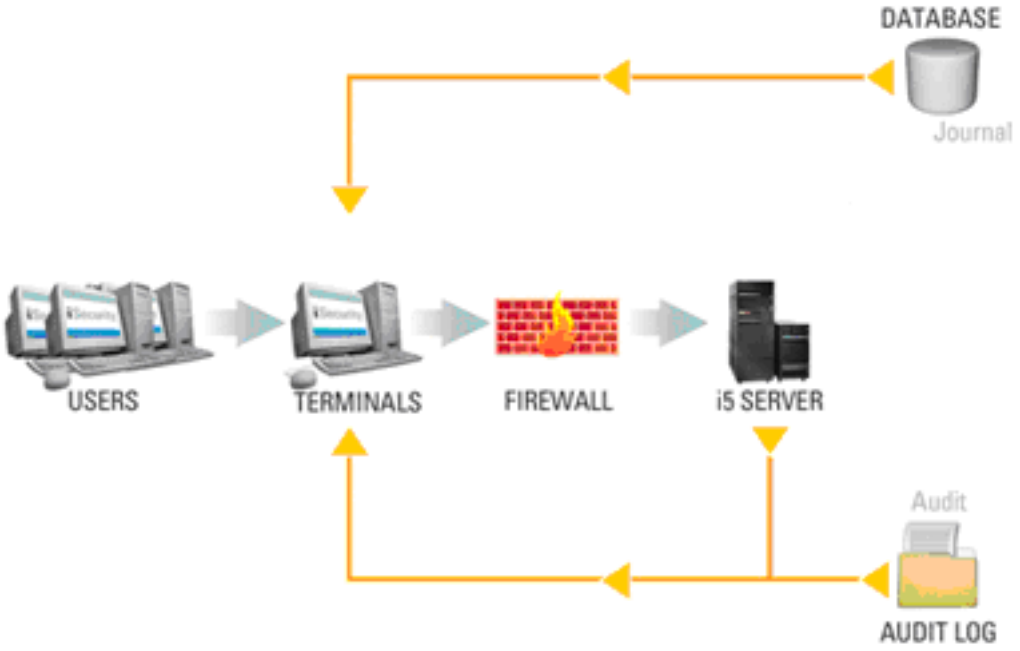
DBU AUDIT JOURNAL PLUG-IN WHITEPAPER

Even years after the US government enacted Sarbanes-Oxley, HIPPA and other regulations, companies continue to define and redefine business processes and functions that touch sensitive information within their organizations. The wave of corporate scandals that rocked the early millennium continues to cause waves years later. Companies scamper to prepare for external audits required to prove corporate compliance to all the Acts government regulations require.

While companies understand the reasons for creating these processes and controls, most do not realize the immense efforts and associated costs required to sustain the effort. Central policies and procedures have to be created and enhanced. Teams continuously assess company controls and assist with testing. Reports and documentation must be made readily available. Over and over these requirements are evaluated. While there is no silver bullet, technology can play a huge role to support ongoing compliance efforts.

Best practice software tools can greatly simplify the job of continuously providing SOX compliance. One such tool provided by ProData is DBU Audit. While it is a relatively simple tool, it's impact on tracking internal database changes can be just what most organizations need to report changes made to data via the database utility.

What follows is a summary of the capabilities already inherent to the IBM i with it's journaling capabilities as well as a summary of ProData's DBU Audit functionality. Once businesses identify their key processes and functions, they can determine how this technology can support ongoing compliance efforts and how to integrate compliance automation into daily IT activities. This makes compliance more cost-effective and less labor intensive.



The IBM i OS can provide an audit trail for your database by using local journal management to recover the changes to an object, as an audit trail or to help replicate an object. Journal management provides a means by which you can record the activity of objects on your system.

When you use journal management:

System i OS journal management can audit objects

* You create an object called a journal.
* The journal records the activities of the objects you specify in the form of journal entries.
* The journal writes the journal entries in another object called a journal receiver.

As the number of objects you are journaling increases:

Journals can impact system performance

* The general performance of the system can be slower.
* The time it takes to perform an IPL on your system can also increase, particularly if your system ends abnormally.
* The auxiliary storage necessary to store the journals, journal receivers and the associated entries increases.

