PowerTech®
your security expert

WHITE PAPER

Auditing Power Systems Servers:

An overview of auditing an IBM Power Systems™ server running IBM i, using PowerTech Compliance Assessment

by Robin Tatam

Executive Summary

Few words strike fear in the heart of a senior executive like *security* and *compliance*. The burden to satisfy stringent audit requirements has become a leading initiative for companies of every size, in every industry. This will continue to grow as the world's governments scramble to enact legislation to address the protection of sensitive information.

The 2001 terrorist attacks in the U.S. focused the spotlight on the flow of electronic information, and the international disruption that can result when the flow is interrupted. And, while hackers used to be satisfied by simply wreaking havoc, the professionals quickly learned that there was little financial gain to be made from that. Today, stealthy activities often are geared toward the theft and resale of some form of valuable information.

Disclaimer:

The information provided in this document is for informational purposes only. This paper is not meant as compliance advice. Prior to taking any steps that may affect your compliance status with any government mandates, always seek advice from your compliance auditor and/or legal counsel.

The Ponemon Institute conducts independent research on privacy, data protection, and information security policy. Through their research they have documented many startling statistics, including:

- There have been 200+ million records breached since 2005
- 65% of the cost of a breach is due to lost business
- 12,000 laptop computers are lost in airports each week; only 30% are recovered

While many corporate IT initiatives are scaled back during an economic crisis, this is a time when the threat of an attack increases—especially from inside sources. Workers who are fearful of losing their jobs are more likely to leak information at a time when resources to monitor employee activities are stretched to the limit. It is imperative that all employees cooperate against the threat of unauthorized activities. For security initiatives to have any chance of being successful, they must include sponsorship from the executive team. After all, it is the executives who are now seen as the responsible party.

Performing an Audit

A common mistake made by companies trying to “get compliant” is to begin remediation activities before having a clear plan on what items need to be addressed. In fact, changes made in one area of the operating system can impact the compliance of another area, so it is also necessary to define the order in which vulnerabilities are addressed.

Documenting the current configuration of the server should always be the first step of any IBM i security initiative. Once you know the current configuration, compare it to the goals set forth by the regulation, legislation, or framework that you need to comply with. Even if the objective is simply to secure a system, rather than obtain formal compliance, a security policy acts as an internal marker to gauge progress and success.

If your organization has never performed an audit, you have several options to help you identify vulnerabilities, and associated remediation tasks:

1) Formal Independent Assessment

A formal assessment is a deep-dive review of the entire IBM i infrastructure, performed by (preferably) an organization that is experienced in assessing IBM i security. Typically, this can take up to 5 days and provides deep analysis into numerous different areas of the security configuration, along with recommendations for remediation. The benefit of this type of professional service is the presentation of independent results, and access to an auditor who is familiar with common vulnerabilities and can help educate your team.

2) Self-Performed Audit

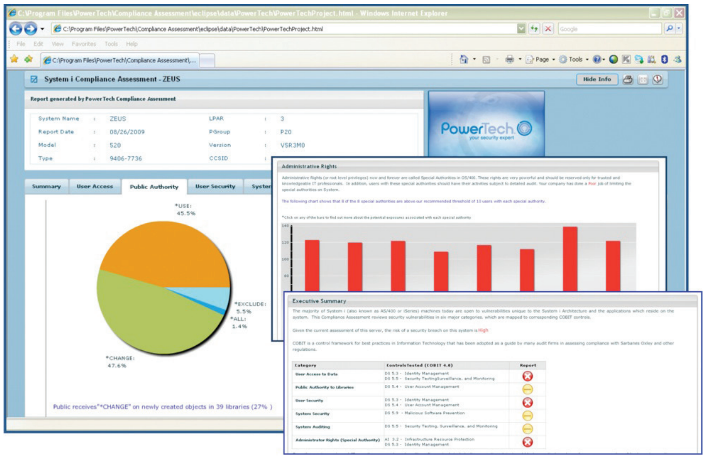
Although self-auditing is not considered a best-practice, performing an assessment of your own environment is usually far less costly than a formal assessment conducted by an outside organization. If your company is fortunate enough to possess the skills necessary to perform this type of assessment in-house, it might be a good option to get you started. You should develop a security policy to supplement the best-practice recommendations you can obtain from various online sources.

