit reviews of IT systems:

- The large number of users with access to "super user" transactions in production
- The ability of development staff to run business transactions in production

Other Big Four audit firms note that on IBM i systems, the assignment of special authority to system users must be limited to those job functions that really require it, and the granting of such privilege must be authorized by management in writing.

Many audit firms use the Control Objectives for Information and related Technology (COBIT) standard from the IT Governance Institute as a comprehensive guideline for determining whether a firm is complying with best practices.

[1] *2010 State of IBM i Security*, which can be downloaded at *www.powertech.com*.

[2] *Sarbanes Oxley: How Does It Affect the IT Department?* Ernst & Young presentation by Teri Shaffer, Gartner IT Security Summit, June 2004

COBIT Regulations

COBIT is a framework of generally applicable and accepted IT governance and control practices promoted by ISACA (Information Systems Audit and Control Association).[3] It is the control framework most often used by IT auditors. Several COBIT regulations are relevant to the use and review of powerful user accounts on Power Systems servers:

COBIT DS 5.4—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. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges." (COBIT 4.1)

Power Systems: *Regularly review the assignment of special authorities, special user classes, and ownership of production data. Do these assignments match the documented security policy?*

COBIT DS 5.5—Security Testing, Surveillance and Monitoring

"Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited 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 and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed." (COBIT 4.1)

Power Systems: *IT management and any other interested parties should be notified any time anyone requests access to a powerful profile to fix production systems.*

COBIT AI6.3—Emergency Changes

"Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process." (COBIT 4.1)

Power Systems: *Emergency changes are a part of life. There should be a policy and procedure in place in advance to deal with such changes. Emergency or temporary access to production systems should be configured in advance and closely scrutinized after the fact. Any temporary access to higher authorities should be fully approved and reviewed by the appropriate management, including the owners of the data.*

ISO 27002

ISO 27002, an internationally recognized information security standard, has found more widespread use in the United States in recent years. Many companies use the ISO standard alone to define their security policy, or they use it to provide more detailed guidance on the security-specific issues outlined by COBIT.

The ISO 27002 standard is an information security-specific standard; whereas COBIT applies more broadly to information technology in general. As such, the ISO standard often provides considerably more detailed guidance on topics of information security.

This standard contains 11 security control clauses collectively containing a total of 39 main security categories. It is quite specific in its recommendations for privileged user management.

Power Systems: *Special authorities should be granted based only on business need requirements. System operators and development staff should be granted special authorities only temporarily on a "need-to-use" or "event-by-event" basis. Programmers and development staff should not own or have change*

[3] *www.isaca.org*

rights to production data. They should not have regular and continuous access to special authorities in the user profiles that they use on a daily basis.

ISO 27002—Section 11.2.2 Privilege Management (ISO/IEC 27002)

Control

The allocation and use of privileges should be restricted and controlled.

Implementation guidance

Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process. The following steps should be considered:

a) The access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified;

b) Privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (11.1.1), i.e., the minimum requirement for their functional role only when needed;

c) An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete;

d) The development and use of system routines should be promoted to avoid the need to grant privileges to users;

e) The development and use of programs which avoid the need to run with privileges should be promoted;

f) Privileges should be assigned to a different user ID from those used for normal business use.

Recommendations

PowerTech recommends that you conduct a regular review of the power of user profiles on your system. Run regular audit reports using comprehensive audit software, such as PowerTech Compliance Monitor, to verify that profiles with special authorities and profiles with direct access to production data actually need this access as part of their job function. Emergency access to fix production data is not an adequate reason for IT staff to have continuous access to power. Best practices, as defined by the standards and regulations, clearly indicate that programmers, operators, and development staff should not have special authorities assigned to the profiles that they use for normal business use. When they require special privileges to make emergency fixes to production data, they should do this with temporary access to a profile that is specifically created for this purpose. All actions using the temporary, powerful profile should be fully audited in secure audit journals, and management should pre-approve any access to such powerful profiles in advance of emergencies.

Today there is a product that you can use to simplify the management of powerful profiles on your Power Systems servers: PowerTech Authority Broker.

PowerTech Authority Broker enables system administrators to reduce the number of profiles with special authorities on their systems without disrupting business production. Users can temporarily “switch” into a powerful profile when they need the higher authorities, and all of their actions are fully audited. Managers can get complete reports of all activity when one of their staff members switches to the powerful profile.

PowerTech Authority Broker is also an excellent supplement to the security required for tools such as Query/400, DFU, DBU, and SQL. In addition, you can use Authority Broker to give end users less authority than they normally have, to make it safer to supply them with query tools.

Authority Broker:

- Allows access to powerful user profiles on an as-needed basis, so administrators can drastically cut back on the number of users with special authorities.
- Logs all activity while individuals are using the powerful profiles into secure audit journals, which cannot be modified.
- Lets you adjust the level of details in the audit reports to suit the audience.
- Sends alerts to interested parties, such as the managers of the user switching or anyone who is concerned with the integrity of specific data.
- Can be called directly from the command line or from programs for additional application security.
- Allows multiple alert methods when a profile swap occurs, including user-configurable options to insert customized alerts.
- Allows date and time restrictions, weekly schedules, and holiday overrides.
- Allows you to delegate swap approvals to the help desk or other personnel using the patent pending FireCall feature.

There are many aspects to your business that you cannot control, but IBM i security is not one of them. By following the tips and techniques described in this white paper, you can keep your system safe, and prove your compliance with regulations to your auditors.

To learn more about PowerTech Compliance Monitor and Authority Broker and how they can help you manage the powerful special authorities on your system, visit **www.powertech.com** or call **1-800-915-7700** and ask to speak with a Security Expert.

References:

ISO copyright office. ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security management. Switzerland: ISO copyright office. 2005.

IT Governance Institute. Cobit 4.1. Rolling Meadows: IT Governance Institute, 2007.