PowerTech
your security expert

WHITE PAPER

Best Practices for Audit and Compliance Reporting for Power Systems Running IBM i

By Robin Tatam

ABSTRACT:

Compliance with regulations such as Sarbanes-Oxley, PCI, HIPAA, and GLBA requires regular audit reporting against critical information technology (IT) assets.

This white paper outlines the key items that need to be reviewed on Power Systems running IBM i for both configuration data and transactional log information from the audit journal.

Sarbanes-Oxley, HIPAA, PCI, and GLBA have placed increased emphasis on the need to adequately secure critical data stored in IT systems. Organizations around the world are implementing a tighter set of controls over the configuration and use of their critical business applications and servers. Many companies have adopted frameworks like ISO17799 (27002) and COBIT to guide the definition and implementation of their security policies. For public companies in the United States, Sarbanes-Oxley section 404 requires management to attest to the validity of their financial results on a quarterly basis. To support this requirement, IT groups are running audit reports against their critical financial systems quarterly or even more frequently.

Power Systems™ running IBM i house business-critical data in organizations across a wide range of industries including retail, banking, manufacturing, and distribution. Today, more than 16,000 banks run core banking and financial applications on IBM i. Some of the better-known software vendors that provide applications for IBM i are: Oracle (JD Edwards ERP); Lawson/ Intentia (Financials); Jack Henry (Core Banking); SSA (BPICS, MAPICS, Infinium, Infor ERP applications); and Manhattan Associates (Supply Chain). Given the mission critical data kept on the system, it is essential to keep a close eye on the system with a rigorous audit reporting program.

The PowerTech Group, Inc.
www.powertech.com • info@powertech.com

TEL USA: 253-872-7788
TOLL FREE: +1 800-915-7700
TEL UK: +44 (0)870 120 3148

Defining a security policy is the first step in any compliance program, but once defined the policy cannot be left to gather dust on the top shelf. It must be implemented for all critical components of IT infrastructure, including Power Systems running IBM i. A system should not only be configured securely—auditors also demand that you demonstrate on a regular basis that the system stays in compliance. Regular audit reports that compare system configuration to policy are essential. Many regulations also call for specific review of log data. The Payment Card Industry Data Security Standard (PCI DSS), for example, specifically requires that logs from critical system components should be reviewed daily and kept online for three months.

It is essential that any audit program for IBM i cover both configuration data and log file analysis. On IBM i, configuration data primarily consists of information on system values, user profiles, and object authorities. Transaction activity is recorded in a secure (but difficult to interpret) journal called the security audit journal (QAUDJRN). This white paper discusses the challenges of auditing and reporting on IBM i today; outlines the various audit items that should be reviewed on a regular basis for IBM i; and explains why PowerTech is preferable to a solution developed in-house.

Build vs. Buy

Auditors may question the reliability of reports that are generated by in-house programming staff. Can IT staff be trusted to write programs and queries that produce reports on their own activity? Auditors demand independent verification. The optimal audit reporting solution for IBM i is robust commercial software that has been:

- Developed by experts focused exclusively on issues and exposures specific to IBM i
- Subjected to rigorous quality assurance testing
- Locked down by rigorous change control procedures
- Proven by successful implementation at hundreds of sites around the world
- Kept current with all the latest operating systems updates and new releases

Audit and reporting tools can result in significant cost savings compared to solutions developed in-house.

System Values

Given that there are hundreds of system values in IBM i, reviewing them is often a bewildering and time-consuming ordeal. They are configuration variables similar to environment variables on Unix or Windows. They can be split into two categories:

- Security settings, including items for password configuration, audit controls, save, and restore settings.
- Operational values that control configuration aspects of the system like performance tuning, power settings, regional, and time controls for the system.

Some system values control relatively insignificant settings, but others control fundamental properties of the systems. QSECURITY, for example, sets the overall system security level. IBM has stated that any value of QSECURITY less than 40 is not secure. Table 1 shows some of the more important security system values in IBM i. While it is not a complete list, it highlights some of the more critical security values.

