FEATURE ARTICLE

Auditing Backup and Restore Procedures

By Mitchell Levine

Backup and recovery procedures always have been included as a review area in all types of IS audits. Typically, the infrastructure and data center groups are the target groups to be audited since the backup and restore processes are executed by these groups. In a client/server and web-based environment, the infrastructure group performs the backups. In the mainframe environment, the data center performs full volume backups which typically are performed weekly. Application development groups maintain the jobs that perform the application level backups which are tied to a synchronization point where the environment will be restored. This does not necessarily coincide with the data center initiated backups. This article is intended to redirect the audit focus on the user areas when reviewing the adequacy of the backup and recovery procedures.

The starting point to determine the adequacy of the backup is to identify the purpose of the backup. The obvious need for backups is to restore an environment in the event of a system failure. To determine the extent in which data can be lost, a risk assessment needs to be performed. This should include user participation, which would indicate the acceptable length of period in which data can be lost (e.g., one minute, one hour, one day). The answer to the question is based on the transaction volume, manual processes for capturing input which can be used to re-input the data and the ability for users who input data to be notified that the data were lost and need to be re-inputted.

Once the frequency of backups has been established, based on the maximum period in which data can be lost, the data need to be traced to the backup routines that perform the backups. These backup routines could be initiated by the application development groups or the infrastructure group. An audit compliance test needs to be performed based on a sample selection of critical files to determine whether they are included in the backup routines.

The second purpose of a backup is to provide users the ability to view the system from a previous point-in- time. This task is not necessarily accomplished based upon restoring the system from the backup files. Alternative approaches include the availability of a data warehouse in which extracts can be developed by users to retrieve historical data. A separate audit of the data warehouse would be needed to ensure that it meets the users' historical data requirements. Another alternative may include the storage of historical data which can be accessed directly from the production system. If this approach is used, then the compliance test would consist of the selection of a sample number of users to identify their historical data requirements and the determination of whether the data are available within the production system. It should be noted that the system being reviewed might not require historical data to be viewed by the user, which would render the various methods presented as not applicable.

Performing a back up of data is only half of the review. The other half of the review consists of the audit of the restore procedures. The first step is to determine whether there is an environment available to restore the data backups. The primary requirement is disk space, which will increase significantly if the restore approach does not consist of overlaying the current production environment. The infrastructure and data center group should have documented procedures for the various types of restores that will be performed—which can be at the file level or a volume level.

As part of auditing backup and restore procedures, a detailed audit approach is required to ensure that all of the system failure scenarios and historical data representations have been considered along with the capacity constraints when trying to restore an environment. ■

***Mitchell Levine** is the founder of Audit Serve, established in 1990. Mitch and his colleagues provide security and IS/ integrated audit consulting services. For additional information contact (203) 972-3567, Levinem@auditserve.com or visit www.auditserve.com.*