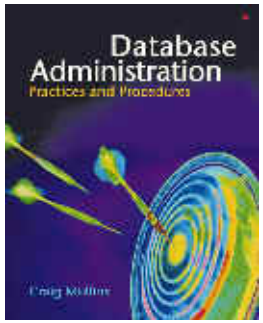
Craig S. Mullins

Return to Home Page

June 2005



The DBA Corner

by Craig S. Mullins

Sarbanes-Oxley Requires Rigor in Database Administration

On June 30, 2002, President Bush signed into legislation the U.S. Public Accounting Reform and Investor Protection Act of 2002, or as it is better known the Sarbanes-Oxley Act. 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.

The Sarbanes-Oxley Act is the most significant government legislation affecting accounting and auditing in more than 70 years. Section 404 of the Sarbanes-Oxley Act specifies that a CFO must do more than simply vow that the company's

finances are accurate; they have to 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 the Sarbanes-Oxley Act 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 which 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?

And how robust is your backup and recovery? You may have been operating for years with a backup plan that has never been tested. The Sarbanes-Oxley Act demands that your company's financial data must 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 to which 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? The Sarbanes-Oxley Act 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 are tracked and reported to ensure that 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 that are made outside of the authorized change approval process?

What about keeping track of the delta of changes between releases to provide complete summary of data structure changes for compliance reporting?

DBAs have had to deal with security and authorization, auditing change, 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 was not 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. This is no longer acceptable.

The Sarbanes-Oxley Act dictates that you must be able to restore or restart the processing in a manner such that it sustains operations and does not lose the integrity and completeness of financial transactions or data.

Today's modern DBMSs are being extended to provide additional capabilities for securing data, ensuring integrity, and making changes accurately with limited outages. For example, DB2 for Linux, Unix and Windows provides improved monitoring capabilities that make it easier to capture and store every SQL statement for posterity. Such new features are helpful, but probably insufficient to assure compliance with all of the strict regulatory requirements imposed by acts such as Sarbanes-Oxley. In most cases, to completely assure database operations are accurate, sustainable, and on-going, robust third party tools are required. For example, who among us feels comfortable scanning database log records to produce database audit reports? Without a tool that understands log records and formats the data legibly, most DBAs will be unable to glean anything usable from the information-rich logs that are already being produced by the DBMS.

The bottom line here is now that your CEO has to vouch for the accuracy of your company's data, it becomes more likely that you can procure a budget for DBA

tools. Now that someone has to stick his or her neck out to vouch for the company's data, tools that can help to assure data accuracy will suddenly be more important than they were just a little while ago. Imagine that…

From Database Trends and Applications, June 2005.

Home.