IBM recommends changing default settings to configure a system securely. PowerTech provides an open source policy that recommends appropriate settings. All system values need to be checked on a regular basis to ensure that they comply with corporate policy. Administrators should investigate any exceptions to the policy and correct the value; alternatively they should prepare a statement for auditors documenting the reasons for accepting the risk.

PowerTech Compliance Monitor can greatly simplify reviewing system values by consolidating system values reports into a single report. Values from different systems can be shown side-by-side to make comparisons easier. Reports can show all values or just exceptions to policy. The product ships with a default policy, which represents the best practices defined in the open source policy. Users can easily edit this policy to match their specific corporate policy and can even establish different policies for different systems.

TABLE 1: SELECTED IBM i SECURITY SYSTEM VALUES

System Value	Description	Policy Recommendation
QSECURITY	System Security Level	**40 or 50**
QINACTITV	Time-out period for inactive jobs	**30** (= 30 minutes)
QMAXSIGN	Number of unsuccessful login attempts allowed for this account	**5**
QCRTAUT	Create default Public Authority	***USE,** then control at Library Level
QALWOBJRST	Allow restore of security-sensitive objects	***ALWPGMADP** or ***ALWPTF** when necessary
QPWDEXPITV	Number of days before a user must change a password	**90** (= 90 days)
QPWDMINLEN	Minimum password length	**6** (= 6 character minimum)
QPWDRQDDIF	Whether duplicate passwords are allowed	**5** (= must be different than last 10 passwords)
QAUDCTL	Auditing control	***AUDLVL, *OBJAUD, *NOQTEMP**
QAUDLVL QAUDLVL2	Security auditing level	See recommendations in Table 2 for auditing
QAUDENDACN	Auditing end act	***NOTIFY** - Send a message if auditing is ended
QCRTOBJAUD	Auditing of new objects	Required: Blank and Allow: *All
QAUTOCFG	Automatic configuration	**0** (= Disabled)
QAUTORMT	Auto-configure remote controllers	**0** (= Disabled)
QRMTSIGN	Remote sign-on control	**Not *SAMEPRF**

User Profiles

There are over 50 attributes or parameters that define a user identity in an IBM i user profile. Special authorities, limited command line capabilities, and initial menu/initial program are some of the more common parameters that are assigned to profiles. The way a profile is configured determines the level of access an individual will have to critical data. Sarbanes-Oxley compliance requires rigorous controls over the creation, deletion, and maintenance of user accounts. User profiles should be reviewed on a regular basis for the following cases:

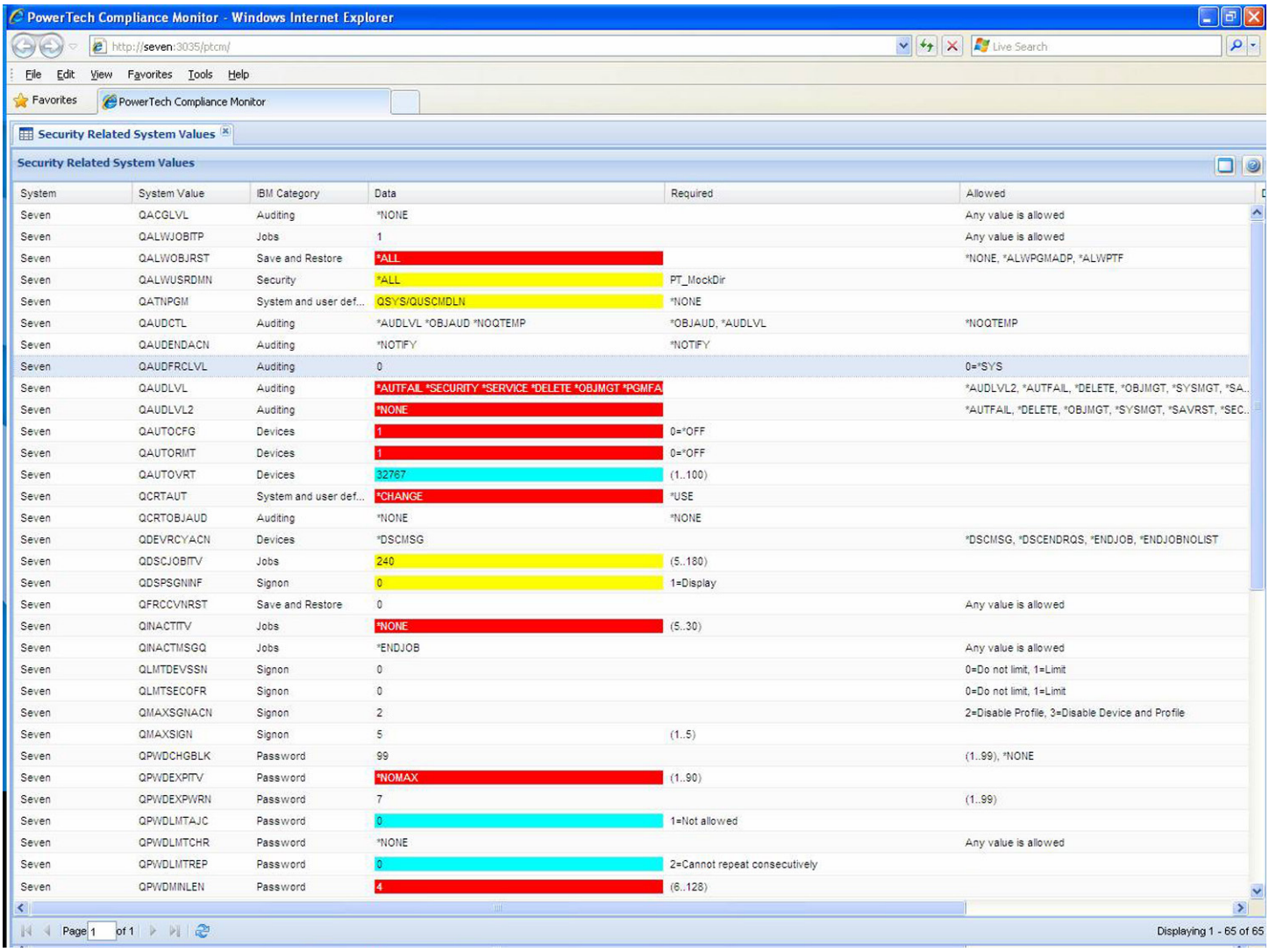
- Users with special authorities
- Users with command line access
- Dormant or inactive profiles that have not been used in the last 60 days
- Profiles with default passwords (same as username)
- Users with non-standard password settings or weak passwords
- Users with suspiciously high numbers of invalid sign-on (login) attempts
- Initial menu and program

Many companies check their profile information by simply sending output from the display user profile (DSPUSRPRF) command to a database file, but this is inadequate for many reasons.

- Profiles with a default password are a common exposure on IBM i. This information is not included in the DSPUSRPRF display and it needs to be checked separately.
- The inactivity information that is displayed with the DSPUSRPRF command may be deceptive since it only tells you the last time that the profile was used to sign on through an interactive telnet session. It does not show if the profile was used recently to sign on through a network interface such as FTP.
- The DSPUSRPRF command may be misleading when it shows special authorities because it does not indicate if the profile will inherit authority from group membership. Special authorities like *ALLOBJ provide a powerful set of administrator capabilities on the system. It is vital to check on a regular basis that these are only applied to those profiles that really need them. Programmers should not have special authorities in everyday profiles on production systems. It is not enough to check the profile using DSPUSRPRF—you also need to check each group the user belongs to. This can be a tedious and laborious process when done manually.
- Other information that needs to be checked includes when the profile was created and who created it. This is found elsewhere in the specific object authority information and is not obtained using the DSPUSRPRF command.

