Craig S. Mullins

Return to Home Page

April / May 2006

The Resource for Users of IBM zSeries & S/390 Systems

z/JOURNAL

zData Perspectives

by Craig S. Mullins

Regulatory Compliance and Data Governance

Almost four years ago now, President Bush signed into legislation the U.S. Public Accounting Reform and Investor Protection Act of 2002. More commonly known as the Sarbanes-Oxley Act, or SOX, the goal of this act is to regulate corporations in order to reduce fraud and conflicts of interest, to improve disclosure and financial reporting, and to strengthen confidence in public accounting.

SOX is the most significant government legislation affecting accounting and auditing in more than 70 years. Section 404 of this act, the one giving IT shops fits, specifies that the CFO must do more than simply vow that the company’s finances are accurate; he or she must guarantee the processes used to add up the numbers. Those processes are typically computer programs that access data in a database, and DBAs create and manage that data as well as many of those processes.

So SOX will bring visibility and additional rigor into DBA practices and procedures. One of the provisions of the Act states that financial data—whether live or at rest—must be hardened against unauthorized access, invalid transactions, or any other type of modification that invalidates the integrity of the financial reports. How stringent are the security controls on your databases? Do you have automated controls in place to scan databases for compliance and vulnerability exposures? Are practices in place to audit access to your data to report on any unusual activity? Are these controls in place for all your mainframe financial data whether it’s stored in DB2, IMS, VSAM, or flat files?

And how robust is your backup and recovery? SOX demands that your company’s financial data be completely recoverable in the event of a logical or physical failure— without loss of data that would invalidate the integrity of the financial reports. Do you have an enterprise backup and recovery policy you manage? Has backup and recovery been fully automated and tested? Can you demonstrate your ability to recover both locally and remotely in case of a disaster?

And how do you manage and track database change? SOX contains provisions for that, as well, stating that changes made to the data structures must be done using an authorized process. All impacts and deltas must be tracked and reported to ensure there are no unauthorized changes that could invalidate the financial reporting systems. Do you have a workflow and task approval process in place? And do you track all changes to data structures and catch those made outside the authorized change approval process? What about keeping track of the changes between releases to provide a complete summary of data structure changes for compliance reporting?

Furthermore, SOX specifies a five-year data retention period (beginning from the end of the fiscal period in which the audit or review was concluded) for your relevant financial data and work papers. Are you confident you can access all your five-year-old financial data? Is all the data there? If not, has it been archived or backed up in a format that can be accessed? And what do you do if the database schema has changed over those five years?

DBAs have had to deal with security and authorization, auditing, backup and recovery, and change management as long as databases have been used. But in many cases, these tasks were attacked in a low-cost, ad hoc manner. Maybe there wasn’t sufficient capital to expend on DBA processes; maybe the DBAs were capable enough to keep the databases up and running without the aid of tools. Such an approach is no longer sufficient.

DBMSes are being extended to provide additional capabilities for securing data, ensuring integrity, and making changes accurately with limited outages. But in most cases, to completely assure database operations are accurate, sustainable, and ongoing, robust third-party tools are required. For example, do you feel comfortable scanning database log records to produce database audit reports? Without a tool that understands log records and legibly formats the data, most DBAs will be unable to glean anything usable from the information-rich database transaction logs.

The Bottom Line

Now that executives have to vouch for the accuracy of your company’s data, it becomes more likely you can procure a budget for proper tools. When someone’s neck is on the line, tools that can help ensure data accuracy will suddenly be more important than they were just a little while ago. Imagine that …

From zJournal, Apr / May 2006
.

Home.