Learning Lessons – Observations From Recent Audits

David Hayes

GAO - Washington, DC

Interesting Situations:

- Datasets controls for important JCL – and the rest of the story
- Read access equals copy access – then where does the data go?
- Applications with many access levels – and security software that defines only a few levels…
- Logging activity to mitigate the effect of powerful access privileges
- What is really shared?

What do you look at when checking controls for Started Tasks?

- We usually check how STCs are defined to the security software.
- We should be determining which libraries are in the PROCLIB concatenation and checking those dataset controls.
- Looking at the JES JCL in the execution queue for STCs associated with processes such as DB2 and CICS gives us a good way to find the actual DSNs for the active parmlibs and proclibs associated with those systems.
- If you actually looked at the code in the STC jobs, what might you find that effects controls?

When End Users Have Read Access to Data – They Make Copies

- Just because the data lives in a controlled environment may not result in business processing actual functioning in that controlled environment.

- Beware of spreadsheets and end user controlled databases.

When Applications Have Many Access Levels – Figure Out How They Work

- Applications can have more granular access controls than what is defined by the security software – so what do you check?
- Can access levels implemented in applications be circumvented at the command line level (TSO or CICS)?
  - Do users have DB2 access and TSO when their DB2 access privileges exceed what they can access through the application?

When the Primary Control is Based on SMF Logging…

- Sometimes the primary control in place is the logging of activity.
- Are detective controls reliable?
  - □ What is recorded in the logs?
  - □ Do questionable patterns continue for extended periods?
  - □ Is there evidence that actions are ever triggered by activity recorded in logs?

What is Really Shared?

- How do you know what is really shared?
- Are naming conventions the controls?
- How often does anyone really check on the boundaries between production and everything else?
- Does logging work to keep production separate from non-production?

Keep Your Eyes Open – Expect to Find a Few Surprises