The IBM i OS security journal is the industry standard for tracking the changes made to your database. The DBU Audit Journal employs the same concept of the OS journaling, however, there is only one file that the journal is built over. Additionally, the software is shipped with a menu system that allows for an easy-to-use reporting process.

DBU Audit accomplishes the following:

IBM i OS Security Journal is the industry standard

* Lessens the impact of system performance, system recovery and auxiliary storage usage, due to the single file journal aspect.
* Allows you to track changes, adds, deletes and even viewing (which is something the OS journaling cannot do) to any database file that is accessed using DBU software.
* Does not interfere with any current journaling strategies you have employed using the System i OS security journal.
* Allows for a reporting process that can be automated with minimal intervention and presented in a method that is easy to understand and complies with audit requirements.

The DBU Audit Journal uses the OS fundamentals of a journal and journal receivers and offers a secure environment to record the journal entries.

DBU Audit Journal uses the OS fundamentals of a journal

* Every journal entry is stored in a compressed format.
* The operating system must convert journal entries to an external form before you can see them.
* You cannot modify or access the journal entries directly. Not even the Security Officer profile can remove or change journal entries in a journal receiver.
* Only changes, adds, deletes or views (if specified) when using DBU are recorded to the DBU Audit Journal.
* These journal entries can be either displayed or printed and, through the use of our proprietary software the depiction of the entries, is displayed in a readable format rather than the somewhat cryptic OS method of displaying journal entries.

The DBU Audit Journal Plug-in offers menu-driven access to control the functionality. You access the menu by executing the command DBUAUDMN with the DBU software library in your library list.

DBU Audit offers menu driven access

* Option 1 allows you to start the journal.
* Option 2 ends the journal. Once the DBU Audit Journal has been started we would recommend not ending it unless your system strategy dictates the need.
* Option 3 allows you to see changes made to a specific file (you will need to input the file that was changed on the File parameter).
* Option 4 allows you to extract a file that will have the changes that were made using DBU (you can specify an individual file or use *ALL for the file name and specify a library or use *ALL/*ALL for file name and library name which will produce an extract file for each object that DBU was used on).
* Option 5 allows the extracted files to be viewed
* Option 6 allows you to work with the extracted files. You can delete extracted files individually using this option.
* Option 7 allows you to clear the audit library (designated when you use Option 1) of all extracted files.
* Option 8 allows you to specify a file or *ALL files in a library to record views of data when using DBU. (We would caution the use of this option; If a search is performed using DBU, all records searched will be included in the DBU Audit Journal entries.)
* Option 9 allows you to maintain the journal receivers. (During the creation of the journal, the receivers are specified to be maintained by the system.)
* Option 10 allows the extracted files to be printed.
* Option 11 allows you to view activity related to starting and stopping the DBU Audit Journal.

You can secure the DBUAUDMN command and the associated commands for each option using object level security. Complete information for the DBU Audit Journal Menu is described in our documentation for this plug-in that is available at our website www.prodatacomputer.com.

The process of reviewing the DBU Audit can be automated by building a CL program which executes the commands that appear to the right of each option. One such scenario might involve leaving the DBU Audit Journal active and then using the following execution from a CL program:

You can automate your reporting process with DBU Audit

* DBUCLRAUD (This will clear previously extracted files).

* DBUEXTAUD *ALL/*ALL (This will produce an extract file for all objects that DBU was used on from the *CURRENT journal receiver. Specifying *CURCHAIN will chain out to all available journal receivers on the system). You can also specify a date range to be used or a specific user profile.

* DBUPRTJRN OUTQ(YOURLIB/YOUROUTQ) (This will produce a printed report for each of the extracted files and output the results to the output queue you designate where YOURLIB/YOUROUTQ points to).

This CL program could then be used in a scheduled routine to produce reports daily, weekly or when your audit strategy dictates the need. Although this is a very simple tool, it provides ease and minimal effort to generate exactly what the auditors need to see for compliance requirements.

The use of DBU Audit can not only provide the tracking and reporting process necessary for compliance with SOX, HIPPA and other government regulatory stipulations but also makes good sense to be employed as a 'best practices' type of tool for companies that do not have requirements that are specifically stipulated.

Your company or organization's data could be the most important part of your computing environment therefore doesn't it just make good sense to guarantee the integrity of that data by being able to have a tool like the DBU Audit Journal Plug-in available?