PowerTech Compliance Monitor gathers all necessary user profile information from different areas of the OS from multiple systems and makes them available in a single report. It indicates if the profile has inherited any authorities from group membership. There are over 15 predefined reports on user profiles, but users can easily customize and create their own reports by making their own filters or adjusting the columns and fields. Users can also filter out and exclude those profiles that are acceptable according to policy (IBM system user profiles, for example). Graphical scorecards provide a quick management-level view of whether the system is in compliance or not.

FIGURE 1: SYSTEM VALUES REPORT SHOWING EXCEPTIONS TO THE CUSTOMIZABLE POLICY



System	System Value	IBM Category	Data	Required	Allowed
Seven	QACGLVL	Auditing	*NONE		Any value is allowed
Seven	QALWJOBITP	Jobs	1		Any value is allowed
Seven	QALWOBJRST	Save and Restore	*ALL		*NONE, *ALWPGMADP, *ALWPTF
Seven	QALWUSRDMN	Security	*ALL	PT_MockDir	
Seven	QATNPGM	System and user def...	QSYS/QUSCMDLN	*NONE	
Seven	QAUDCTL	Auditing	*AUDLVL *OBJAUD *NOQTEMP	*OBJAUD, *AUDLVL	*NOQTEMP
Seven	QAUDENDACN	Auditing	*NOTIFY	*NOTIFY	
Seven	QAUDFRCLVL	Auditing	0		0=*SYS
Seven	QAUDLVL	Auditing	*AUTFAIL *SECURITY *SERVICE *DELETE *OBJMGT *PGMFA		*AUDLVL2, *AUTFAIL, *DELETE, *OBJMGT, *SYSMGT, *SA..
Seven	QAUDLVL2	Auditing	*NONE		*AUTFAIL, *DELETE, *OBJMGT, *SYSMGT, *SAVRST, *SEC..
Seven	QAUTOCFG	Devices	1	0=*OFF	
Seven	QAUTORMT	Devices	1	0=*OFF	
Seven	QAUTOVRT	Devices	32767	(1..100)	
Seven	QCRTAUT	System and user def...	*CHANGE	*USE	
Seven	QCRTOBJAUD	Auditing	*NONE	*NONE	
Seven	QDEVRCYACN	Devices	*DSCMSG		*DSCMSG, *DSCENDRQS, *ENDJOB, *ENDJOBNOLIST
Seven	QDSCJOBITV	Jobs	240	(5..180)	
Seven	QDSPSGNINF	Signon	0	1=Display	
Seven	QFRCCVNRST	Save and Restore	0		Any value is allowed
Seven	QINACTITV	Jobs	*NONE	(5..30)	
Seven	QINACTMSGQ	Jobs	*ENDJOB		Any value is allowed
Seven	QLMTDEVSSN	Signon	0		0=Do not limit, 1=Limit
Seven	QLMTSECOFR	Signon	0		0=Do not limit, 1=Limit
Seven	QMAXSGNACN	Signon	2		2=Disable Profile, 3=Disable Device and Profile
Seven	QMAXSIGN	Signon	5	(1..5)	
Seven	QPWDCHGBLK	Password	99		(1..99), *NONE
Seven	QPWDEXPITV	Password	*NOMAX	(1..90)	
Seven	QPWDEXPWRN	Password	7		(1..99)
Seven	QPWDLMTAJC	Password	0	1=Not allowed	
Seven	QPWDLMTCHR	Password	*NONE		Any value is allowed
Seven	QPWDLMTREP	Password	0	2=Cannot repeat consecutively	
Seven	QPWDMINLEN	Password	4	(6..128)	

Log Files

One of the powerful features of IBM i is the ability to log and record many events to a secure audit journal. This journal, QAUDJRN, is tamper-proof: Once an event is logged to the journal, it cannot be changed. Yet many people do not use the capability because they are not sure how to configure it to selectively gather events of importance. Auditing can be configured by event type, object, and user profile. The audit journal can consume enormous quantities of disk space and the data logged is difficult to read and interpret.