3) Automated Assessment

Although not as detailed as a formal audit, an automated assessment can rapidly assess the current state of security on the server. While a tool can measure configuration elements, it’s important that someone can interpret the findings correctly to ensure that they don’t over- or under-assess the vulnerabilities. One advantage of a tool-based approach is that you can use it as a precursor to a formal audit—using it to justify the deeper, more costly audit.

Introducing PowerTech Compliance Assessment

PowerTech’s professional services team performs IBM i assessments for customers of all sizes, and has used that experience to develop a fully automated solution that reviews six important categories of security configuration. The audit usually takes less than 15 minutes to complete, and returns the results in an easy-to-read, browser-based application. A great benefit of this solution is that it is available without cost or obligation; PowerTech even provides an IBM i Security Specialist to help you interpret the results.


C:\Program Files\PowerTech\Compliance Assessment\eclipse\data\PowerTech\PowerTechProject.html - Windows Internet Explorer
C:\Program Files\PowerTech\Compliance Assessment\eclipse\data\PowerTech\PowerTechProject.html
Google
File
Edit
View
Favorites
Tools
Help
C:\Program Files\PowerTech\Compliance Assessment\...
Page
Tools
Hide Info
PowerTech
your security expert
Summary
User Access
Public Authority
User Security
Systen
*USE:
45.5%
*EXCLUDE:
5.5%
*ALL:
1.4%
*CHANGE:
47.6%
140
120
100
80

System i Compliance Assessment - ZEUS

Report generated by PowerTech Compliance Assessment

System Name	ZEUS	LPAR	3
Report Date	08/26/2009	PGroup	P20
Model	520	Version	V5R3M0
Type	9406-7736	CCSID	

Public receives"*CHANGE" on newly created objects in 39 libraries (27%)

Administrative Rights

Administrative Rights (or root level privileges) now and forever are called Special Authorities in OS/400. 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 detailed audit. Your company has done a Poor job of limiting the special authorities on System.

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

*Click on any of the bars to find out more about the potential exposures associated with each special authority

Executive Summary

The majority of System i (also known as AS/400 or iSeries) machines today are open to vulnerabilities unique to the System i Architecture and the applications which reside on the system. This Compliance Assessment reviews security vulnerabilities in six major categories, which are mapped to corresponding COBIT controls.

Given the current assessment of this server, the risk of a security breach on this system is High

COBIT is a control framework for best practices in Information Technology that has been adopted as a guide by many audit firms in assessing compliance with Sarbanes Oxley and other regulations.

Category	ControlsTested (COBIT 4.0)	Report
User Access to Data	DS 5.3 - Identity Management DS 5.5 - Security TestingSurveillance, 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	☒

PowerTech Compliance Assessment

The PowerTech Compliance Assessment is a Microsoft Windows application that can assess an IBM i server connected to the network. While there are a few simple prerequisites (a list is supplied), they are common requirements that are easily met. The goal was to make the assessment process simple, fast, and non-invasive. You can perform the audit during normal business activities; it doesn't add measurable workload to the server and leaves no permanent footprint on the server.

Performing the Assessment

To get started, request a Compliance Assessment from the PowerTech Web site (www.powertech.com). A PowerTech representative will contact you to schedule your Assessment. You'll also receive an overview of the Assessment process that explains any requirements. The Compliance Assessment is conducted via WebEx with a PowerTech Security Specialist.

Interpreting the Assessment Findings

A knowledgeable PowerTech Security Specialist helps you interpret the Assessment findings. Each of the assessed categories has a related tab that provides background details. The Assessment is typically reviewed in the following order:

Executive Summary

The executive summary page provides a simple ranking of the overall condition of the server. The summary presents the six areas of review using red, yellow, and green indicators to show the state of compliance against best-practices, along with a reference to the appropriate COBIT framework section to which they apply.