There are over 70 different types of security events and transactions that the operating system can record to the journal. Many vendors, including PowerTech, have also leveraged the secure nature of the audit journal to log and record their own transactions.

Some of the more common activity that can be gleaned from QAUDJRN include:

- Invalid login (sign-on) attempts
- Command usage by specific users
- Creation, movement, restoration, and deletion of objects
- Changes to system values and user profiles
- Authority failures
- FTP and ODBC network transaction details
- Profile swapping

Three steps are required to start security auditing on IBM i:

1. Start Security Auditing using the change security auditing (CHGSECAUD) command. Configure auditing for the most important values (QAUDLVL). Table 2 provides a recommended set.

2. Start auditing sensitive and critical files using the change object auditing (CHGOBJAUD) command.

3. Start auditing for powerful or privileged users using the change user auditing (CHGUSRAUD) command.

The PowerTech white paper "Security Auditing In The Real World" provides a detailed guide to configuring and adjusting audit controls on IBM i; and explains appropriate settings for these parameters. Table 2 indicates the QAUDLVL values used to audit some common event types.

Figure 2 (on the next page) shows an example of an event as it appears when the journal is viewed directly using the native IBM i commands. Sometimes there can even be binary data in an event that requires an API to read the full details. Even if you can figure out the right parameters in the DSPJRN command to view events of interest, it's quite difficult to read and understand the events that are displayed.

TABLE 2: RECOMMENDED AUDIT LEVEL SETTINGS (QAUDLVL)

Auditing Options	Description
***AUTFAIL**	Records failed sign-on attempts and unauthorized attempts to access files and other objects
***SECURITY**	Records many security-sensitive operations such as system value changes, QSECOFR DST password resets, and changes to Object authority and ownership
***SERVICE**	Records the use of System Service Tools (STRSST) and Dedicated Service Tools (DST)
***SYSMGT**	Log changes to certain system management areas
***SAVRST**	Log restore actions to security sensitive objects
***DELETE**	Records the deletion of any object
***OBJMGT**	Records object move and rename operations (you need this only on a production box)
***PGMFAIL**	Records programs that run restricted MI instructions or access internal OS/400 structures through unsupported interfaces—required information if you're moving to system security level 40 from a lower level

FIGURE 2: AN AUDIT TRAIL ENTRY VIEWED DIRECTLY IN IBM i

Any effective audit and reporting solution for IBM i should parse and explain each event to make it easier to filter and find critical activity. It should be possible to drill down into the details and easily identify activity by privileged user profiles or activity that affects the most sensitive database files.

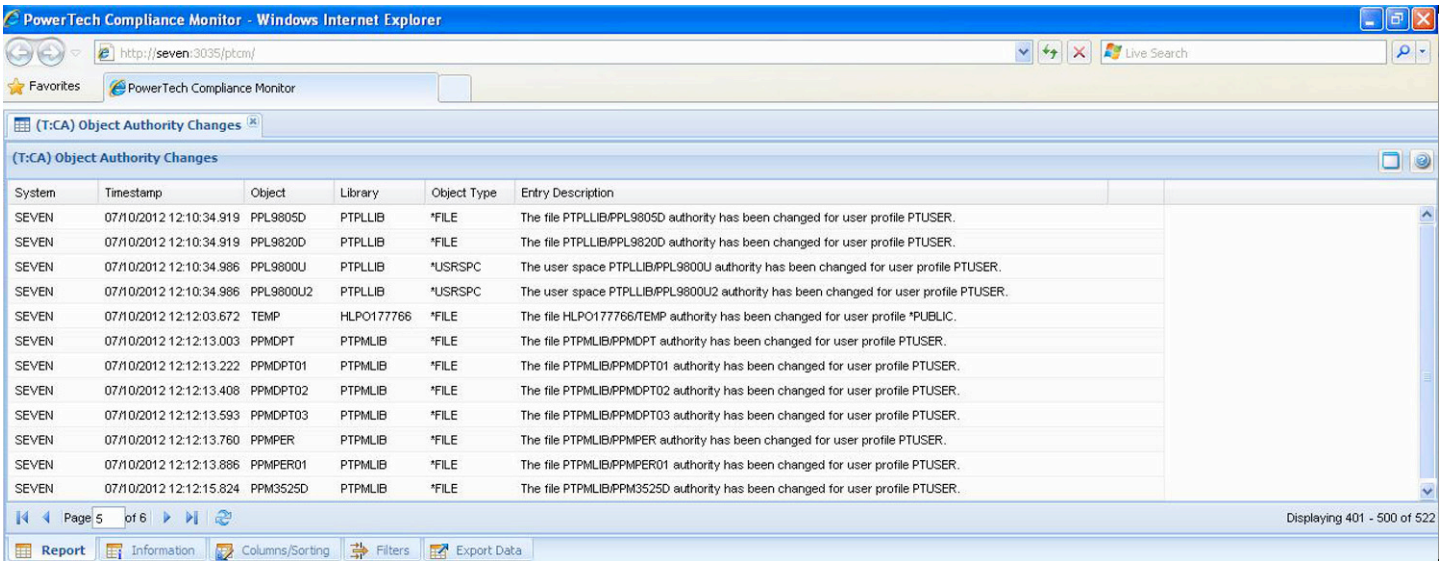
PowerTech Compliance Monitor parses complete event details for all 74 security-related (Type T) events that the operating system writes to the audit journal. Users can quickly search and sort logs of object activity by the affected object.

PowerTech Compliance Monitor makes it easy to answer questions like:

- Which files in critical libraries have been changed, and who changed them?
- What commands did privileged users run from the command line yesterday?
- Which user profiles were changed, and who changed them?
- How many sign-on (login) failures have there been?

Figure 3 (on the next page) shows the same audit event in Figure 2 reported with PowerTech Compliance Monitor.

FIGURE 3: AUDIT TRAIL ENTRY VIEWED IN COMPLIANCE MONITOR



PowerTech Compliance Monitor also parses and combines the complex entries from IBM i audit journals to provide a simple message that explains the event. For example:

- "System Value QPWDMINLEN was changed from 6 to 5"
- "An invalid password was entered for user profile JOHN"
- "An SQL Server transaction was allowed for user QSECOFR"
- "An object change occurred against library QSYS/PTNSLIB"
- "The user profile TOML has been changed using the CHGUSRPRF command"

Saving Disk Space

The audit journal can consume over five gigabytes (GB) of disk space on production systems each day. Often, users of High Availability software are required to log all object-related transactions. Many of these events may not be relevant for security issues, but the operating system records everything in the same journal. Often, due to the size of the journal, companies can only afford to keep one to two weeks of data online before saving copies to tape. This is a problem for complying with PCI since it requires that logs be kept online for three months. PowerTech Compliance Monitor copies the security audit journal events to a central server where they are compressed by as much as 95%. The high compression rate enables the storage of many more months of data online. Compliance Monitor also provides additional filtering of events before they are passed from the endpoint systems back to the central consolidation server. This feature also helps to cut down the amount of disk space that is consumed by the log data.

Integration with Security Information Management (SIM) Solutions

As companies broaden their focus from perimeter security to insider threats and regulatory compliance, a new category of security application, Security Information Management (SIM), has emerged. Companies like ArcSight, OpenService, Symantec, LogRhythm, and Novell have created powerful applications that gather security events from many sources and correlate and aggregate the events to produce a single, real-time view of security issues. Given that IBM i runs business critical applications, it needs to be monitored as diligently as any other

platform, and its logs should also be integrated in real time with SIM solutions. Typically, security operators that monitor SIM systems are not usually proficient in IBM i terminology, so it is important that any SIM solution parse the event into an easily understood format.