Administrative Rights

One of the biggest areas of influence on the vulnerability of application data, as well as server functions, is determined by the administrative capabilities of the users who sign on. Administrative rights, assigned via eight separate special authorities, are often specified without sufficient consideration if there's a proven business need. The PowerTech Security Specialist reviews the capabilities—and vulnerabilities—that are associated with each of the following special authorities:

- All Object (*ALLOBJ)
- Security Administrator (*SECADM)
- I/O System Configuration (*IOSYSCFG)
- Audit (*AUDIT)
- Service (*SERVICE)
- Spool control (*SPLCTL)
- Job Control (*JOBCTL)
- Save System (*SAVSYS)

Even when users have a legitimate need for one or more special authorities, it's preferable not to assign those authorities without accountability. This ensures that powerful users aren't able to circumvent the security policy and procedures. Recommended mechanisms for accomplishing this accountability include auditing command use, as well as using application programs that adopt authority to perform specific functions like resetting passwords. A more robust approach is to use profile switching technology, as found in PowerTech's award-winning Authority Broker software.

Public Authority

Unlike virtually any other server, IBM i contains an integrated database, as well as a built-in security infrastructure. While this infrastructure is available, it is not implemented by default. This area of review measures the level of public access assigned to the libraries on the system. The public is defined as any user with a profile and password, and is a good indicator of how easy it would be circumvent legacy menu and application security mechanisms.

User Access

Once the Assessment provides a picture of the capabilities of the users and public openness of the server libraries, it's easier to see if network access represents a significant vulnerability. If the security infrastructure depends on legacy controls—such as command line restrictions, menus, and application security—it's possible that users can simply circumvent those controls. Users easily can find inexpensive software online (or pre-installed on a desktop PC) that provides easy access to services such as FTP, ODBC, and remote commands.

These tools enable powerful access to the database and represent a fast conduit for data leaks. Many of them also do not provide any form of audit log—a clear violation of virtually every form of regulation.

Fortunately, you can easily control and audit this type of network traffic with the operating system's exit points, and a leading exit program solution like PowerTech's Network Security.

System Security

The server takes much of its configuration direction from system values. A category of system values specifies security settings, and this section of the Assessment analyzes a number of key values. Ensuring compliance to a standard, whether the standard is built on best-practices or your organization's own security policy, should be a standard part of ongoing audits.

User Security

A solid security infrastructure is only as strong as the user profiles and passwords used to control access. This category reviews the state of user profiles, including how many have not been used for a period of at least 30 days, how many have default passwords, as well as the basic password rules that control how secure those profiles are. The Assessment also reviews some lesser-known vulnerabilities, including profiles that can by used by other users to execute jobs and potentially gain unauthorized access.

System Auditing

IBM i includes extensive event auditing capabilities. You can capture events for system events, user activities, and object access. A special secure repository is configurable to store the event logs, and this will satisfy most audit requirements. Since you can perform forensics only on data that has been collected, it's important to understand if auditing currently is active. The Compliance Assessment checks for the existence of the security audit journal and documents the types of events currently being audited. The Assessment also tries to determine if you have a tool installed on your system that analyzes the log entries.

The Next Steps

Depending on vulnerabilities identified by the Compliance Assessment, the PowerTech Security Specialist can provide direction about applicable remediation steps. Recommendations typically include changes to the security controls in the operating system, as well as discussion and mentoring on the procedures that you should adopt for best-practice security. PowerTech also can work with your team to determine the need for an in-depth assessment, or help you evaluate applicable commercial security solutions.

Additional Reading

To read about how other organizations measure up, we recommend that you download our annual State of IBM i Security study. This white paper is a compilation of the anonymous Compliance Assessment data that is collected throughout the year, along with expert analysis of the statistics. To download the latest edition of this frequently quoted study, go to www.powertech.com.

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 was also co-author of the IBM RedBook "System i Security: Protecting i5/OS Data with Encryption." Robin can be reached by e-mail at robin.tatam@powertech.com*.*