Another PowerTech product, Interact™, reads the same events from the audit journal as Compliance Monitor and exports them to syslog. Originally a Unix standard, syslog is now used by a wide variety of devices and applications. Most SIM systems can read syslog data and are often used to provide a central aggregation of log data from many different sources. Interact provides the additional benefit of being able to filter events by user, IP address, day, and time before sending events to the syslog server. Administrators can apply even more fine-grained server controls than those available with the operating system's audit settings, thus reducing the volume of information sent to the remote console.

Network Configuration and Monitoring

Over the years, IBM has extended the power of IBM i by adding tools that allow IBM i data to be accessed from other platforms, including PCs. Well-known services such as FTP, ODBC, JDBC, and DDM are active and ready to serve up data across the network as soon as the machine is powered on. Any user that has a profile on the system and authority to the objects has the means to access critical corporate data. IBM has provided a means to mitigate this exposure by creating "exit points" at the network services. An 'exit program' that is attached (registered) to the exit point can be used to monitor and control access through that service.

Users can download or otherwise manipulate data only if they have the required authority to the objects; however, studies have shown that object level authority is poorly implemented on most systems. An effective audit program for IBM i should check the status of the common network services to see if there are exit programs registered to monitor and control traffic.

PowerTech Compliance Monitor provides the ability to report on network configuration parameters and whether there are registered exit programs. But that is only half the battle. Administrators also need to be able to monitor the traffic through the exit programs. When PowerTech Network Security™ exit programs are used, Compliance Monitor can report on all of the detailed transactions through the servers that are logged to the audit journal.

Object Authority

One of the benefits of IBM i is integration of the database with the operating system. This helps to greatly simplify the management of the system. But there are security implications: Every user that has a profile with access to the OS also gets access to database files.

The files themselves can be secured by the use of specific object authorities:

- *ALL (the rights to read, change, and delete all the data; all rights to the object itself)
- *CHANGE (the rights to read the data)
- *USE (the rights to read, change and delete the data)
- *EXCLUDE (no rights to the data or to the object)

According to the most recent *State of IBM i Security Study*, most authorities have not been securely configured. Everyone (*PUBLIC) often has full change access to every object on the system. The default value for newly created objects in the operating system is that everyone (*PUBLIC) should receive change (*CHANGE) access. It is alarming that administrators often do not find the time to change their application defaults and implement effective object authority schemes.

PowerTech Compliance Monitor provides the capability to check the object authority scheme for production libraries. Access should be restricted to only those users that have a demonstrated need. Public access should be set at *EXCLUDE and individual access should be granted only where there is an appropriate business need.

Conclusion

A comprehensive audit tool for IBM i needs to cover many different areas:

- System Values
- User Profiles
- Log File Data
- Network Configuration and Transactions
- Object Authorities

PowerTech Compliance Monitor provides all of these in an intuitive browser-based interface. An interactive grid view makes it easy to manipulate and drill down into the details of the data on the fly. Reports can be saved in PDF format or exported to Microsoft Excel and CSV. A distinguishing strength of Compliance Monitor is its ability to customize and save modified report definitions for a specific environment.

Powerful batch reporting functionality enables reports to be run during off-peak hours, with assessment results distributed via secure email, or deposited into the IFS for mobile device access or sharing.

Compliance Monitor includes a recommended set of audit reports for compliance with Sarbanes-Oxley, PCI, and MICS (for the gaming industry). Throughout the product there are links to a compliance guide that cross-refers IBM i concepts to regulations and standards.

About the Author

Robin Tatam is the Director of Security Technologies for PowerTech, a leading provider of security solutions for IBM i servers. A frequent speaker on security topics, he is co-author of the IBM RedBook "System i® Security: Protecting i5/OS Data with Encryption." *Robin can be reached by email at robin.tatam@powertech.com.*